



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0034101
(43) 공개일자 2020년03월31일

(51) 국제특허분류(Int. Cl.)

G16C 10/00 (2019.01)

(52) CPC특허분류

G16C 10/00 (2019.02)

G16C 20/10 (2019.02)

(21) 출원번호 10-2018-0113382

(22) 출원일자 2018년09월21일

심사청구일자 2018년09월21일

(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)

파취 아마드

경기도 수원시 영통구 청명남로60번길 24 B04 호

(74) 대리인

김홍석

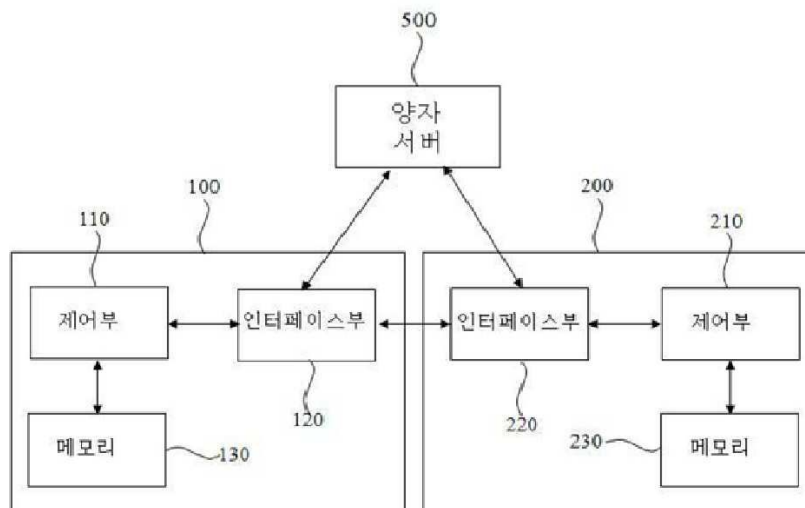
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 다자간 양자얽힘분석방법 및 이를 이용하는 양자시스템

(57) 요약

본 발명에 따른 다자간 양자얽힘 분석 방법이 제공된다. 상기 방법은, 다분 양자 시스템의 서브 시스템 간에 서브-가산성(subadditivity) 만족 여부를 판단하는 서브-가산성 판단 단계; 및 상기 서브-가산성이 만족되면, 상기 서브 시스템의 엔트로피의 합을 이용하여 상기 다분 양자 시스템의 엔트로피의 상한을 설정하는 엔트로피 상한 설정 단계를 포함하고, 새로운 부등식 관계를 갖는 서브시스템의 바이너리 벡터 타입 분포의 해밍 가중치에 기반하는 더 긴밀한 관계를 갖는 다자간 양자 얽힘 분석 방법을 제공할 수 있다.

대표도 - 도2



(52) CPC특허분류

G16C 20/30 (2019.02)

이 발명을 지원한 국가연구개발사업

과제고유번호 2016R1A2B2014462

부처명 미래과학창조부

연구관리전문기관 한국연구재단

연구사업명 개인연구지원사업(중견연구)

연구과제명 양자 초엄힘을 이용한 하이브리드 양자통신 핵심기술 연구

기 여 율 4/10

주관기관 경희대학교 산학협력단

연구기간 2018.04.01 ~ 2019.02.28

이 발명을 지원한 국가연구개발사업

과제고유번호 2018R1D1A1B07050584

부처명 미래과학창조부

연구관리전문기관 한국연구재단

연구사업명 이공분야기초연구사업/이공학개인기초연구지원사업

연구과제명 반사실적 통신 핵심기술 연구

기 여 율 3/10

주관기관 경희대학교 산학협력단

연구기간 2018.06.01 ~ 2019.02.28

이 발명을 지원한 국가연구개발사업

과제고유번호 R0190-15-2030

부처명 미래과학창조부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보통신방송연구개발사업

연구과제명 비밀성증폭 후처리 기술개발

기 여 율 3/10

주관기관 경희대학교 산학협력단

연구기간 2018.05.01 ~ 2019.02.28

명세서

청구범위

청구항 1

다자간 양자얽힘 분석 방법에 있어서,

다분 양자 시스템의 서브 시스템 간에 서브-가산성(subadditivity) 만족 여부를 판단하는 서브-가산성 판단 단계; 및

상기 서브-가산성이 만족되면, 상기 서브 시스템의 엔트로피의 합을 이용하여 상기 다분 양자 시스템의 엔트로피의 상한을 설정하는 엔트로피 상한 설정 단계를 포함하는, 다자간 양자얽힘 분석 방법.

청구항 2

제1항에 있어서,

상기 엔트로피 상한 설정 단계에서,

상기 서브 시스템의 바이너리 벡터 타입의 해밍 가중치($\omega(j)$)에 기반하여, $0 \leq \beta \leq 1$, $q \geq 1$ 및 임의의 다분 양자 상태 $\rho_{A|B_0 B_1, \dots, B_{N-1}}$ 에 대해, Tsallis-q 상호 엔트로피(T_q)에 대한 서브-가산성(subadditivity) 조

$$\left(T_q^a(\rho_{A|B_0 B_1 \dots B_{N-1}})\right)^\beta \leq \sum_{j=0}^{N-1} (2^\beta - 1)^{\omega(j)} \left(T_q^a(\rho_{A|B_j})\right)^\beta$$

건하에서, 상기 상한을

로 설

정하는, 다자간 양자얽힘 분석 방법.

청구항 3

제2 항에 있어서,

상기 서브 시스템의 엔트로피를 상기 해밍 가중치에 기반하여 합산한 상기 상한에 기반하여, 상기 다분 시스템을 상기 서브 시스템으로 분해하는 다분 시스템 분해 단계를 포함하는, 다자간 양자얽힘 분석 방법.

청구항 4

제3 항에 있어서,

상기 다분 시스템 분해 단계는,

$(2^n + 1)$ 개의 양자 상태(quantum state)를 갖는 상기 다분 시스템이

$$T_q^a(\gamma_{AB_0 B_1 \dots B_{2^n-1}}) = T_q^a(\rho_{AB_0 B_1 \dots B_{N-1}})$$

를 만족하여 N개의 양자 상태를 갖

는 제1 서브 시스템으로 분해 가능한지 여부를 판단하고,

상기 제1 서브 시스템으로 분해 가능하면, 상기 다분 시스템의 상한을

$$\begin{aligned} \left(T_q^a(\rho_{AB_0 B_1 \dots B_{N-1}})\right)^\beta &= \left(T_q^a(\gamma_{AB_0 B_1 \dots B_{2^n-1}})\right)^\beta \\ &\leq \sum_{j=0}^{2^n-1} (2^\beta - 1)^{\omega(j)} \left(T_q^a(\gamma_{A|B_j})\right)^\beta \\ &= \sum_{j=0}^{N-1} (2^\beta - 1)^{\omega(j)} \left(T_q^a(\rho_{A|B_j})\right)^\beta, \end{aligned}$$

에 의해 상기 제1 서브 시스템

의 상한을 이용하여 설정하고,

여기서, T_q^a 는 Tsallis-q 상호 엔트로피이고, $\rho_{AB_0B_1 \dots B_{N-1}}$ 는 임의의 다분 시스템 $AB_0B_1 \dots B_{N-1}$ 의 밀도 행렬을 나타내고, $\rho_{AB_0B_1 \dots B_{N-1}}$ 는 임의의 다분 시스템 $AB_0B_1 \dots B_{N-1}$ 의 밀도 행렬을 나타내는, 다자간 양자얽힘 분석 방법.

청구항 5

제4항에 있어서,

상기 제1 서브 시스템으로 분해 가능하면, 상기 제1 서브 시스템에 속하는 양자 기기로 양자 엔트로피 상태 정보를 피드백하고,

상기 제1 서브 시스템으로 분해 가능하고, 상기 제1 서브 시스템의 상한이 임계치 이하이면, 상기 제1 서브 시스템을 이분 양자 시스템으로 분해하는, 다자간 양자얽힘 분석 방법.

청구항 6

다자간 양자얽힘 분석 방법에 있어서,

다분 양자 시스템의 서브 시스템 간에 서브-가산성(subadditivity) 만족 여부를 판단하는 서브-가산성 판단 단계; 및

상기 서브-가산성이 만족되면, 상기 서브 시스템과 연관된 얽힘(entanglement)의 합을 이용하여 상기 다분 양자 시스템의 얽힘의 상한을 설정하는 얽힘 상한 설정 단계를 포함하는, 다자간 양자얽힘 분석 방법.

청구항 7

제6항에 있어서,

상기 얽힘 상한 설정 단계에서,

상기 서브 시스템의 바이너리 벡터 타입의 해밍 가중치($\omega(j)$)에 기반하여, $0 \leq \beta \leq 1$, $q \geq 1$ 및 임의의 다분 양자 상태 $\rho_{AB_0B_1 \dots B_{N-1}}$ 에 대해, 얽힘(E^a)에 대한 서브-가산성(subadditivity) 조건하에서, 상기 상한을

$$(E^a(\rho_{AB_0B_1 \dots B_{N-1}}))^{\beta} \leq \sum_{j=0}^{N-1} (2^{\beta} - 1)^{\omega(j)} (E^a(\rho_{AB_j}))^{\beta}$$

로 설정하는, 다자간 양자얽힘 분석 방법.

청구항 8

제7 항에 있어서,

상기 서브 시스템의 얽힘을 상기 해밍 가중치에 기반하여 합산한 상기 상한에 기반하여, 상기 다분 시스템을 상기 서브 시스템으로 분해하는 다분 시스템 분해 단계를 포함하는, 다분 양자얽힘상태 분석 방법.

청구항 9

제8 항에 있어서,

상기 다분 시스템 분해 과정은,

$(2^n + 1)$ 개의 양자 상태(quantum state)를 갖는 상기 다분 시스템이 N개의 양자 상태를 갖는 제1 서브 시스템으로 분해 가능한지 여부를 판단하고,

상기 제1 서브 시스템으로 분해 가능하면, 상기 다분 시스템과 연관된 얽힘의 상한을

$$\begin{aligned} (E^a(\rho_{A|B_0B_1\cdots B_{N-1}}))^\beta &\leq \sum_{j=0}^{N-1} (2^\beta - 1)^{\omega(j)} (E^a(\rho_{A|B_j}))^\beta \\ &\leq \sum_{j=0}^{N-1} \beta^{\omega(j)} (E^a(\rho_{A|B_j}))^\beta \\ &\leq \sum_{j=0}^{N-1} (E^a(\rho_{A|B_j}))^\beta, \end{aligned}$$

에 의해 상기 제1 서브 시스템

과 연관된 얽힘의 상한을 이용하여 설정하고,

여기서, E^a 는 얽힘(entanglement)이고, $\rho_{A|B_0B_1\cdots B_{N-1}}$ 는 임의의 다분 시스템 $AB_0B_1\cdots B_{N-1}$ 의 밀도 행렬을 나타내는, 다분 양자얽힘상태 분석 방법.

청구항 10

제9항에 있어서,

상기 제1 서브 시스템으로 분해 가능하면, 상기 제1 서브 시스템에 속하는 양자 기기로 양자 얽힘 상태 정보를 피드백하고,

상기 제1 서브 시스템으로 분해 가능하고, 상기 제1 서브 시스템과 연관된 얽힘의 상한이 임계치 이하이면, 상기 제1 서브 시스템을 이분 양자 시스템으로 분해하는, 다분 양자얽힘상태 분석 방법.

청구항 11

다자간 양자얽힘 분석을 수행하는 양자 시스템에 있어서,

다분 양자 시스템에 속하는 양자 기기 간에 양자 정보를 교환하도록 구성된 인터페이스부; 및

상기 다분 양자 시스템의 서브 시스템 간에 서브-가산성(subadditivity) 만족 여부를 판단하고,

상기 서브-가산성이 만족되면, 상기 서브 시스템의 엔트로피의 합을 이용하여 상기 다분 양자 시스템의 엔트로피의 상한을 설정하도록 구성된 제어부를 포함하는, 양자 시스템.

청구항 12

제11항에 있어서,

상기 제어부는,

상기 서브 시스템의 바이너리 벡터 타입의 해밍 가중치($\omega(j)$)에 기반하여, $0 \leq \beta \leq 1$, $q \geq 1$ 및 임의의 다분 양자 상태 $\rho_{A|B_0B_1\cdots B_{N-1}}$ 에 대해, Tsallis-q 상호 엔트로피(T_q^a)에 대한 서브-가산성(subadditivity) 조건하

$$(T_q^a(\rho_{A|B_0B_1\cdots B_{N-1}}))^\beta \leq \sum_{j=0}^{N-1} (2^\beta - 1)^{\omega(j)} (T_q^a(\rho_{A|B_j}))^\beta$$

에서, 상기 상한을
는, 양자 시스템.

로 설정하

청구항 13

제12 항에 있어서,

상기 제어부는,

상기 서브 시스템의 엔트로피를 상기 해밍 가중치에 기반하여 합산한 상기 상한에 기반하여, 상기 다분 시스템을 상기 서브 시스템으로 분해하는 것을 특징으로 하는, 양자 시스템.

청구항 14

제13 항에 있어서,

상기 제어부는,

$(2^n + 1)$ 개의 양자 상태(quantum state)를 갖는 상기 다분 시스템이

$T_q^a(\gamma_{AB_0B_1 \dots B_{2^n-1}}) = T_q^a(\rho_{AB_0B_1 \dots B_{N-1}})$ 를 만족하여 N개의 양자 상태를 갖는 제1 서브 시스템으로 분해 가능한지 여부를 판단하고,

상기 제1 서브 시스템으로 분해 가능하면, 상기 다분 시스템의 상한을

$$\begin{aligned} (T_q^a(\rho_{AB_0B_1 \dots B_{N-1}}))^{\beta} &= (T_q^a(\gamma_{AB_0B_1 \dots B_{2^n-1}}))^{\beta} \\ &\leq \sum_{j=0}^{2^n-1} (2^{\beta} - 1)^{\omega(j)} (T_q^a(\gamma_{A|B_j}))^{\beta} \\ &= \sum_{j=0}^{N-1} (2^{\beta} - 1)^{\omega(j)} (T_q^a(\rho_{A|B_j}))^{\beta}, \end{aligned}$$

에 의해 상기 제1 서브 시스템의 상한을 이용하여 설정하고,

여기서, T_q^a 는 Tsallis-q 상호 엔트로피이고, $\rho_{AB_0B_1 \dots B_{N-1}}$ 는 임의의 다분 시스템 $AB_0B_1 \dots B_{N-1}$ 의 밀도 행렬을 나타내고, $\gamma_{AB_0B_1 \dots B_{2^n-1}}$ 는 임의의 다분 시스템 $AB_0B_1 \dots B_{2^n-1}$ 의 밀도 행렬을 나타내는, 양자 시스템.

청구항 15

제14 항에 있어서,

상기 제어부는,

상기 제1 서브 시스템으로 분해 가능하면, 상기 제1 서브 시스템에 속하는 양자 기기로 양자 엔트로피 상태 정보를 피드백하도록 제어하고,

상기 제1 서브 시스템으로 분해 가능하고, 상기 제1 서브 시스템의 상한이 임계치 이하이면, 상기 제1 서브 시스템을 이분 양자 시스템으로 분해하는, 양자 시스템.

청구항 16

다자간 양자얽힘 분석을 수행하는 양자 시스템에 있어서,

다분 양자 시스템에 속하는 양자 기기 간에 양자 정보를 교환하도록 구성된 인터페이스부; 및

상기 다분 양자 시스템의 서브 시스템 간에 서브-가산성(subadditivity) 만족 여부를 판단하고,

상기 서브-가산성이 만족되면, 상기 서브 시스템과 연관된 얽힘(entanglement)의 합을 이용하여 상기 다분 양자 시스템의 얽힘의 상한을 설정하는 제어부를 포함하는, 양자 시스템.

청구항 17

제16항에 있어서,

상기 제어부는,

상기 서브 시스템의 바이너리 벡터 타입의 해밍 가중치($\omega(j)$)에 기반하여, $0 \leq \beta \leq 1$, $q \geq 1$ 및 임의의 다분 양자 상태 $\rho_{A|B_0B_1 \dots B_{N-1}}$ 에 대해, 얽힘(E^a)에 대한 서브-가산성(subadditivity) 조건하에서, 상기 상한을

$$(E^a(\rho_{A|B_0B_1\cdots B_{N-1}}))^{\beta} \leq \sum_{j=0}^{N-1} (2^{\beta} - 1)^{\omega(j)} (E^a(\rho_{A|B_j}))^{\beta}$$

로 설정하는, 양자 시스템.

청구항 18

제17 항에 있어서,

상기 제어부는,

상기 서버 시스템의 얽힘을 상기 해밍 가중치에 기반하여 합산한 상기 상한에 기반하여, 상기 다분 시스템을 상기 서버 시스템으로 분해하는 다분 시스템 분해 단계를 포함하는, 양자 시스템.

청구항 19

제18 항에 있어서,

상기 제어부는,

$(2^n + 1)$ 개의 양자 상태(quantum state)를 갖는 상기 다분 시스템이 N개의 양자 상태를 갖는 제1 서버 시스템으로 분해 가능한지 여부를 판단하고,

상기 제1 서버 시스템으로 분해 가능하면, 상기 다분 시스템과 연관된 얽힘의 상한을

$$\begin{aligned} (E^a(\rho_{A|B_0B_1\cdots B_{N-1}}))^{\beta} &\leq \sum_{j=0}^{N-1} (2^{\beta} - 1)^{\omega(j)} (E^a(\rho_{A|B_j}))^{\beta} \\ &\leq \sum_{j=0}^{N-1} \beta^{\omega(j)} (E^a(\rho_{A|B_j}))^{\beta} \\ &\leq \sum_{j=0}^{N-1} (E^a(\rho_{A|B_j}))^{\beta}, \end{aligned}$$

에 의해 상기 제1 서버 시스템

과 연관된 얽힘의 상한을 이용하여 설정하고,

여기서, E^a 는 얽힘(entanglement)이고, $\rho_{A|B_0B_1\cdots B_{N-1}}$ 는 임의의 다분 시스템 $AB_0B_1\cdots B_{N-1}$ 의 밀도 행렬을 나타내는, 양자 시스템.

청구항 20

제19항에 있어서,

상기 제어부는,

상기 제1 서버 시스템으로 분해 가능하면, 상기 제1 서버 시스템에 속하는 양자 기기로 양자 얽힘 상태 정보를 피드백하도록 제어하고,

상기 제1 서버 시스템으로 분해 가능하고, 상기 제1 서버 시스템과 연관된 얽힘의 상한이 임계치 이하이면, 상기 제1 서버 시스템을 이분 양자 시스템으로 분해하는, 양자 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 양자얽힘분석방법 및 이를 이용하는 양자시스템에 관한 것이다. 보다 상세하게는, 다자간 양자얽힘분석방법 및 이를 이용하는 양자 기기를 포함하는 양자시스템에 관한 것이다.

배경 기술

[0002] 얽힘(Entanglement)은 양자 역학 분야에서 가장 특징적이고 놀라운 현상이다. 이러한 현상은 양자 역학의 핵심에 해당하는 것으로 간주된다. 얽힘은 예컨대 양자 키 분배, 초집적 코딩 및 양자 전송과 같은 양자 정보 처리의 다양한 응용을 갖는다.

[0003] 한편, 얽힘의 가장 흥미로운 특징 중 하나는 모노가미 행동(monogamous behavior)이다. 두 대상이 상호 간에 최대 얽힘 상태이면, 이들은 이들의 상관(correlation)을 제3자와 공유할 수 없다. 제3자와 이들의 상관관계는 두 대상 간의 얽힘량에 의해 크게 제한된다. 한편, 상이한 얽힘 측정과 관련된 모노가미에 대해 연구가 진행되었으나, 임의의 양자 상태에 대한 다분 시스템으로 일반화가 수행될 필요가 있다.

[0004] 한편, 상이한 얽힘 측정에 대한 폴리가미 관계의 설정 이후에, 이들의 관계의 긴밀성(tightness)에 대한 연구가 필요하다. 하지만, 이와 같이 상이한 얽힘 측정에 대한 폴리가미 관계 설정 이후, 이들의 관계에 대한 긴밀성에 대한 명시적인 연구가 없다는 문제점이 있었다.

[0005] 따라서, 본 발명에서는 일반화된 모노가미 관계와 함께 양자 상태 간의 더 긴밀한 결과를 제공할 필요가 있다.

발명의 내용

해결하려는 과제

[0006] 따라서, 본 발명에서 해결하고자 하는 과제는, 다자간 양자얽힘분석방법 및 이를 이용하는 양자 기기를 포함하는 양자시스템을 제공하는 것을 목표로 한다.

[0007] 또한, 본 발명에서 해결하고자 하는 과제는, 임의의 차원의 다자간 양자 시스템의 엔트로피 및/또는 얽힘에 대한 더 긴밀한 한계를 제공하는 것을 목표로 한다.

과제의 해결 수단

[0008] 상기와 같은 과제를 해결하기 위해 본 발명에 따른 다자간 양자얽힘 분석 방법이 제공된다. 상기 방법은, 다분 양자 시스템의 서브 시스템 간에 서브-가산성(subadditivity) 만족 여부를 판단하는 서브-가산성 판단 단계; 및 상기 서브-가산성이 만족되면, 상기 서브 시스템의 엔트로피의 합을 이용하여 상기 다분 양자 시스템의 엔트로피의 상한을 설정하는 엔트로피 상한 설정 단계를 포함하고, 새로운 부등식 관계를 갖는 서브시스템의 바이너리 벡터 타입 분포의 해밍 가중치에 기반하는 더 긴밀한 관계를 갖는 다자간 양자 얽힘 분석 방법을 제공할 수 있다.

[0009] 일 실시예에서, 상기 엔트로피 상한 설정 단계에서, 상기 서브 시스템의 바이너리 벡터 타입의 해밍 가중치($\omega(j)$)에 기반하여 상기 상한을

$$(T_q^a(\rho_{A|B_0B_1\cdots B_{N-1}}))^{\beta} \leq \sum_{j=0}^{N-1} (2^{\beta} - 1)^{\omega(j)} (T_q^a(\rho_{A|B_j}))^{\beta}$$

로 설정할 수 있다.

[0010] 일 실시예에서, 상기 서브 시스템의 엔트로피를 상기 해밍 가중치에 기반하여 합산한 상기 상한에 기반하여, 상기 다분 시스템을 상기 서브 시스템으로 분해할 수 있다.

[0011] 일 실시예에서, 상기 다분 시스템 분해 과정은, $(2^n + 1)$ 개의 양자 상태(quantum state)를 갖는 상기 다분 시스템이

$$T_q^a(\gamma_{AB_0B_1\cdots B_{2^n-1}}) = T_q^a(\rho_{AB_0B_1\cdots B_{N-1}})$$

를 만족하여 N개의 양자 상태를 갖는 제1 서브 시스템으로 분해 가능한지 여부를 판단할 수 있다. 이때, 상기 제1 서브 시스템으로 분해 가능하면, 상기 다분 시스템의 상한을 수학적식 23에 의해 상기 제1 서브 시스템의 상한을 이용하여 설정할 수 있다.

[0012] 일 실시예에서, 상기 제1 서브 시스템으로 분해 가능하면, 상기 제1 서브 시스템에 속하는 양자 기기로 양자 엔트로피 상태 정보를 피드백할 수 있다. 또한, 상기 제1 서브 시스템으로 분해 가능하고, 상기 제1 서브 시스템의 상한이 임계치 이하이면, 상기 제1 서브 시스템을 이분 양자 시스템으로 분해할 수 있다.

[0013] 본 발명의 다른 측면에 따른 다자간 양자얽힘 분석 방법이 제공된다. 상기 방법은, 다분 양자 시스템의 서브 시스템 간에 서브-가산성(subadditivity) 만족 여부를 판단하는 서브-가산성 판단 단계; 및 상기 서브-가산성이

만족되면, 상기 서브 시스템과 연관된 얽힘(entanglement)의 합을 이용하여 상기 다분 양자 시스템의 얽힘의 상한을 설정하는 얽힘 상한 설정 단계를 포함한다.

[0014] 일 실시예에서, 상기 얽힘 상한 설정 단계에서, 상기 서브 시스템의 바이너리 벡터 타입의 해밍 가중치($\omega(j)$)

$$(E^a(\rho_{A|B_0B_1\cdots B_{N-1}}))^{\beta} \leq \sum_{j=0}^{N-1} (2^{\beta} - 1)^{\omega(j)} (E^a(\rho_{A|B_j}))^{\beta}$$

에 기반하여 상기 상한을
로 설정
할 수 있다.

[0015] 일 실시예에서, 상기 서브 시스템의 얽힘을 상기 해밍 가중치에 기반하여 합산한 상기 상한에 기반하여, 상기 다분 시스템을 상기 서브 시스템으로 분해할 수 있다.

[0016] 일 실시예에서, 상기 다분 시스템 분해 과정은, $(2^n + 1)$ 개의 양자 상태(quantum state)를 갖는 상기 다분 시스템이 N개의 양자 상태를 갖는 제1 서브 시스템으로 분해 가능한지 여부를 판단할 수 있다. 이때, 상기 제1 서브 시스템으로 분해 가능하면, 상기 다분 시스템과 연관된 얽힘의 상한을 수학적 식 24에 의해 상기 제1 서브 시스템과 연관된 얽힘의 상한을 이용하여 설정할 수 있다.

[0017] 일 실시예에서, 상기 제1 서브 시스템으로 분해 가능하면, 상기 제1 서브 시스템에 속하는 양자 기기로 양자 얽힘 상태 정보를 피드백할 수 있다. 또한, 상기 제1 서브 시스템으로 분해 가능하고, 상기 제1 서브 시스템과 연관된 얽힘의 상한이 임계치 이하이면, 상기 제1 서브 시스템을 이분 양자 시스템으로 분해할 수 있다.

[0018] 본 발명의 또 다른 측면에 따른 다자간 양자얽힘 분석을 수행하는 양자 시스템이 제공된다. 상기 양자 시스템은, 다분 양자 시스템에 속하는 양자 기기 간에 양자 정보를 교환하도록 구성된 인터페이스부; 및 상기 다분 양자 시스템의 서브 시스템 간에 서브-가산성(subadditivity) 만족 여부를 판단하고, 상기 서브-가산성이 만족되면, 상기 서브 시스템의 엔트로피의 합을 이용하여 상기 다분 양자 시스템의 엔트로피의 상한을 설정하도록 구성된 제어부를 포함한다.

[0019] 일 실시예에서, 제어부는, 상기 서브 시스템의 바이너리 벡터 타입의 해밍 가중치($\omega(j)$)에 기반하여

$$(T_q^a(\rho_{A|B_0B_1\cdots B_{N-1}}))^{\beta} \leq \sum_{j=0}^{N-1} (2^{\beta} - 1)^{\omega(j)} (T_q^a(\rho_{A|B_j}))^{\beta}$$

로 상기 상한을 설정할 수 있다.

[0020] 일 실시예에서, 상기 제어부는, 상기 서브 시스템의 엔트로피를 상기 해밍 가중치에 기반하여 합산한 상기 상한에 기반하여, 상기 다분 시스템을 상기 서브 시스템으로 분해할 수 있다.

[0021] 일 실시예에서, 상기 제어부는, $2^n + 1$ 개의 양자 상태(quantum state)를 갖는 상기 다분 시스템이

$$T_q^a(\gamma_{AB_0B_1\cdots B_{2^n-1}}) = T_q^a(\rho_{AB_0B_1\cdots B_{N-1}})$$

를 만족하여 N개의 양자 상태를 갖는 제1 서브 시스템으로 분해 가능한지 여부를 판단할 수 있다. 이때, 상기 제1 서브 시스템으로 분해 가능하면, 상기 다분 시스템의 상한을 수학적 식 23에 의해 상기 제1 서브 시스템의 상한을 이용하여 설정할 수 있다.

[0022] 일 실시예에서, 상기 제어부는, 상기 제1 서브 시스템으로 분해 가능하면, 상기 제1 서브 시스템에 속하는 양자 기기로 양자 엔트로피 상태 정보를 피드백하도록 제어할 수 있다. 또한, 상기 제1 서브 시스템으로 분해 가능하고, 상기 제1 서브 시스템의 상한이 임계치 이하이면, 상기 제1 서브 시스템을 이분 양자 시스템으로 분해할 수 있다.

[0023] 본 발명의 또 다른 측면에 따른 다자간 양자얽힘 분석을 수행하는 양자 시스템이 제공된다. 상기 양자 시스템은 다분 양자 시스템에 속하는 양자 기기 간에 양자 정보를 교환하도록 구성된 인터페이스부; 및 상기 다분 양자 시스템의 서브 시스템 간에 서브-가산성(subadditivity) 만족 여부를 판단하고, 상기 서브-가산성이 만족되면, 상기 서브 시스템과 연관된 얽힘(entanglement)의 합을 이용하여 상기 다분 양자 시스템의 얽힘의 상한을 설정하는 제어부를 포함한다.

[0024] 일 실시예에서, 제어부는, 상기 서브 시스템의 바이너리 벡터 타입의 해밍 가중치($\omega(j)$)에 기반하여

$$(E^a(\rho_{A|B_0B_1\cdots B_{N-1}}))^{\beta} \leq \sum_{j=0}^{N-1} (2^{\beta} - 1)^{\omega(j)} (E^a(\rho_{A|B_j}))^{\beta}$$

로 상기 상한을 설정할 수 있다.

[0025] 일 실시 예에서, 상기 제어부는, 상기 서버 시스템의 얽힘을 상기 해밍 가중치에 기반하여 합산한 상기 상한에 기반하여, 상기 다분 시스템을 상기 서버 시스템으로 분해할 수 있다.

[0026] 일 실시 예에서, 상기 제어부는, $(2^n + 1)$ 개의 양자 상태(quantum state)를 갖는 상기 다분 시스템이 N개의 양자 상태를 갖는 제1 서버 시스템으로 분해 가능한지 여부를 판단할 수 있다. 또한, 상기 제1 서버 시스템으로 분해 가능하면, 상기 다분 시스템과 연관된 얽힘의 상한을 수학적 식 24에 의해 상기 제1 서버 시스템과 연관된 얽힘의 상한을 이용하여 설정할 수 있다.

[0027] 일 실시 예에서, 상기 제어부는, 상기 제1 서버 시스템으로 분해 가능하면, 상기 제1 서버 시스템에 속하는 양자 기기로 양자 얽힘 상태 정보를 피드백하도록 제어할 수 있다. 또한, 상기 제1 서버 시스템으로 분해 가능하고, 상기 제1 서버 시스템과 연관된 얽힘의 상한이 임계치 이하이면, 상기 제1 서버 시스템을 이분 양자 시스템으로 분해할 수 있다.

발명의 효과

[0028] 본 발명의 적어도 일 실시예에 따르면, 새로운 부등식 관계를 갖는 서브시스템의 바이너리 벡터 타입 분포의 해밍 가중치에 기반하는 더 긴밀한 관계를 갖는 다자간 양자 얽힘 분석 방법을 제공할 수 있다는 장점이 있다.

[0029] 또한, 본 발명의 적어도 일 실시예에 따르면, 고차원 큐빗 시스템에 대한 von Neumann 엔트로피의 일반화를 제공할 수 있다는 장점이 있다.

[0030] 또한, 본 발명의 적어도 일 실시예에 따르면, 얽힘 형태의 관계보다 더 긴밀한 특성을 갖는다. 폴리가미 관계의 긴밀성은 보조 얽힘 분포의 더 세밀한 특성을 반영할 수 있다는 장점이 있다.

도면의 간단한 설명

[0031] 도 1은 본 발명에 따른 다자가 양자 얽힘 분석을 수행하는 양자 시스템을 도시한다.

도 2는 본 발명에 따른 양자 기기 및 양자 서버의 상세 구성을 도시한다.

도 3은 본 발명과 관련하여, t의 함수로서 t 및 $2^t - 1$ 의 나머지 상한(residual bound)을 나타낸다.

도 4는 본 발명의 일 실시예에 따른 엔트로피 기반 다자간 양자얽힘 분석 방법의 흐름도를 나타낸다.

도 5는 본 발명의 다른 실시예에 따른 양자얽힘 기반 다자간 양자얽힘 분석 방법의 흐름도를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0032] 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.

[0033] 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용한다.

[0034] 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.

[0035] 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.

- [0036] 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.
- [0037] 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않아야 한다.
- [0038] 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.
- [0039] 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.
- [0040] 이하, 본 발명에 따른 다자간 양자얽힘 분석 방법 및 이를 수행하는 양자 시스템에 대해 살펴보기로 하자.
- [0041] 이와 관련하여, 도 1은 본 발명에 따른 다자가 양자 얽힘 분석을 수행하는 양자 시스템을 도시한다. 도 1에 도시된 바와 같이, 양자 시스템은 복수의 서버 시스템을 포함하고, 편의상 제1 서버 시스템(100) 내지 제4 서버 시스템(400)이 포함된 것으로 표현할 수 있다. 하지만, 상기 제1 내지 제4 서버 시스템(100 내지 400)에만 한정되는 것이 아니라, 임의의 개수의 서버 시스템 간에도 적용될 수 있다. 한편, 상기 제1 내지 제4 서버 시스템(100 내지 400) 간의 양자 통신 또는 양자 암호화를 수행하는 양자 서버(500)를 더 포함할 수 있다. 이때, 양자 서버(500)는 상기 제1 내지 제4 서버 시스템(100 내지 400)으로부터 다분 양자 상태에 관한 정보를 수신하고, 양자 상태 정보를 이용하여 다분 양자얽힘상태를 구분할 수 있다. 이때, 양자 서버(500)는 제1 내지 제3 서버 시스템 (100 내지 300)으로부터 양자 상태에 관한 정보를 수신하고, 양자 상태 정보를 이용하여 삼분 양자얽힘 상태를 구분할 수 있다. 또한, 양자 서버(500)는 제1 내지 제3 서버 시스템 (100 내지 400)으로부터 양자 상태에 관한 정보를 수신하고, 양자 상태 정보를 이용하여 사분 양자 양자얽힘상태를 구분할 수 있다. 한편, 양자 서버(500)는 서버 시스템의 개수에 따라 n분 양자얽힘 상태를 구분할 수 있다.
- [0042] 또한, 상기 제1 내지 제4 서버 시스템(100-400)은 임의의 양자 기기이거나 이들 간에 통신을 수행하는 양자 서버일 수 있다. 즉, 제1 내지 제4 서버 시스템(100 내지 400)은 각각 송신 기기인 제1 양자 기기와 수신 기기인 제2 양자 기기이거나 이들 간에 통신을 수행하는 양자 서버일 수 있다. 이때, 양자 서버(500) 없이, 제1 내지 제4 서버 시스템(100 내지 400) 중 어느 하나가 양자 서버의 역할을 수행할 수 있다.
- [0043] 도 2는 본 발명에 따른 양자 기기 및 양자 서버의 상세 구성을 도시한다. 편의상, 양자 기기들을 제1 내지 제4 양자 기기(100 내지 400)으로, 양자 서버를 양자 서버(500)로 지칭할 수 있다. 한편, 제1 내지 제4 양자 기기(100 내지 400) 중 어느 하나가 양자 서버(500)를 대신하여 양자 서버의 역할을 하는 경우를 포함할 수 있다.
- [0044] 한편, 도 2는 본 발명에 따른 다자간 양자얽힘 분석 방법을 수행하는 양자 기기의 상세 구성을 나타낸다. 한편, 본 발명에 따른 다자간 양자얽힘 분석 방법은 송신 기기인 제1 기기(100) 또는 수신 기기인 제2 기기(200)에 수행되거나, 또는 양자 서버(500)에 의해서 수행될 수 있다. 이하 설명에서는 편의상 제1 기기(100) 또는 제2 기기(200)에 의해 수행되는 것으로 설명하지만, 이에 한정되지 않고 다양한 엔티티에 의해 수행 가능하다.
- [0045] 인터페이스부(120, 220)는 다분 양자 시스템에 속하는 양자 기기 간에 양자 정보를 교환하도록 구성된다. 한편, 제어부(110, 210)는 상기 다분 양자 시스템의 서버 시스템 간에 서버-가산성(subadditivity) 만족 여부를 판단한다. 또한, 제어부(110, 210)는 상기 서버-가산성이 만족되면, 상기 서버 시스템의 엔트로피의 합을 이용하여 상기 다분 양자 시스템의 엔트로피의 상한을 설정하도록 구성된다. 한편, 메모리(130, 230)은 양자얽힘 분석, 엔트로피 관련 또는 양자 통신과 관련된 양자 정보 및 일반 정보를 저장하도록 구성된다.
- [0046] 한편, 본 발명에 따른 다자간 양자얽힘 분석 방법은 전술한 바와 같이 엔트로피 기반 분석 이외에 얽힘(entanglement) 기반 분석에 의해서도 수행 가능하다.
- [0047] 이러한 경우에도 제어부(110, 210)는 상기 다분 양자 시스템의 서버 시스템 간에 서버-가산성(subadditivity) 만족 여부를 판단한다. 또한, 제어부(110, 210)는 상기 서버-가산성이 만족되면, 상기 서버 시스템과 연관된 얽힘(entanglement)의 합을 이용하여 상기 다분 양자 시스템의 얽힘의 상한을 설정하도록 구성된다. 또한, 메모리(130, 230)은 양자얽힘 분석 또는 양자 통신과 관련된 양자 정보 및 일반 정보를 저장하도록 구성된다.
- [0048] 전술한 바와 같이 본 발명에 따른 다자간 양자얽힘 분석을 위하여 모노가미 및 폴리가미에 기반한 서버 시스템

에서의 해당 동작이 필요하다. 이와 관련하여, 모노가미에 대한 수학적 표현에 대해 살펴보면 다음과 같다.

[0049] 수학적으로, 모노가미는 임의의 3-큐빗 양자 시스템, 예를 들어 ρ_{ABC} 에 대하여 수학적 식 1과 같이 표현되는 부등식에 의해 특징된다.

수학적 식 1

$$\tau(\rho_{A|BC}) \geq \tau(\rho_{AB}) + \tau(\rho_{AC})$$

[0050]

[0051] 여기서, $\tau(\cdot)$ 는 두 개의 서브 시스템, 예컨대 $\tau(\rho_{AB})$ 는 서브시스템 A 및 B 간의 얽힘을 정량화하는 임의의 2분 얽힘 측정이다. 여기서, ρ_{AB} 는 서브시스템 AB의 감소된 밀도 행렬, 즉 $\rho_{AB} = \text{tr}_C(\rho_{ABC})$ 이다. 본 발명에서는 시스템이 두 개 이상의 대상으로 이루어진 경우 해당 시스템의 이분화(bipartition)에 대해 명시적으로 언급한다. 이와 관련하여, $\tau(\rho_{A|BC})$ 는 서브시스템 A와 BC 간에 얽힘일 수 있다.

[0052] 모노가미 부등식이 공유 능력 얽힘을 한정하는 반면에, 폴리가미 부등식은 다분 시스템의 이분 얽힘의 분포에 관한 하한(lower bound)을 수학적 식 2와 같이 제공할 수 있다.

수학적 식 2

$$\tau^a(\rho_{A|BC}) \leq \tau^a(\rho_{AB}) + \tau^a(\rho_{AC})$$

[0053]

[0054] 여기서, $\tau^a(\rho_{A|BC})$ 는 보조 얽힘이다.

[0055] 한편, 큐빗 시스템에 대한 보조 얽힘의 폴리가미(polygamy of assisted entanglement)가 von Neumann 엔트로피, Tsallis 엔트로피, Renyi 엔트로피 및 통합 엔트로피 등과 같은 다양한 엔트로피에 대하여 제안된다. von Neumann 엔트로피 및 Tsallis 엔트로피와 관련된 결과들이 큐빗(qubit) 시스템에 일반화 가능하다. 상이한 얽힘 측정에 대한 폴리가미 관계의 설정 이후에, 이들의 관계의 긴밀성(tightness)에 대한 연구가 필요하다. 예를 들어, 보조 얽힘에 대한 더 긴밀한 폴리가미 관계가 서브시스템의 바이너리 벡터 관련 분포의 해밍 가중치를 이용하여 설정될 수 있다. 본 발명에서는 새로운 부등식 관계를 제안한다. 서브 시스템의 바이너리 벡터 관련 분포의 해밍 가중치를 이용하여, β 번째 거듭제곱(power) ($0 \leq \beta \leq 1$)에 대한 보조 Tsallis 엔트로피의 폴리가미 부등식을 제공할 수 있다. 본 발명에 대한 결과는 일반화된 모노가미 관계를 제공하고, 이는 더 긴밀한 결과를 제공한다.

[0056] **쓰살리스-엔트로피 및 해밍 가중치(Tsallis Entropy and Hamming Weight)**

[0057] ρ 를 양자 상태라 하면, 차수 q 의 Tsallis 엔트로피는 수학적 식 3과 같이 표현된다.

수학적 식 3

$$T_q(\rho) = \frac{1}{q-1} (1 - \text{tr}\rho^q)$$

[0058]

[0059] 여기서, $q > 0$ 이고, $q \neq 1$ 이다. 순수 이분 상태(pure bipartite state)에 대한 Tsallis- q 얽힘은 수학적 식 4와 같이 표현된다.

수학식 4

$$\mathcal{T}_q(|\psi\rangle_{AB}) = T_q(\rho_A)$$

[0060]

[0061] 여기서, $\rho_A = \text{tr}_B |\psi\rangle_{AB} \langle \psi|$ 는 서브시스템 A의 감소된 밀도 행렬(reduced density matrix)이다. Tsallis 엔트로피의 보조는 수학식 5와 같이 혼합 상태에 대해 정의된다.

수학식 5

$$\mathcal{T}_q^a(\rho_{AB}) = \max \sum_i p_i \mathcal{T}_q(|\psi_i\rangle_{AB})$$

[0062]

[0063] 여기서, 최대화는 ρ_{AB} 의 모든 가능한 순수 상태 분해를 통해 수행된다.

[0064] 비-네거티브 정수 j의 바이너리 표현은 수학식 6과 같이 표현된다.

수학식 6

$$j = \sum_{i=0}^{n-1} b_i 2^i$$

[0065]

[0066] 여기서, $i = 0, \dots, n-1$ 에 대해, $j \leq 2n$, $b_i \in \{0, 1\}$ 이다. 이때, 수학식 7과 같이 특이(unique) 바이너리 벡터를 표현할 수 있다.

수학식 7

$$\mathbf{j} = (b_0, b_1, \dots, b_{n-1})$$

[0067]

[0068] j의 해밍 가중치는 $\omega(j)$ 에 의해 표현되고, 이는 해당 좌표에서 1의 개수에 의해 판단된다.

[0069] **뜨랄리스-q 엔트로피의 폴리가미 관계(Polygamy Relation of Tsallis-q Entropy)**

[0070] 본 발명에서는 아래와 같은 결과를 얻기 위해 양자 네트워크에 관한 서브시스템의 바이너리 벡터 관련 분포를 이용하여 더 긴밀한 부등식 관계를 유도하고, 이러한 부등식 관계를 적용한다.

[0071] **Lemma 1** $0 \leq x \leq 1$ 및 임의의 양의 실수 $0 \leq t \leq 1$ 에 대해, 수학식 8의 관계를 얻을 수 있다.

수학식 8

$$(1+x)^t \leq 1 + (2^t - 1)x^t$$

[0072]

[0073] 이와 관련하여 베르누이 부등식 관계는 $0 \leq t \leq 1$ 및 $0 \leq x \leq 1$ 에 대해 $(1+x)^t \leq 1 + tx^t$ 이다. 위의

Lemma 1의 부등식과 베르누이 부등식의 차이점은 우측의 t 대신에 $2^t - 1$ 의 요소를 갖는다는 점이다. 도 3은 본 발명과 관련하여, t 의 함수로서 t 및 $2^t - 1$ 의 나머지 상한(residual bound)을 나타낸다. 이제, 서브시스템의 바이너리 벡터 타입 분포의 해밍 가중치에 기반한 폴리가미 관계의 결과를 제시하기로 한다.

Theorem 2 $0 \leq \beta \leq 1$, $q \geq 1$ 및 임의의 다분 양자 상태 $\rho_{A|B_0 B_1 \dots B_{N-1}}$ 에 대해, Tsallis- q 상호 엔트로피에 대한 서브-가산성(subadditivity) 조건하에서 수학적 9가 성립한다.

수학적 9

$$(T_q^a(\rho_{A|B_0 B_1 \dots B_{N-1}}))^\beta \leq \sum_{j=0}^{N-1} (2^\beta - 1)^{\omega(j)} (T_q^a(\rho_{A|B_j}))^\beta$$

이와 관련하여, Tsallis- q 엔트로피의 서브-가산성의 조건이 만족한다고 가정하자. 양자 네트워크의 순서화 및 재인덱싱화 이후에, $j = 0, \dots, N-2$ 에 대해 수학적 10과 같은 형태로 서브시스템을 가정할 수 있다.

수학적 10

$$T_q^a(\rho_{A|B_j}) \geq T_q^a(\rho_{A|B_{j+1}}) \geq 0$$

$0 \leq \beta \leq 1$ 에 대해 함수 $f(x) = x^\beta$ 의 단조성(monotonicity)으로부터, Tsallis 엔트로피의 폴리가미 부등식은 수학적 11과 같다.

수학적 11

$$(T_q^a(\rho_{A|B_0 B_1 \dots B_{N-1}}))^\beta \leq \left(\sum_{j=0}^{N-1} T_q^a(\rho_{A|B_j}) \right)^\beta$$

이러한 theorem을 증명하기 위해, 아래의 수학적 12와 같은 조건을 증명하는 것으로 충분하다.

수학적 12

$$\left(\sum_{j=0}^{N-1} T_q^a(\rho_{A|B_j}) \right)^\beta \leq \sum_{j=0}^{N-1} (2^\beta - 1)^{\omega(j)} (T_q^a(\rho_{A|B_j}))^\beta$$

n 에 대한 수학적 귀납법을 이용하여 $N = 2n$ 에 대해 상기 부등식이 유효하다는 것을 증명할 수 있다. 이후, 이를 임의의 비-네거티브 정수 N 으로 확장할 수 있다. $n = 1$ 및 임의의 3분 상태(tripartite state) $\rho_{AB_0 B_1}$ 에 대해, 수학적 11의 우측을 아래의 수학적 13과 같이 표현할 수 있다.

수학식 13

$$\begin{aligned} & (T_q^a(\rho_{A|B_0}) + T_q^a(\rho_{A|B_1}))^\beta \\ &= (T_q^a(\rho_{A|B_0}))^\beta \left(1 + \frac{T_q^a(\rho_{A|B_1})}{T_q^a(\rho_{A|B_0})}\right)^\beta \end{aligned}$$

[0083]

[0084] $0 \leq T_q^a(\rho_{A|B_1}) / T_q^a(\rho_{A|B_0}) \leq 1$ 인 서브 시스템의 순서화에 기인하여, 수학식 13을 수학식 14와 같이 재작성할 수 있다.

수학식 14

$$\begin{aligned} & (T_q^a(\rho_{A|B_0}) + T_q^a(\rho_{A|B_1}))^\beta \\ & \leq (T_q^a(\rho_{A|B_0}))^\beta + (2^\beta - 1) (T_q^a(\rho_{A|B_1}))^\beta \end{aligned}$$

[0085]

[0086] 여기서, 부등식은 Lemma 1에 기인한다. 수학식 14로부터, $n = 1$ 에 대하여, 수학식 12를 복원할 수 있다. 본 발명에서는 $n \geq 2$ 인 경우 $N = 2^n - 1$ 에 대해 수학식 12가 유효하다고 가정한다. 이후, $N = 2n$ 인 경우에 대해, 감소된 밀도 행렬 ρ_{AB_j} 를 갖는 $(N + 1)$ -큐빗 상태 $\rho_{AB_0B_1 \dots B_{N-1}}$ 에 대해 수학식 15가 성립한다.

수학식 15

$$\begin{aligned} & \left(\sum_{j=0}^{N-1} T_q^a(\rho_{A|B_j}) \right)^\beta \leq \left(\sum_{j=0}^{2^{n-1}-1} T_q^a(\rho_{A|B_j}) \right)^\beta \\ & \quad \times \left(1 + \frac{\sum_{j=2^{n-1}}^{2^n-1} T_q^a(\rho_{A|B_j})}{\sum_{j=0}^{2^{n-1}-1} T_q^a(\rho_{A|B_j})} \right)^\beta \end{aligned}$$

[0087]

[0088] 서브시스템의 순서화와 Lemma 1을 통해 수학식 16을 얻을 수 있다.

수학식 16

$$\begin{aligned} & \left(\sum_{j=0}^{N-1} T_q^a(\rho_{A|B_j}) \right)^\beta \leq \left(\sum_{j=0}^{2^{n-1}-1} T_q^a(\rho_{A|B_j}) \right)^\beta \\ & \quad + (2^\beta - 1) \left(\sum_{j=2^{n-1}}^{2^n-1} T_q^a(\rho_{A|B_j}) \right)^\beta \end{aligned}$$

[0089]

[0090] 귀납 가정에 기인하여, 수학식 16의 우측의 첫번째 term은 수학식 17과 같이 표현될 수 있다.

수학식 17

$$\left(\sum_{j=0}^{2^{n-1}-1} T_q^a(\rho_{A|B_j}) \right)^\beta \leq \sum_{j=0}^{2^{n-1}-1} (2^\beta - 1)^{\omega(j)} (T_q^a(\rho_{A|B_j}))^\beta$$

[0091]

[0092] 수학식 16에서, 두번째 term은 $j = 2^{n-1}$ 에서 $j = 2^n - 1$ 까지의 합에 해당한다. 따라서, 필요하다면 가능한 순서화와 재인덱싱화 이후, 귀납 가정으로부터 수학식 18이 성립한다.

수학식 18

$$\left(\sum_{j=2^{n-1}}^{2^n-1} T_q^a(\rho_{A|B_j}) \right)^\beta \leq \sum_{j=2^{n-1}}^{2^n-1} (2^\beta - 1)^{\omega(j)-1} (T_q^a(\rho_{A|B_j}))^\beta$$

[0093]

[0094] 이후, 수학식 16, 17 및 18로부터, 수학식 19가 성립한다.

수학식 19

$$\left(\sum_{j=0}^{2^n-1} T_q^a(\rho_{A|B_j}) \right)^\beta \leq \sum_{j=0}^{2^n-1} (2^\beta - 1)^{\omega(j)} (T_q^a(\rho_{A|B_j}))^\beta$$

[0095]

[0096] 이는 수학식 12의 결과와 동일하다.

[0097] 이제, 임의의 양의 정수 N 및 $(N + 1)$ 다분 상태 $\rho_{AB_0B_1 \dots B_{N-1}}$ 을 고려하기로 한다. 한편, n 에 대한 상한 $0 \leq N \leq 2^n$ 에 해당하는 2의 거듭제곱을 고려할 수 있다. 또한, $(2n + 1)$ -다자간 양자 상태(party quantum state)를 고려할 수 있고, 이는 수학식 20과 같은 두 개의 상태의 곱으로 표현 가능하다.

수학식 20

$$\gamma_{AB_0B_1 \dots B_{2n-1}} = \rho_{AB_0B_1 \dots B_{N-1}} \otimes \sigma_{B_N \dots B_{2n-1}}$$

[0098]

[0099] 수학식 19로부터, 다분 상태 $\gamma_{AB_0B_1 \dots B_{2n-1}}$ 은 수학식 21의 부등호 관계가 성립한다.

수학식 21

$$(T_q^a(\gamma_{AB_0B_1\cdots B_{2^n-1}}))^\beta \leq \sum_{j=0}^{2^n-1} (2^\beta - 1)^{\omega(j)} (T_q^a(\gamma_{A|B_j}))^\beta$$

[0100]

[0101] 여기서, γ_{AB_j} 는 $j = 0, \dots, 2^n-1$ 에 대해 $\gamma_{AB_0B_1\cdots B_{2^n-1}}$ 의 감소된 상태이다. 상태 $\gamma_{AB_0B_1\cdots B_{2^n-1}}$ 는 분리가능하고 이에 대해 수학식 22이 성립한다.

수학식 22

$$T_q^a(\gamma_{AB_0B_1\cdots B_{2^n-1}}) = T_q^a(\rho_{AB_0B_1\cdots B_{N-1}})$$

[0102]

[0103] 이는 $j = N, \dots, 2^n-1$ 에 대해 $T_q^a(\gamma_{A|B_j}) = 0$ 임을 의미한다. 따라서, $j = 0, \dots, N-1$ 에 대해 $\gamma_{AB_j} = \rho_{AB_j}$ 이기 때문에, 수학식 23이 성립한다.

수학식 23

$$\begin{aligned} (T_q^a(\rho_{AB_0B_1\cdots B_{N-1}}))^\beta &= (T_q^a(\gamma_{AB_0B_1\cdots B_{2^n-1}}))^\beta \\ &\leq \sum_{j=0}^{2^n-1} (2^\beta - 1)^{\omega(j)} (T_q^a(\gamma_{A|B_j}))^\beta \\ &= \sum_{j=0}^{N-1} (2^\beta - 1)^{\omega(j)} (T_q^a(\rho_{A|B_j}))^\beta, \end{aligned}$$

[0104]

[0105] 정보의 얽힘은 q 가 1에 근접함에 따라 Tsallis- q 엔트로피의 특수한 경우이다. 본 발명에서는 von Neumann 엔트로피를 얻을 수 있고, von Neumann 엔트로피에 대한 서브-가산성 조건이 항상 참이다. 이후, 수학식 9의 결과가 수학식 24와 같이 보조 얽힘의 형태로 변환된다.

수학식 24

$$\begin{aligned} (E^a(\rho_{A|B_0B_1\cdots B_{N-1}}))^\beta &\leq \sum_{j=0}^{N-1} (2^\beta - 1)^{\omega(j)} (E^a(\rho_{A|B_j}))^\beta \\ &\leq \sum_{j=0}^{N-1} \beta^{\omega(j)} (E^a(\rho_{A|B_j}))^\beta \\ &\leq \sum_{j=0}^{N-1} (E^a(\rho_{A|B_j}))^\beta, \end{aligned}$$

[0106]

[0107] 여기서, 첫번째 부등식은 수학식 9에서 $q = 1$ 로 설정하여 획득되고, 두번째 부등식은 도 1에서 제시된 관계로부

터 획득된다. 한편, 세번째 부등식은 폴리가미 관계로부터 획득된다.

[0108] 이상에서는, 본 발명에 따른 새로운 부등식 관계를 갖는 서브시스템의 바이너리 벡터 타입 분포의 해밍 가중치에 기반하는 더 긴밀한 폴리가미 관계가 제공된다. 본 발명에 따른 결과는 고차원 큐빗 시스템에 대한 von Neumann 엔트로피의 일반화를 제공한다. 또한, 본 결과는 얽힘 형태의 관계보다 더 긴밀한 특성을 갖는다. 폴리가미 관계의 긴밀성은 보조 얽힘 분포의 더 세밀한 특성을 반영한다.

[0109] 전술한 내용에 기반하여, 도 2를 참조하여 다자간 양자얽힘 분석 방법을 수행하는 양자 시스템의 상세한 동작에 대해 살펴보면 다음과 같다.

[0110] 이와 관련하여, 제어부(110, 210)는 서브 시스템의 바이너리 벡터 타입의 해밍 가중치($\omega(j)$)에 기반하여

$$(T_q^a(\rho_{A|B_0B_1\cdots B_{N-1}}))^{\beta} \leq \sum_{j=0}^{N-1} (2^{\beta} - 1)^{\omega(j)} (T_q^a(\rho_{A|B_j}))^{\beta}$$

로 상한을 설정할 수 있다. 이와

관련하여, 구체적인 내용은 수학적 9에 따른다.

[0111] 또한, 제어부(110, 210)는 상기 서브 시스템의 엔트로피를 상기 해밍 가중치에 기반하여 합산한 상기 상한에 기반하여, 상기 다분 시스템을 상기 서브 시스템으로 분해할 수 있다. 이와 관련하여, 상기 상한 값에 기반하여 상기 다분 시스템의 서브 시스템 간에 상호 연관 정도가 낮다고 판단되면, 서브 시스템으로의 분해가 가능하다.

[0112] 또한, 제어부(110, 210)는 $(2^n + 1)$ 개의 양자 상태(quantum state)를 갖는 상기 다분 시스템이

$$T_q^a(\gamma_{AB_0B_1\cdots B_{2^n-1}}) = T_q^a(\rho_{AB_0B_1\cdots B_{N-1}})$$

를 만족하여 N개의 양자 상태를 갖

는 제1 서브 시스템으로 분해 가능한지 여부를 판단할 수 있다. 구체적으로, 상기 제1 서브 시스템으로 분해 가능하면, 상기 다분 시스템의 상한을 수학적 23에 의해 상기 제1 서브 시스템의 상한을 이용하여 설정할 수 있다. 즉, $(2^n + 1)$ 개의 양자 상태를 갖는 다분 시스템을 N개의 양자 상태를 갖는 제1 서브 시스템으로 분해한 다음, 제1 서브 시스템에 대한 상한 값에 기반하여 제1 서브 시스템 내의 복수의 제2 서브 시스템 간에 상호 연관 정도가 낮다고 판단되면, 제2 서브 시스템으로의 분해가 가능하다. 이러한 방식으로, $(2^n + 1)$ -다분 시스템을 N분 시스템으로 단순화한 이후에, 이를 다시 2분 시스템으로까지 분해 가능하다.

[0113] 또한, 제어부(110, 210)는 상기 제1 서브 시스템으로 분해 가능하면, 상기 제1 서브 시스템에 속하는 양자 기기로 양자 엔트로피 상태 정보를 피드백하도록 제어할 수 있다. 이때, 제1 서브 시스템에 속하지 않는 양자 기기에 대해서는 엔트로피 상태 정보를 피드백하지 않아 시그널링을 단순화할 수 있다. 또한, 제어부(110, 210)는 상기 제1 서브 시스템으로 분해 가능하고, 상기 제1 서브 시스템의 상한이 임계치 이하이면, 상기 제1 서브 시스템을 이분 양자 시스템으로 분해할 수 있다.

[0114] 양자 엔트로피 상태가 아닌 서브 시스템과 연관된 얽힘(entanglement)의 합을 이용하는 다른 실시예에 따르면, 제어부(110, 210)는 다음과 같은 동작을 수행할 수 있다. 이와 관련하여, 제어부(110, 210)는 상기 서브 시스템의 바이너리 벡터 타입의 해밍 가중치($\omega(j)$)에 기반하여 상기 상한을

$$(E^a(\rho_{A|B_0B_1\cdots B_{N-1}}))^{\beta} \leq \sum_{j=0}^{N-1} (2^{\beta} - 1)^{\omega(j)} (E^a(\rho_{A|B_j}))^{\beta}$$

로 설정할 수 있다.

[0115] 한편, 제어부(110, 210)는 상기 서브 시스템의 얽힘을 상기 해밍 가중치에 기반하여 합산한 상기 상한에 기반하여, 상기 다분 시스템을 상기 서브 시스템으로 분해할 수 있다.

[0116] 또한, 제어부(110, 210)는 $(2^n + 1)$ 개의 양자 상태(quantum state)를 갖는 상기 다분 시스템이 N개의 양자 상태를 갖는 제1 서브 시스템으로 분해 가능한지 여부를 판단할 수 있다. 이때, 상기 제1 서브 시스템으로 분해 가능하면, 상기 다분 시스템과 연관된 얽힘의 상한을 수학적 24에 의해 상기 제1 서브 시스템과 연관된 얽힘의 상한을 이용하여 설정할 수 있다.

[0117] 또한, 제어부(110, 210)는 상기 제1 서브 시스템으로 분해 가능하면, 상기 제1 서브 시스템에 속하는 양자 기기로 양자 엔트로피 상태 정보를 피드백하도록 제어할 수 있다. 또한, 상기 제1 서브 시스템으로 분해 가능하고, 상기 제1 서브 시스템의 상한이 임계치 이하이면, 상기 제1 서브 시스템을 이분 양자 시스템으로 분해할 수 있다.

다.

[0118] 이상에서는 본 발명에 따른 다자간 양자얽힘 분석 방법을 수행하는 양자 시스템에 대해 살펴보았다. 이하에서는, 본 발명에 따른 다자간 양자얽힘 분석 방법의 알고리즘에 대해 살펴보면 다음과 같다. 이와 관련하여, 도 4는 본 발명의 일 실시예에 따른 엔트로피 기반 다자간 양자얽힘 분석 방법의 흐름도를 나타낸다. 반면에, 도 5는 본 발명의 다른 실시예에 따른 양자얽힘 기반 다자간 양자얽힘 분석 방법의 흐름도를 나타낸다.

[0119] 도 4를 참조하면, 다자간 양자얽힘 분석 방법은 서브-가산성 판단 단계(S110), 엔트로피 상한 설정 단계(S120) 및 다분 시스템 분해 단계(S130)를 포함한다. 서브-가산성 판단 단계(S110)에서, 다분 양자 시스템의 서브 시스템 간에 서브-가산성(subadditivity) 만족 여부를 판단한다. 또한, 엔트로피 상한 설정 단계(S120)에서, 서브-가산성이 만족되면, 상기 서브 시스템의 엔트로피의 합을 이용하여 상기 다분 양자 시스템의 엔트로피의 상한을 설정한다. 또한, 다분 시스템 분해 단계(S130)에서, 상기 서브 시스템의 엔트로피를 상기 해밍 가중치에 기반하여 합산한 상기 상한에 기반하여, 상기 다분 시스템을 상기 서브 시스템으로 분해한다.

[0120] 전술한 엔트로피 상한 설정 단계(S120)에서, 상기 서브 시스템의 바이너리 벡터 타입의 해밍 가중치($\omega(j)$)에

$$(T_q^a(\rho_{A|B_0B_1\cdots B_{N-1}}))^{\beta} \leq \sum_{j=0}^{N-1} (2^{\beta} - 1)^{\omega(j)} (T_q^a(\rho_{A|B_j}))^{\beta}$$

기반하여 상기 상한을
정할 수 있다.

로 설

[0121] 전술한 다분 시스템 분해 단계(S130)에서, $(2^n + 1)$ 개의 양자 상태를 갖는 상기 다분 시스템이

$$T_q^a(\gamma_{AB_0B_1\cdots B_{2^n-1}}) = T_q^a(\rho_{AB_0B_1\cdots B_{N-1}})$$

를 만족하여 N개의 양자 상태를 갖는 제1 서브 시스템으로 분해 가능한지 여부를 판단할 수 있다. 이때, 상기 제1 서브 시스템으로 분해 가능하면, 상기 다분 시스템의 상한을 수학적 23의 상한을 이용하여 설정할 수 있다.

[0122] 한편, 다분 시스템 분해 단계(S130)에서, 상기 제1 서브 시스템으로 분해 가능하면, 상기 제1 서브 시스템에 속하는 양자 기기로 양자 엔트로피 상태 정보를 피드백할 수 있다. 또한, 상기 제1 서브 시스템으로 분해 가능하고, 상기 제1 서브 시스템의 상한이 임계치 이하이면, 상기 제1 서브 시스템을 이분 양자 시스템으로 분해할 수 있다.

[0123] 한편, 도 5를 참조하면, 다자간 양자얽힘 분석 방법은 서브-가산성 판단 단계(S210), 얽힘 상한 설정 단계(S220) 및 다분 시스템 분해 단계(S230)를 포함한다. 서브-가산성 판단 단계(S210)에서, 다분 양자 시스템의 서브 시스템 간에 서브-가산성(subadditivity) 만족 여부를 판단한다. 또한, 얽힘 상한 설정 단계(S220)에서, 상기 서브-가산성이 만족되면, 상기 서브 시스템과 연관된 얽힘(entanglement)의 합을 이용하여 상기 다분 양자 시스템의 얽힘의 상한을 설정한다. 또한, 다분 시스템 분해 단계(S230)에서, 상기 서브 시스템의 얽힘을 상기 해밍 가중치에 기반하여 합산한 상기 상한에 기반하여, 상기 다분 시스템을 상기 서브 시스템으로 분해할 수 있다.

[0124] 전술한 상기 얽힘 상한 설정 단계(S220)에서, 상기 서브 시스템의 바이너리 벡터 타입의 해밍 가중치($\omega(j)$)에

$$(E^a(\rho_{A|B_0B_1\cdots B_{N-1}}))^{\beta} \leq \sum_{j=0}^{N-1} (2^{\beta} - 1)^{\omega(j)} (E^a(\rho_{A|B_j}))^{\beta}$$

기반하여 상기 상한을
수 있다.

로 설정할

[0125] 전술한 상기 다분 시스템 분해 과정(S230)에서, $(2^n + 1)$ 개의 양자 상태(quantum state)를 갖는 상기 다분 시스템이 N개의 양자 상태를 갖는 제1 서브 시스템으로 분해 가능한지 여부를 판단할 수 있다. 이때, 상기 제1 서브 시스템으로 분해 가능하면, 상기 다분 시스템과 연관된 얽힘의 상한을 수학적 24에 의해 상기 제1 서브 시스템과 연관된 얽힘의 상한을 이용하여 설정할 수 있다.

[0126] 전술한 상기 다분 시스템 분해 과정(S230)에서, 상기 제1 서브 시스템으로 분해 가능하면, 상기 제1 서브 시스템에 속하는 양자 기기로 양자 얽힘 상태 정보를 피드백할 수 있다. 또한, 상기 제1 서브 시스템으로 분해 가능하고, 상기 제1 서브 시스템과 연관된 얽힘의 상한이 임계치 이하이면, 상기 제1 서브 시스템을 이분 양자 시스템으로 분해할 수 있다.

템으로 분해할 수 있다.

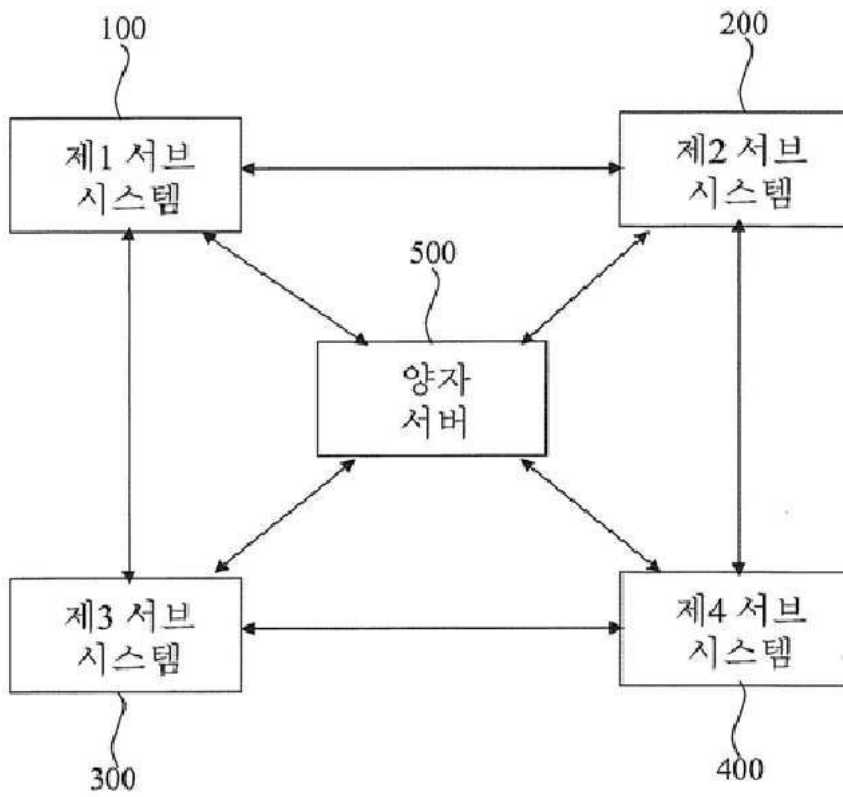
- [0127] 이상에서는 본 발명에 따른 다자간 양자 얽힘 분석방법 및 이를 이용하는 양자시스템에 대해 살펴보았고, 이의 기술적 효과는 다음과 같다.
- [0128] 본 발명의 적어도 일 실시예에 따르면, 새로운 부등식 관계를 갖는 서브시스템의 바이너리 벡터 타입 분포의 해밍 가중치에 기반하는 더 긴밀한 관계를 갖는 다자간 양자 얽힘 분석 방법을 제공할 수 있다는 장점이 있다.
- [0129] 또한, 본 발명의 적어도 일 실시예에 따르면, 고차원 큐딧 시스템에 대한 von Neumann 엔트로피의 일반화를 제공할 수 있다는 장점이 있다.
- [0130] 또한, 본 발명의 적어도 일 실시예에 따르면, 얽힘 형태의 관계보다 더 긴밀한 특성을 갖는다. 폴리가미 관계의 긴밀성은 보조 얽힘 분포의 더 세밀한 특성을 반영할 수 있다는 장점이 있다.
- [0131] 본 발명의 활용분야와 관련하여, 폴리가미 관계의 긴밀성은 보조 얽힘 분포의 더 세밀한 특성을 반영하여 다자간 양자얽힘분석방법 및 이를 이용하는 양자시스템에 활용할 수 있다는 것이다.
- [0132] 또한, 본 발명의 기대효과와 관련하여, 다차원 큐딧 시스템에 대한 Tsallis-q 엔트로피의 폴리가미 부등식이 기존에 제시된 관계식보다 더 긴밀성을 제공하여, 다자간 양자 얽힘 분석방법 및 이를 이용하는 양자 시스템에 활용할 수 있다는 것이다.
- [0133] 또한, 본 발명의 기술의 사업화 전망과 관련하여, 양자 시스템의 폴리가미 관계는 다자간 통신에서 각 대상 간의 얽힘을 분배하는 방법을 제공하며, 이는 다자간 양자 얽힘 분석방법 및 이를 이용하는 양자 시스템의 사업화를 위해 필요하다는 것이다.
- [0134] 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

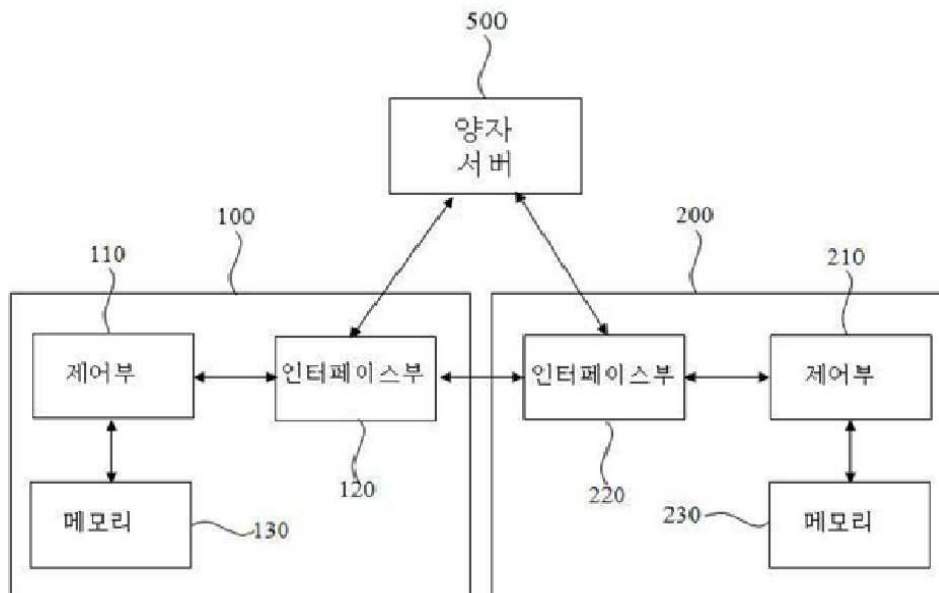
- [0135] 00: 제1 서브 시스템 200: 제2 서브 시스템
- 500: 양자 서버
- 110, 210: 제어부 120, 220: 인터페이스부
- 130, 230: 메모리

도면

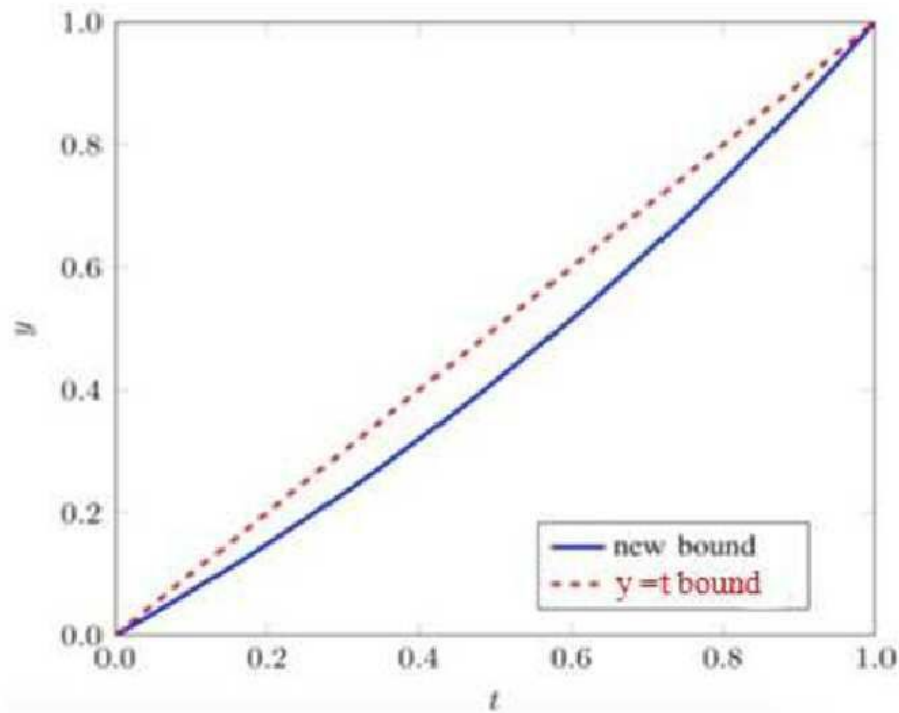
도면1



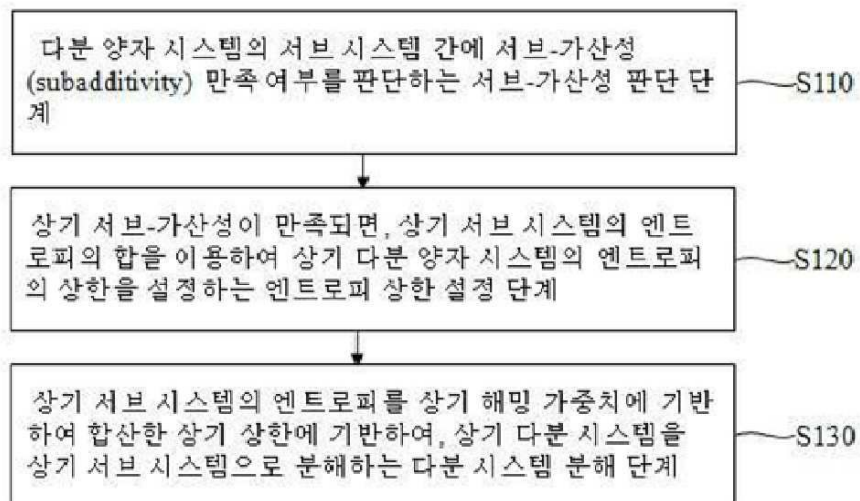
도면2



도면3



도면4



도면5

