(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2017 년 12 월 21 일 (21.12.2017)

WIPO | PCT

(10) 국제공개번호
WO 2017/217577 A1

(51) 국제특허분류:
H03M 13/29 (2006.01) *G06N 99/00* (2010.01)
H03M 13/11 (2006.01)

(21) 국제출원번호: PCT/KR2016/006809

(22) 국제출원일: 2016 년 6 월 24 일 (24.06.2016)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2016-0073350 2016 년 6 월 13 일 (13.06.2016) KR

(71) 출원인: 고려대학교 산학협력단 (KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION) [KR/KR]; 02841 서울시 성북구 안암로 145, Seoul (KR).

(72) 발명자: 허준 (HEO, Jun); 06359 서울시 강남구 광평로10길 6, 206동 103호, Seoul (KR). 손일권 (SOHN, Il Kwon); 08208 서울시 구로구 경인로65길 16-15, 1105동 2001호, Seoul (KR).

(74) 대리인: 심경식 등 (SHIM, Kyoung-Shik et al.); 06719 서울시 서초구 반포대로 10, 신원빌딩 4층 (서초동), Seoul (KR).

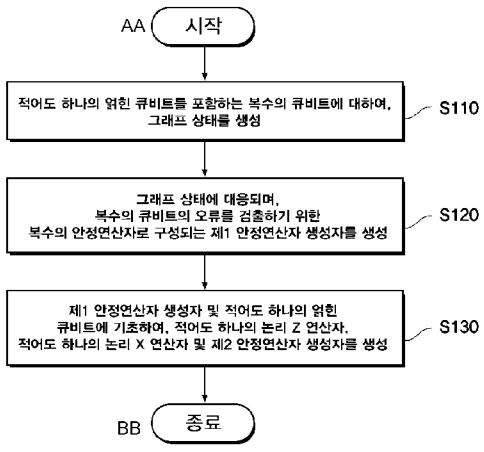
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

WO 2017/217577 A1

(54) **Title:** METHOD AND APPARATUS FOR GENERATING QUANTUM ERROR CORRECTION CODE USING GRAPH STATE

(54) **발명의 명칭:** 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법 및 장치

[도1]



S110 ... Generate graph state for plurality of qubits including at least one entangled qubit
S120 ... Generate first stabilizer generator which corresponds to graph state and comprises plurality of stabilizers for detecting errors of plurality of qubits
S130 ... Generate at least one logical Z operator, at least one logical X operator and second stabilizer generator, on basis of first stabilizer generator and at least one entangled qubit
AA ... Start
BB ... End

(57) **Abstract:** Provided is a method for generating a quantum error correction code by using a graph state. The method for generating a quantum error correction code by using a graph state, according to one embodiment of the present invention, comprises the steps of: for a plurality of qubits including at least one entangled qubit (ebit), generating the graph state indicating an adjacency relation among the qubits; generating a first stabilizer generator which corresponds to the graph state and comprises a plurality of stabilizers for detecting errors of the plurality of qubits; and generating at least one logical Z operator used for a phase-flip operation of a codeword, at least one logical X operator used for a bit-flip operation of the codeword, and a second stabilizer generator that is a subset of the first stabilizer generator, on the basis of the first stabilizer generator and the at least one entangled qubit.

[다음 쪽 계속]

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

(57) 요약서: 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법을 제공한다. 본 발명의 일 실시예에 따른 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법 은 적어도 하나의 얽힌 큐비트(entangled qubit: ebit)를 포함하는 복수의 큐비트에 대하여, 각 큐비트 간의 인접 관계를 나타내는 그래프 상태(graph state)를 생성하는 단계; 상기 그래프 상태에 대응되며, 상기 복수의 큐비트의 오류를 검출하기 위한 복수의 안정연산자로 구성되는 제1 안정연산자 생성자(stabilizer generator)를 생성하는 단계; 및 상기 제1 안정연산자 생성자 및 상기 적어도 하나의 얽힌 큐비트에 기초하여, 코드워드의 위상플립연산에 이용되는 적어도 하나의 논리 Z 연산자, 코드워드의 비트플립연산에 이용되는 적어도 하나의 논리 X 연산자 및 상기 제1 안정연산자 생성자의 부분집합인 제2 안정연산자 생성자를 생성하는 단계를 포함한다.

명세서

발명의 명칭: 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법 및 장치

기술분야

[1] 본 발명은 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법 및 장치에 관한 것으로, 보다 구체적으로는, 그래프 상태에 얽힌 양자가 포함됨으로써 차원이 확장된 오류 정정 부호를 생성하는 방법 및 장치에 관한 것이다.

배경기술

[2] 양자 정보 통신(quantum information communication technology)은 20세기 말에 등장한 새로운 기술로 양자물리학의 원리에 입각하여 정보를 저장, 전송 및 처리하는 과정에 관한 기술로, 양자물리학과 정보통신기술이 융합되어 형성되었다.

[3] 양자 오류 정정 부호(quantum error correction code)는 고전 이진 정보(binary information)와는 달리 외부 환경의 간섭에 매우 취약하며 스스로 붕괴하는 특징을 가진 양자 정보(quantum information)를 보호하기 위해 도입되어, 사용되고 있다.

[4] 송신단 및 수신단에서 공유되는 얽힌 양자(entangled quantum)를 이용할 경우, 오류 정정 부호의 차원을 확장할 수 있거나 최소 거리(minimum distance)를 증가시킬 수 있다는 장점은 기존의 연구를 통해서 이미 알려져 있지만, 그 방법이 매우 복잡하다.

[5] 따라서, 그래프 상태(graph state)에 얽힌 양자를 추가하고, 안정연산자 생성자(stabilizer generator)를 선택하여 사용함으로써, 부호의 차원을 용이하게 확장할 수 있는 양자 오류 정정 부호의 생성 방법 및 장치를 제안하고자 한다.

발명의 상세한 설명

기술적 과제

[6] 본 발명은 그래프 상태에 얽힌 양자를 추가하여 양자 오류 정정 부호를 생성함으로써, 양자 오류 정정 부호의 차원을 용이하게 확장하는 방법을 제공하고자 한다.

과제 해결 수단

[7] 상기 목적을 달성하기 위해, 본 발명에서 제공하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법은 적어도 하나의 얽힌 큐비트(entangled qubit: ebit)를 포함하는 복수의 큐비트에 대하여, 각 큐비트 간의 인접 관계를 나타내는 그래프 상태(graph state)를 생성하는 단계; 상기 그래프 상태에 대응되며, 상기 복수의 큐비트의 오류를 검출하기 위한 복수의 안정연산자로 구성되는 제1 안정연산자 생성자(stabilizer generator)를 생성하는 단계; 및 상기 제1 안정연산자 생성자 및 상기 적어도 하나의 얽힌 큐비트에 기초하여, 코드워드의 위상플립연산에

이용되는 적어도 하나의 논리 Z 연산자, 코드워드의 비트플립연산에 이용되는 적어도 하나의 논리 X 연산자 및 상기 제1 안정연산자 생성자의 부분집합인 제2 안정연산자 생성자를 생성하는 단계를 포함한다.

[8] 바람직하게는, 상기 제2 안정연산자 생성자를 생성하는 단계는 상기 적어도 하나의 얽힌 큐비트에 기초하여, 상기 제1 안정연산자 생성자를 구성하는 상기 복수의 안정연산자 중 적어도 하나를 상기 적어도 하나의 논리 Z 연산자로 결정하고, 나머지로 상기 제2 안정연산자 생성자를 생성하는 단계; 및 상기 적어도 하나의 논리 Z 연산자 및 상기 제2 안정연산자 생성자를 이용하여 상기 적어도 하나의 논리 X 연산자를 생성하는 단계를 포함할 수 있다.

[9] 바람직하게는, 상기 나머지로 제2 안정연산자 생성자를 생성하는 단계는 상기 제1 안정연산자 생성자를 구성하는 상기 복수의 안정연산자 중에서, 상기 적어도 하나의 얽힌 큐비트에 대응되는 위치에 비트플립연산에 이용되는 X 연산자를 포함하는 적어도 하나를 상기 적어도 하나의 논리 Z 연산자로 결정하는 단계; 및 상기 적어도 하나의 논리 Z 연산자를 제외한 나머지로 구성되는 상기 제2 안정연산자 생성자를 생성하는 단계를 포함할 수 있다.

[10] 바람직하게는, 상기 적어도 하나의 논리 X 연산자를 생성하는 단계는 상기 적어도 하나의 논리 Z 연산자에 포함된 상기 X 연산자를 큐비트의 위상플립연산에 이용되는 Z 연산자로 대체한 적어도 하나의 후보연산자를 생성하는 단계; 및 상기 제2 안정연산자 생성자 중 상기 적어도 하나의 후보연산자와 동일한 위치에 상기 Z 연산자를 포함하는 안정연산자 및 상기 적어도 하나의 후보연산자를 이용하여 상기 적어도 하나의 논리 X 연산자를 생성하는 단계를 포함할 수 있다.

[11] 바람직하게는, 상기 적어도 하나의 논리 X 연산자는 수학식 1에 의해 산출될 수 있다.

[12] [수학식 1]

[13]

$$\overline{X} = X_j Z^{r_i} \,|\, I \quad \text{for } i = 1,\ldots,k(k=c)$$

[14] 여기서, $\overline{X}$는 상기 적어도 하나의 논리 X 연산자이고, X는 상기 X 연산자이고, Z는 상기 Z 연산자이고, I는 항등 연산자이고, i는 상기 얽힌 큐비트의 인덱스이고, r_i는 상기 그래프 상태에 대응되는 인접행렬(adjacency matrix)에서 상기 얽힌 큐비트에 대응되는 i번째 행이고, k와 c는 상기 얽힌 큐비트의 개수이고, n이 상기 복수의 큐비트 중 논리적 큐비트의 개수일 때 j는 i+(n-c)로 정의되는 값이다.

[15] 바람직하게는, 상기 제1 안정연산자 생성자를 생성하는 단계는 상기 그래프

상태에 기초하여, 상기 복수의 큐비트 상호 간의 인접 여부를 나타내는 인접행렬을 생성하는 단계; 파울리 연산자로 구성되며, 상기 인접행렬의 각 행에 대응되는 복수의 안정연산자를 산출하는 단계; 및 상기 산출된 복수의 안정연산자를 포함하는 상기 제1 안정연산자 생성자를 생성하는 단계를 포함할 수 있다.

[16] 바람직하게는, 상기 제1 안정연산자 생성자는 수학식 2에 의해 산출될 수 있다.

[17] [수학식 2]

[18]

$$S = \begin{cases} X_i Z^{r_i} | I \quad (i=1,\ldots,n-c) \\ X_i Z^{r_i} | Z_j \quad (i=n-c+1,\ldots,n) \\ Z_i | X_j \quad (i=n-c+1,\ldots,n) \end{cases}$$

[19] 여기서, S는 상기 제1 안정연산자 생성자이고, X는 큐비트의 비트플립연산에 이용되는 연산자이고, Z는 큐비트의 위상플립연산에 이용되는 연산자이고, I는 큐비트의 항등 연산자이고, n은 상기 복수의 큐비트 중 논리적 큐비트의 개수이고, c는 상기 얽힌 큐비트의 개수이고, j는 i-(n-c)로 정의되는 값이고, r_i는 상기 인접행렬의 i번째 행이다.

[20] 바람직하게는, 상기 적어도 하나의 논리 X 연산자, 상기 적어도 하나의 논리 Z 연산자 및 상기 제2 안정연산자 생성자를 이용하여, 상기 적어도 하나의 얽힌 큐비트를 포함하는 복수의 큐비트에 대응되는 양자 오류 정정 부호를 생성하는 단계를 더 포함할 수 있다.

[21] 또한, 상기 목적을 달성하기 위해, 본 발명에서 제공하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 장치는 적어도 하나의 얽힌 큐비트를 포함하는 복수의 큐비트에 대하여, 각 큐비트 간의 인접 관계를 나타내는 그래프 상태를 생성하는 그래프부; 상기 그래프 상태에 대응되며, 상기 복수의 큐비트의 오류를 검출하기 위한 복수의 안정연산자로 구성되는 제1 안정연산자 생성자를 생성하는 제1 생성자부; 및 상기 제1 안정연산자 생성자 및 상기 적어도 하나의 얽힌 큐비트에 기초하여, 코드워드의 위상플립연산에 이용되는 적어도 하나의 논리 Z 연산자, 코드워드의 비트플립연산에 이용되는 적어도 하나의 논리 X 연산자 및 상기 제1 안정연산자 생성자의 부분집합인 제2 안정연산자 생성자를 생성하는 제2 생성자부를 포함한다.

[22] 바람직하게는, 상기 제2 생성자부는 상기 적어도 하나의 얽힌 큐비트에 기초하여, 상기 제1 안정연산자 생성자를 구성하는 상기 복수의 안정연산자 중 적어도 하나를 상기 적어도 하나의 논리 Z 연산자로 결정하고, 나머지로 상기

제2 안정연산자 생성자를 생성하고, 상기 적어도 하나의 논리 Z 연산자 및 상기 제2 안정연산자 생성자를 이용하여 상기 적어도 하나의 논리 X 연산자를 생성할 수 있다.

[23] 바람직하게는, 상기 제2 생성자부는 상기 제1 안정연산자 생성자를 구성하는 상기 복수의 안정연산자 중에서, 상기 적어도 하나의 얽힌 큐비트에 대응되는 위치에 비트플립연산에 이용되는 X 연산자를 포함하는 적어도 하나를 상기 적어도 하나의 논리 Z 연산자로 결정하고, 상기 적어도 하나의 논리 Z 연산자를 제외한 나머지로 구성되는 상기 제2 안정연산자 생성자를 생성할 수 있다.

[24] 바람직하게는, 상기 제2 생성자부는 상기 적어도 하나의 논리 Z 연산자에 포함된 상기 X 연산자를 큐비트의 위상플립연산에 이용되는 Z 연산자로 대체한 적어도 하나의 후보연산자를 생성하고, 상기 제2 안정연산자 생성자 중 상기 적어도 하나의 후보연산자와 동일한 위치에 상기 Z 연산자를 포함하는 안정연산자 및 상기 적어도 하나의 후보연산자를 이용하여 상기 적어도 하나의 논리 X 연산자를 생성할 수 있다.

[25] 바람직하게는, 상기 제1 생성자부는 상기 그래프 상태에 기초하여, 상기 복수의 큐비트 상호 간의 인접 여부를 나타내는 인접행렬을 생성하고, 파울리 연산자로 구성되며, 상기 인접행렬의 각 행에 대응되는 복수의 안정연산자를 산출하고, 상기 산출된 복수의 안정연산자를 포함하는 상기 제1 안정연산자 생성자를 생성할 수 있다.

[26] 바람직하게는, 상기 제1 안정연산자 생성자는 수학식 3에 의해 산출될 수 있다.

[27] [수학식 3]

[28]

$$S = \begin{cases} X_i Z^{r_i} | I \quad (i=1,\ldots,n-c) \\ X_i Z^{r_i} | Z_j \quad (i=n-c+1,\ldots,n) \\ Z_i | X_j \quad (i=n-c+1,\ldots,n) \end{cases}$$

[29] 여기서, S는 상기 제1 안정연산자 생성자이고, X는 큐비트의 비트플립연산에 이용되는 연산자이고, Z는 큐비트의 위상플립연산에 이용되는 연산자이고, I는 큐비트의 항등 연산자이고, n은 상기 복수의 큐비트 중 논리적 큐비트의 개수이고, c는 상기 얽힌 큐비트의 개수이고, j는 i-(n-c)로 정의되는 값이고, r_i는 상기 인접행렬의 i번째 행이다.

[30] 바람직하게는, 상기 적어도 하나의 논리 X 연산자, 상기 적어도 하나의 논리 Z 연산자 및 상기 제2 안정연산자 생성자를 이용하여, 상기 적어도 하나의 얽힌 큐비트를 포함하는 복수의 큐비트에 대응되는 양자 오류 정정 부호를 생성하는

ECC생성부를 더 포함할 수 있다.

발명의 효과

[31] 본 발명은 얽힌 양자가 적용된 그래프 상태에 대응되는 양자 오류 정정 부호를 생성함으로써, 그 얽힌 양자의 추가만으로 용이하게 양자 오류 정정 부호의 차원을 확장할 수 있는 효과가 있다.

[32] 또한, 본 발명은 양자 바운드(bound)를 만족하는 양자 오류 정정 부호를 생성할 수 있는 효과가 있다.

도면의 간단한 설명

[33] 도 1은 본 발명의 일 실시예에 따른 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법을 도시하기 위한 흐름도이다.

[34] 도 2는 본 발명의 일 실시예에 따른 제1 안정연산자 생성자의 생성 방법을 도시하기 위한 흐름도이다.

[35] 도 3은 본 발명의 일 실시예에 따른 그래프 상태를 이용한 양자 오류 정정 부호의 생성 장치를 도시하기 위한 도면이다.

[36] 도 4는 본 발명의 일 실시에에 따른 그래프 상태를 설명하기 위하여 도시하기 위한 도면이다.

[37] 도 5는 본 발명의 일 실시에에 따른 인접행렬을 설명하기 위하여 도시하기 위한 도면이다.

[38] 도 6은 본 발명의 다른 실시에에 따른 그래프 상태를 설명하기 위하여 도시하기 위한 도면이다.

[39] 도 7은 본 발명의 다른 실시에에 따른 인접행렬을 설명하기 위하여 도시하기 위한 도면이다.

[40] 도 8은 본 발명의 일 실시에에 따른 n=12 및 k=6일 때의 양자 바운드(quantum bound)를 설명하기 위하여 도시하기 위한 도면이다.

발명의 실시를 위한 형태

[41] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[42] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 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.

[43] 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.

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

[45] 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 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[46] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[47] 도 1은 본 발명의 일 실시예에 따른 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법을 도시하기 위한 흐름도이다.

[48] 단계 S110에서는, 양자 오류 정정 부호 생성 장치가 적어도 하나의 얽힌 큐비트(entangled qubit: ebit)를 포함하는 복수의 큐비트에 대하여, 각 큐비트 간의 인접 관계를 나타내는 그래프 상태(graph state)를 생성한다.

[49] 큐비트는 양자 정보의 단위로, 기존의 디지털 정보의 단위인 비트(bit)를 대신하여 사용된다. 또한, 큐비트는 서로 구별되는 두 양자상태의 선형 중첩으로 나타낼 수 있다. 즉, 큐비트는 0 또는 1의 값을 가질 수 있을 뿐만 아니라, 0과 1의 값을 동시에 가질 수도 있는 것이다.

[50] 얽힌 큐비트는 다른 양자와 얽힌 양자(entangled quantum)에 대응되는 큐비트를 의미하며, 얽혀있는 2개의 큐비트의 값은 어느 하나의 큐비트의 값에 의해 다른 하나의 큐비트의 값이 결정될 수 있다.

[51] 그래프 상태는 복수의 큐비트의 상태를 그래프에 의해 나타내는 방법이다. 즉, 각 큐비트는 그래프에서 꼭지점에 해당하고, 모든 상호작용하는 큐비트의 쌍 간에는 선이 연결될 수 있다. 도 4 및 도 6을 참조하면, 각각 큐비트 6개 및 7개에 대한 그래프 상태가 나타나 있다. 또한, 도 4 및 도 6은 각각 1개(6번 큐비트) 및

2개의 얽힌 큐비트(6번 및 7번 큐비트)를 포함하고 있다.

[52] 이때, 도 4를 참조하면, 총 물리적인 큐비트의 개수는 6개이고, 논리적인 큐비트의 개수는 5개이며, 얽힌 큐비트의 개수는 1개이다. 또한, 도 6를 참조하면, 총 물리적인 큐비트의 개수는 7개이고, 논리적인 큐비트의 개수는 5개이며, 얽힌 큐비트의 개수는 2개이다.

[53] 단계 S120에서는, 양자 오류 정정 부호 생성 장치가 그 그래프 상태에 대응되며, 그 복수의 큐비트의 오류를 검출하기 위한 복수의 안정연산자로 구성되는 제1 안정연산자 생성자(stabilizer generator)를 생성한다.

[54] 복수의 안정연산자(stabilizer)는 복수의 파울리 연산자(2x2의 행렬)로 구성될 수 있다. 이때, 파울리 연산자는 수학식 1에서와 같이, 항등 연산자인 I 연산자, 비트 플립 연산자인 X 연산자, 비트 및 위상 플립 연산자인 Y 연산자 및 위상 플립 연산자인 Z 연산자 중 하나일 수 있다.

[55] [수학식 1]

[56]

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ Y = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix},\ Z = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

[57] 일반적으로, 복수의 큐비트에 대응되는 그래프 상태의 안정연산자는 아래의 수학식 2에 의해 산출될 수 있다.

[58] [수학식 2]

[59]

$$S_i = X_i Z^{r_i} \quad \text{for} \quad i = 1, \ldots, n$$

[60] 여기서, S_i는 i번째 안정연산자이고, X는 X 연산자이고, Z는 Z 연산자이고, r_i는 그래프 상태에 대응되는 인접행렬(adjacency matrix)의 i번째 행의 값이고, n은 논리 큐비트의 개수이다.

[61] 이때, 안정연산자는 편의를 위해 간략하게 표현되었으며, 연산자의 아래 첨자는 그 연산자의 위치를 의미할 수 있다. 즉, $X_i Z^{r_i}$는 i번째 큐비트에 대응되는 위치에 X 연산자가 존재하고, 그 이외의 위치에는 인접행렬의 대응되는 행 및 열의 값을 이용하여 1일 경우 Z가, 0일 경우 I가 존재하는 것으로 나타낼 수 있다. 예를 들어, i=2이고, r_i={10100}일 때, 안정연산자는 ZXZII일 수 있다.

[62] 그러나, 얽힌 큐비트를 포함하고 있는 그래프 상태의 안정연산자는 아래의 수학식 3에 의해 산출될 수 있다.

[63] [수학식 3]

[64]

$$S = \begin{cases} X_i Z^{r_i} | I \quad (i=1,\ldots,n-c) \\ X_i Z^{r_i} | Z_j \quad (i=n-c+1,\ldots,n) \\ Z_i | X_j \quad (i=n-c+1,\ldots,n) \end{cases}$$

[65] 여기서, S_i는 i번째 안정연산자이고, X는 X 연산자이고, Z는 Z 연산자이고, I는 항등 연산자이고, r_i는 그래프 상태에 대응되는 인접행렬(adjacency matrix)의 i번째 행의 값이고, n은 논리적 큐비트의 개수이고, c는 얽힌 큐비트의 개수이고, j는 i-(n-c)로 정의되는 값이다.

[66] 즉, 도 4를 참조하면, n은 5이고, c는 1이므로, 1번 내지 4번 큐비트에 대응되는 안정연산자는 $X_i Z^{r_i} | I$ 이고, 5번 큐비트에 대응되는 안정연산자는 $X_i Z^{r_i} | Z_j$ 이고, 6번 큐비트에 대응되는 안정연산자는 $Z_i | X_j$ 일 수 있다. 이때, 6번 큐비트에 대응되는 안정연산자는 얽힌 큐비트인 6번 큐비트에 대응되는 위치에서의 오류를 검출할 수 있어, 수신단에 할당된 안정연산자가 될 수 있다.

[67] 보다 구체적으로는, 도 4를 참조하면, 도 4에는 총 6개의 큐비트가 나타나 있지만, 6번 큐비트는 5번 큐비트와 얽힌 큐비트로 존재한다. 즉, 논리적 큐비트의 개수인 n은 5이고, 얽힌 큐비트의 개수인 c는 6번 큐비트 하나이므로 1이다. 또한, 도 5를 참조하면, 도 5는 도 4에 나타난 각 큐비트에 대하여 이웃하는 큐비트와의 관계를 나타낸 인접행렬이다. 즉, 도 4의 1번 큐비트는 2번 및 5번 큐비트와 인접하였으므로, 1번 큐비트와 다른 큐비트 간의 관계를 나타내는 인접행렬의 1행은 {0, 1, 0, 0, 1, 0}으로 나타낼 수 있다. 마찬가지 방법으로, 2번 내지 5번 큐비트에 대한 인접행렬의 2행 내지 5행을 나타낼 수 있다.

[68] 따라서, 도 4의 그래프 상태에 대하여, 도 5의 인접행렬 및 수학식 3을 이용하는 경우, 그래프 상태의 안정연산자는 S_1 = XZIIZ|I, S_2 = ZXZII|I, S_3 = IZXZI|I, S_4 = IIZXZ|I, S_5 = ZIIZX|Z, S_6 = IIIIZ|X 로 산출될 수 있다. 이때, | 기호는 얽힌 큐비트인 6번 큐비트의 위치에 대응되는 연산자와 얽히지 않은 일반 큐비트의 위치에 대응되는 연산자를 구분하기 위하여 사용될 수 있다.

[69] 그리고, 양자 오류 정정 부호 생성 장치가 그 생성된 안정연산자를 포함하는 제1 안정연산자 생성자를 생성할 수 있다. 이때, 제1 안정연산자 생성자는 최소한의 안정연산자를 포함하고 있는 안정연산자의 집합으로, 수학식 4와 같이 나타낼 수 있다.

[70] [수학식 4]

[71] $S = \{ S_1, S_2, ..., S_n \}$

[72] 한편, 양자 오류 정정 부호 생성 장치가 그래프 상태의 안정연산자 생성자를 산출하는 이유는 그래프 상태의 안정연산자 생성자가 최대 아벨리안 서브그룹(Maximal Abelian subgroup)을 구성하기 때문이다. 최대 아벨리안 서브그룹은 그룹 내의 원소들이 모두 서로 교환법칙이 성립(commute)하는 관계이며, 그룹 외의 원소와는 교환법칙이 성립하지 않는 그룹일 수 있다.

[73] 단계 S130에서는, 양자 오류 정정 부호 생성 장치가 생성된 제1 안정연산자 생성자 및 적어도 하나의 얽힌 큐비트에 기초하여, 코드워드의 위상플립연산에 이용되는 적어도 하나의 논리 Z 연산자, 코드워드의 비트플립연산에 이용되는 적어도 하나의 논리 X 연산자 및 제1 안정연산자 생성자의 부분집합인 제2 안정연산자 생성자를 생성한다.

[74] 예컨대, 양자 오류 정정 부호 생성 장치가 제1 안정연산자 생성자에 포함된 안정연산자 중에서 적어도 하나의 얽힌 큐비트에 대응되는 안정연산자를 이용하여, 적어도 하나의 논리 Z 연산자, 적어도 하나의 논리 X 연산자 및 제2 안정연산자 생성자를 생성할 수 있다.

[75] 다른 실시예에서는, 양자 오류 정정 부호 생성 장치가 적어도 하나의 얽힌 큐비트를 이용하여, 제1 안정연산자 생성자로부터 적어도 하나의 논리 Z 연산자 및 제2 안정연산자 생성자를 생성하고, 그 생성된 적어도 하나의 논리 Z 연산자 및 제2 안정연산자 생성자를 이용하여 적어도 하나의 논리 X 연산자를 생성할 수 있다.

[76] 즉, 적어도 하나의 논리 Z 연산자는 그 적어도 하나의 얽힌 큐비트에 대응되는 안정연산자일 수 있으며, 제2 안정연산자 생성자는 제1 안정연산자 생성자에서 그 적어도 하나의 얽힌 큐비트에 대응되는 안정연산자를 제외한 나머지를 포함할 수 있다. 또한, 적어도 하나의 논리 X 연산자는 적어도 하나의 논리 Z 연산자 및 제1 안정연산자 생성자로부터 생성될 수 있다.

[77] 한편, 적어도 하나의 논리 Z 연산자, 적어도 하나의 논리 X 연산자 및 제2 안정연산자 생성자를 생성하는 구체적인 방법에 대하여는 아래에서 자세하게 후술한다.

[78] 또 다른 실시예에서는, 양자 오류 정정 부호 생성 장치가 제1 안정연산자 생성자에 포함된 복수의 안정연산자 생성자 중에서 적어도 하나의 얽힌 큐비트에 대응되는 위치에 X 연산자를 포함하는 적어도 하나를 적어도 하나의 논리 Z 연산자로 결정하고, 그 나머지로부터 제2 안정연산자 생성자를 생성할 수 있다.

[79] 즉, 양자 오류 정정 부호 생성 장치가, 양자 오류 정정 부호의 안정연산자 생성자와 적어도 하나의 논리 Z 연산자는 최대 아벨리안 서브그룹을 형성한다는 점을 이용하여, 제1 안정연산자 생성자에 포함되는 안정연산자 중 일부를 적어도 하나의 논리 Z 연산자로 결정하고, 그 나머지로 제2 안정연산자 생성자를 생성할 수 있다.

[80] 보다 구체적으로는, 양자 오류 정정 부호 생성 장치가 제1 안정연산자 생성자에 포함된 복수의 안정연산자 중에서 적어도 하나의 얽힌 큐비트에 대응되는 위치에 X 연산자를 포함하는 적어도 하나의 안정연산자를 적어도 하나의 논리 Z 연산자로 결정할 수 있다. 그리고, 그 나머지 안정연산자로 제2 안정연산자 생성자를 생성할 수 있다.

[81] 이때, 양자 오류 정정 부호 생성 장치가 이와 같이 논리 Z 연산자를 결정하는 것은 얽힌 큐비트의 특징을 이용하기 위한 것일 수 있다. 즉, 수학식 2에 대한 설명을 참조하면, 안정연산자는 각 큐비트에 대응되는 위치에 X 연산자를 포함할 수 있다. 그런데, 얽힌 큐비트가 아닌 큐비트에 대응되는 위치에 X 연산자를 포함하는 안정연산자는, 그 안정연산자가 논리 Z 연산자로 결정되어 변경되었을 때, 그 큐비트에 대응되는 위치에서 발생하는 Z 오류가 검출되지 않을 수 있다. 그러나, 얽힌 큐비트에 대응되는 위치에 X 연산자를 포함하는 경우에, 양자 통신의 수신단에서는 채널을 통과하면서 그 얽힌 큐비트에 대응되는 위치에서 Z 오류가 원천적으로 발생하지 않기 때문에, Z 오류가 검출되지 않는 문제는 발생하지 않는다. 이때, 그 얽힌 큐비트에 대응되는 위치에서 Z 오류가 발생하지 않는 것은, 얽힌 큐비트의 값은 그 큐비트와 얽혀있는 다른 큐비트의 값에 의해 이미 결정되어 있기 때문일 수 있다.

[82] 예컨대, 양자 오류 정정 부호 생성 장치가 제1 안정연산자 생성자 S_1 = {XZIIZII, ZXZIIII, IZXZIII, IIZXZII, ZIIZXIZ, IIIIZIX}에 대하여, 얽힌 큐비트인 6번 큐비트에 대응되는 위치에 X 연산자를 포함하는 IIIIZIX를 논리 Z 연산자로 결정하고, 그 나머지로부터 제2 안정연산자 생성자 S_2 = {XZIIZII, ZXZIIII, IZXZIII, IIZXZII, ZIIZXIZ}를 생성할 수 있다. 이때, 만약에, 6번의 얽힌 큐비트가 아닌 3번 큐비트에 대응되는 위치에 X 연산자를 포함하는 안정연산자인 IZXZIII를 논리 Z 연산자로 결정할 경우, 그 3번 큐비트에 대응되는 위치에 Z 오류가 발생할 경우, 그 오류는 검출되지 않을 수 있다.

[83] 또 다른 실시예에서는, 양자 오류 정정 부호 생성 장치가 적어도 하나의 논리 Z 연산지 및 제2 안정연산자 생성자로부터 논리 X 연산자를 생성할 수 있다.

[84] 즉, 양자 오류 정정 부호 생성 장치가 결정된 적어도 하나의 논리 Z 연산자에 포함된 X 연산자를 Z 연산자로 대체한 적어도 하나의 후보연산자를 생성하고, 제2 안정연산자 생성자 중에서 그 적어도 하나의 후보연산자와 동일한 위치에 Z 연산자를 포함하는 안정연산자 및 생성된 적어도 하나의 후보연산자를 이용하여 적어도 하나의 논리 X 연산자를 생성할 수 있다.

[85] 예컨대, 양자 오류 정정 부호 생성 장치가 논리 Z 연산자로 결정된 IIIIZIX에

대하여 X 연산자를 Z 연산자로 대체한 IIIIIZ로 후보연산자를 생성할 수 있다. 이때, 후보연산자의 5번째 큐비트에 대응되는 위치에서 Z 연산자는 I 연산자로 대체될 수 있다. 그리고, 제2 안정연산자 생성자 중에서 후보연산자인 IIIIIZ와 그 후보연산자와 동일하게 6번 큐비트에 대응되는 위치에 Z 연산자를 포함하는 안정연산자인 ZIIZXIZ를 서로 곱하여 논리 X 연산자인 ZIIZXII를 생성할 수 있다. 이는, Z 연산자와 Z 연산자를 곱할 경우 I 연산자가 되므로, Z 연산자가 상쇄되는 성질을 이용하기 위한 것일 수 있다.

[86] 또 다른 실시예에서는, 적어도 하나의 논리 X 연산자는 수학식 5에 의해 산출될 수 있다.

[87] [수학식 5]

[88]
$$\overline{X} = S_i \bullet I \,|\, Z_i$$
$$= X_j Z^{r_i} \,|\, I \quad \text{for } i = 1,\ldots,k(k=c)$$

[89] 여기서, $\overline{X}$는 적어도 하나의 논리 X 연산자이고, S_i는 안정연산자이고, X는 X 연산자이고, Z는 Z 연산자이고, I는 항등 연산자이고, i는 얽힌 큐비트의 인덱스이고, r_i는 그래프 상태에 대응되는 인접행렬(adjacency matrix)에서 얽힌 큐비트에 대응되는 i번째 행이고, k와 c는 얽힌 큐비트의 개수이고, n이 복수의 큐비트 중 논리적 큐비트의 개수일 때 j는 i+(n-c)로 정의되는 값이다.

[90] 이때, 수학식 5에서 S_i는 제2 안정연산자 생성자에 포함된 안정연산자 중에서 후보연산자와 동일한 위치에 Z 연산자를 포함하는 안정연산자이고, IIZ_i는 후보연산자일 수 있다. 그리고, 양자 오류 정정 부호 생성 장치가 그 안정연산자와 후보연산자를 곱셈 연산하여 최종적으로 논리 X 연산자를 생성할 수 있다.

[91] 즉, 양자 오류 정정 부호 생성 장치가, 수신단 측은 부호를 직접 인코딩할 수 없기 때문에, 후보연산자 및 그 후보연산자와 동일한 위치에 Z 연산자를 포함하는 안정연산자 간에 곱셈 연산을 수행하여 논리 X 연산자에 포함된 Z 연산자를 상쇄할 수 있다.

[92] 또 다른 실시예에서는, 양자 오류 정정 부호 생성 장치가 적어도 하나의 논리 X 연산자, 적어도 하나의 논리 Z 연산자 및 제2 안정연산자 생성자를 이용하여, 적어도 하나의 얽힌 큐비트를 포함하는 복수의 큐비트에 대응되는 양자 오류 정정 부호를 생성할 수 있다.

[93] 예컨대, 양자 오류 정정 부호 생성 장치가, 적어도 하나의 논리 X 연산자,

적어도 하나의 논리 Z 연산자 및 제2 안정연산자 생성자를 이용하여, 그 복수의 큐비트에 대응되는 코드워드가 양자 통신 과정에서 채널을 통과하면서 발생하는 오류를 검출하여 복원할 수 있다.

[94] 즉, 양자 오류 정정 부호 생성 장치가 n개의 논리적 큐비트에 대하여 c개의 얽힌 큐비트가 존재할 때, [[n,c,d;c]] 부호를 생성하여, 양자 오류를 검출하고 정정할 수 있다.

[95] 이와 같이, 본 발명의 일 실시예에 따른 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법은 얽힌 양자가 적용된 그래프 상태에 대해, 얽힌 큐비트에 대응되는 안정연산자를 논리 Z 연산자로 결정하고, 그에 따라 안정연산자 생성자 및 논리 X 연산자를 생성함으로써, 그 얽힌 큐비트 위치에서의 Z 오류가 검출되지 않는 문제없이, 용이하게 양자 오류 정정 부호를 생성하고 그 부호의 차원을 확장시킬 수 있는 효과가 있다.

[96] 도 2는 본 발명의 일 실시예에 따른 제1 안정연산자 생성자의 생성 방법을 도시하기 위한 흐름도이다.

[97] 단계 S210에서는, 양자 오류 정정 부호 생성 장치가 그래프 상태에 기초하여, 복수의 큐비트 상호 간의 인접 여부를 나타내는 인접행렬을 생성한다.

[98] 이때, 인접행렬은 큐비트의 물리적인 개수와 동일한 개수의 행 및 열을 가질 수 있으며, 인접행렬 내부에서 인접 여부는 인접할 경우 1로, 인접하지 않은 경우 0으로 표현될 수 있다. 즉, 큐비트의 물리적인 개수가 6인 경우, 인접행렬은 6x6의 행렬일 수 있다. 한편, 각 큐비트는 각 큐비트 자신과는 인접하지 않은 것으로 간주될 수 있다. 즉, 1번 큐비트와 1번 큐비트 간의 인접여부는 0일 수 있다.

[99] 예컨대, 도 4를 참조하면, 1번 큐비트는 2번 및 5번 큐비트와 인접하므로 인접행렬의 1행은 {0, 1, 0, 0, 1, 0}의 값으로 나타낼 수 있다. 또한, 2번 큐비트는 1번 및 3번 큐비트와 인접하므로 인접행렬의 2행은 {1, 0, 1, 0, 0, 0}의 값으로 나타낼 수 있다. 동일한 방법으로 인접행렬을 생성한 결과는 도 5와 같다.

[100] 단계 S220에서는, 양자 오류 정정 부호 생성 장치가 파울리 연산자로 구성되며, 인접행렬의 각 행에 대응되는 복수의 안정연산자를 산출한다.

[101] 예컨대, 양자 오류 정정 부호 생성 장치가 도 4의 각 큐비트별로 대응되는 인덱스(i) 및 수학식 3을 이용하여 복수의 안정연산자를 산출할 수 있다.

[102] 단계 S230에서는, 양자 오류 정정 부호 생성 장치가 그 산출된 복수의 안정연산자를 포함하는 제1 안정연산자 생성자를 생성한다.

[103] 예컨대, 양자 오류 정정 부호 생성 장치가 산출된 복수의 안정연산자를 포함하도록 하여 제1 안정연산자 생성자를 생성할 수 있다. 즉, 제1 안정연산자 생성자는 복수의 안정연산자 각각을 원소로 하는 집합으로 볼 수 있다.

[104] 다른 실시예에서는, 제1 안정연산자 생성자는 수학식 3에 의해 산출될 수 있다.

[105] 즉, 양자 오류 정정 부호 생성 장치가 얽힌 큐비트를 포함하고 있는 그래프 상태의 안정연산자를 위에서 설명한 수학식 3을 이용하여 산출할 수 있다.

[106] 본 발명의 일 실시예에 따른 도 6의 2개의 얽힌 큐비트를 포함하는 그래프 상태에 대하여 양자 오류 정정 부호를 생성하는 방법은 다음과 같다.

[107] 이때, 논리적 큐비트는 5개이고, 얽힌 큐비트는 2개이므로, 양자 오류 정정 부호 생성 장치는 [[5,1,3;1]] 부호를 생성할 수 있다.

[108] 도 7 및 수학식 3을 이용하여, 양자 오류 정정 부호 생성 장치가 도 6의 그래프 상태에 대응되는 제1 안정연산자 생성자를 생성하면, S_1 = {XZIIZIII, ZXZIIIII, IZXZIIII, IIZXZIZI, ZIIZXIIZ, IIIZIIXI, IIIIZIIX}와 같다. 그리고, 이 제1 안정연산자 생성자 중에서, 얽힌 큐비트인 6번 및 7번 큐비트에 대응되는 안정연산자인 IIIZIIXI 및 IIIIZIIX를 논리 Z_1 연산자 및 논리 Z_2 연산자로 결정한다.

[109] 또한, 논리 Z_1 연산자 및 논리 Z_2 연산자를 제외한 나머지를 이용하여 제2 안정연산자 생성자인 S_2 = {XZIIZIII, ZXZIIIII, IZXZIIII, IIZXZIZI, ZIIZXIIZ}를 생성한다.

[110] 또한, 논리 Z_1 연산자인 IIIZIIXI에 대응되는 후보연산자인 IIIIIIZI와 동일한 위치에 Z 연산자를 포함하는 안정연산자인 IIZXZIZI를 곱하여, 논리 X_1 연산자인 IIZXZIII를 생성한다. 마찬가지 방법으로, 논리 Z_2 연산자인 IIIIZIIX에 대응되는 후보연산자인 IIIIIIIZ와 동일한 위치에 Z 연산자를 포함하는 안정연산자인 ZIIZXIIZ를 곱하여, 논리 X_2 연산자인 ZIIZXIII를 생성한다.

[111] 이와 같이, 그래프 상태에 얽힘 양자를 추가하여 얽힌 큐비트의 개수를 증가시킴에 따라서, 양자 오류 정정 부호 생성 장치가 그 증가된 개수만큼 부호의 차원을 확장할 수 있다.

[112] 또한, 본 발명의 일 실시예에 따른 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법은 양자 바운드를 만족하는 부호를 용이하게 생성할 수 있다.

[113] 예컨대, 8 링 그래프(8 ring graph)에 얽힌 양자를 4개 추가하는 경우, 가장 만족시키기 어려운 바운드 중 하나인 선형 프로그래밍 바운드(linear programming bound)를 만족하는 [[8,4,4;4]]부호를 생성할 수 있다. 또한, 도 8을 참조하면, n=12 및 k=8일 때, 가장 큰 최소 거리(minimum distance)를 가지는 것으로 알려진 도 8의 그래프에 6개의 얽힌 양자를 추가하여 [[12,6,5;6]]부호를 생성할 수 있다.

[114] 도 3은 본 발명의 일 실시예에 따른 그래프 상태를 이용한 양자 오류 정정 부호의 생성 장치를 도시하기 위한 도면이다.

[115] 도 3을 참조하면, 본 발명의 일 실시예에 따른 그래프 상태를 이용한 양자 오류 정정 부호의 생성 장치(300)는 그래프부(310), 제1 생성자부(320) 및 제2 생성자부(330)를 포함한다. 또한, 선택적으로 ECC생성부(미도시)를 더 포함할 수 있다. 한편, 그래프 상태를 이용한 양자 오류 정정 부호의 생성 장치(300)는 컴퓨터, 스마트폰 및 태블릿 등에 탑재될 수 있다.

[116] 그래프부(310)는 적어도 하나의 얽힌 큐비트를 포함하는 복수의 큐비트에 대하여, 각 큐비트 간의 인접 관계를 나타내는 그래프 상태를 생성한다.

[117] 제1 생성자부(320)는 그 그래프 상태에 대응되며, 그 복수의 큐비트의 오류를 검출하기 위한 복수의 안정연산자로 구성되는 제1 안정연산자 생성자를 생성한다.

[118] 다른 실시예에서는, 제1 생성자부(320)는 그래프 상태에 기초하여, 복수의 큐비트 상호 간의 인접 여부를 나타내는 인접행렬을 생성하고, 파울리 연산자로 구성되며, 그 인접행렬의 각 행에 대응되는 복수의 안정연산자를 산출하고, 그 산출된 복수의 안정연산자를 포함하는 제1 안정연산자 생성자를 생성할 수 있다.

[119] 또 다른 실시예에서는, 제1 안정연산자 생성자는 수학식 3에 의해 산출될 수 있다.

[120] 제2 생성자부(330)는 그 제1 안정연산자 생성자 및 적어도 하나의 얽힌 큐비트에 기초하여, 코드워드의 위상플립연산에 이용되는 적어도 하나의 논리 Z 연산자, 코드워드의 비트플립연산에 이용되는 적어도 하나의 논리 X 연산자 및 제1 안정연산자 생성자의 부분집합인 제2 안정연산자 생성자를 생성한다.

[121] 다른 실시예에서는, 제2 생성자부(330)는 그 적어도 하나의 얽힌 큐비트에 기초하여, 제1 안정연산자 생성자를 구성하는 복수의 안정연산자 중 적어도 하나를 적어도 하나의 논리 Z 연산자로 결정하고, 나머지로 제2 안정연산자 생성자를 생성하고, 적어도 하나의 논리 Z 연산자 및 제2 안정연산자 생성자를 이용하여 적어도 하나의 논리 X 연산자를 생성할 수 있다.

[122] 또 다른 실시예에서는, 제2 생성자부(330)는 제1 안정연산자 생성자를 구성하는 복수의 안정연산자 중에서, 그 적어도 하나의 얽힌 큐비트에 대응되는 위치에 비트플립연산에 이용되는 X 연산자를 포함하는 적어도 하나를 적어도 하나의 논리 Z 연산자로 결정하고, 그 적어도 하나의 논리 Z 연산자를 제외한 나머지로 구성되는 제2 안정연산자 생성자를 생성할 수 있다.

[123] 또 다른 실시예에서는, 제2 생성자부(330)는 그 적어도 하나의 논리 Z 연산자에 포함된 X 연산자를 큐비트의 위상플립연산에 이용되는 Z 연산자로 대체한 적어도 하나의 후보연산자를 생성하고, 제2 안정연산자 생성자 중 그 적어도 하나의 후보연산자와 동일한 위치에 Z 연산자를 포함하는 안정연산자 및 그 적어도 하나의 후보연산자를 이용하여 적어도 하나의 논리 X 연산자를 생성할 수 있다.

[124] 마지막으로 ECC생성부(미도시)는 적어도 하나의 논리 X 연산자, 적어도 하나의 논리 Z 연산자 및 제2 안정연산자 생성자를 이용하여, 적어도 하나의 얽힌 큐비트를 포함하는 복수의 큐비트에 대응되는 양자 오류 정정 부호를 생성한다.

[125] 한편, 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

[126] 상기 컴퓨터로 읽을 수 있는 기록매체는 마그네틱 저장매체(예를 들면, 롬,

플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등) 를 포함한다.

[127] 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

청구범위

[청구항 1] 적어도 하나의 얽힌 큐비트(entangled qubit: ebit)를 포함하는 복수의 큐비트에 대하여, 각 큐비트 간의 인접 관계를 나타내는 그래프 상태(graph state)를 생성하는 단계;
상기 그래프 상태에 대응되며, 상기 복수의 큐비트의 오류를 검출하기 위한 복수의 안정연산자로 구성되는 제1 안정연산자 생성자(stabilizer generator)를 생성하는 단계; 및
상기 제1 안정연산자 생성자 및 상기 적어도 하나의 얽힌 큐비트에 기초하여, 코드워드의 위상플립연산에 이용되는 적어도 하나의 논리 Z 연산자, 코드워드의 비트플립연산에 이용되는 적어도 하나의 논리 X 연산자 및 상기 제1 안정연산자 생성자의 부분집합인 제2 안정연산자 생성자를 생성하는 단계
를 포함하는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법.

[청구항 2] 제1항에 있어서,
상기 제2 안정연산자 생성자를 생성하는 단계는
상기 적어도 하나의 얽힌 큐비트에 기초하여, 상기 제1 안정연산자 생성자를 구성하는 상기 복수의 안정연산자 중 적어도 하나를 상기 적어도 하나의 논리 Z 연산자로 결정하고, 나머지로 상기 제2 안정연산자 생성자를 생성하는 단계; 및
상기 적어도 하나의 논리 Z 연산자 및 상기 제2 안정연산자 생성자를 이용하여 상기 적어도 하나의 논리 X 연산자를 생성하는 단계
를 포함하는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법.

[청구항 3] 제2항에 있어서,
상기 나머지로 제2 안정연산자 생성자를 생성하는 단계는
상기 제1 안정연산자 생성자를 구성하는 상기 복수의 안정연산자 중에서, 상기 적어도 하나의 얽힌 큐비트에 대응되는 위치에 비트플립연산에 이용되는 X 연산자를 포함하는 적어도 하나를 상기 적어도 하나의 논리 Z 연산자로 결정하는 단계; 및
상기 적어도 하나의 논리 Z 연산자를 제외한 나머지로 구성되는 상기 제2 안정연산자 생성자를 생성하는 단계
를 포함하는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법.

[청구항 4] 제2항에 있어서,
상기 적어도 하나의 논리 X 연산자를 생성하는 단계는
상기 적어도 하나의 논리 Z 연산자에 포함된 상기 X 연산자를 큐비트의

위상플립연산에 이용되는 Z 연산자로 대체한 적어도 하나의 후보연산자를 생성하는 단계; 및

상기 제2 안정연산자 생성자 중 상기 적어도 하나의 후보연산자와 동일한 위치에 상기 Z 연산자를 포함하는 안정연산자 및 상기 적어도 하나의 후보연산자를 이용하여 상기 적어도 하나의 논리 X 연산자를 생성하는 단계

를 포함하는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법.

[청구항 5] 제4항에 있어서,

상기 적어도 하나의 논리 X 연산자는 수학식 1에 의해 산출되는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법.

[수학식 1]

$$\overline{X} = X_j Z^{r_i} | I \quad \text{for } i = 1, \ldots, k (k = c)$$

여기서, $\overline{X}$는 상기 적어도 하나의 논리 X 연산자이고, X는 상기 X 연산자이고, Z는 상기 Z 연산자이고, I는 항등 연산자이고, i는 상기 얽힌 큐비트의 인덱스이고, r_i는 상기 그래프 상태에 대응되는 인접행렬(adjacency matrix)에서 상기 얽힌 큐비트에 대응되는 i번째 행이고, k와 c는 상기 얽힌 큐비트의 개수이고, n이 상기 복수의 큐비트 중 논리적 큐비트의 개수일 때 j는 i+(n-c)로 정의되는 값이다.

[청구항 6] 제1항에 있어서,

상기 제1 안정연산자 생성자를 생성하는 단계는

상기 그래프 상태에 기초하여, 상기 복수의 큐비트 상호 간의 인접 여부를 나타내는 인접행렬을 생성하는 단계;

파울리 연산자로 구성되며, 상기 인접행렬의 각 행에 대응되는 복수의 안정연산자를 산출하는 단계; 및

상기 산출된 복수의 안정연산자를 포함하는 상기 제1 안정연산자 생성자를 생성하는 단계

를 포함하는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법.

[청구항 7] 제6항에 있어서,

상기 제1 안정연산자 생성자는 수학식 2에 의해 산출되는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법.

[수학식 2]

$$S = \begin{cases} X_i Z^{r_i} | I \quad (i=1,\ldots,n-c) \\ X_i Z^{r_i} | Z_j \quad (i=n-c+1,\ldots,n) \\ Z_i | X_j \quad (i=n-c+1,\ldots,n) \end{cases}$$

여기서, S는 상기 제1 안정연산자 생성자이고, X는 큐비트의 비트플립연산에 이용되는 연산자이고, Z는 큐비트의 위상플립연산에 이용되는 연산자이고, I는 큐비트의 항등 연산자이고, n은 상기 복수의 큐비트 중 논리적 큐비트의 개수이고, c는 상기 얽힌 큐비트의 개수이고, j는 i-(n-c)로 정의되는 값이고, r_i는 상기 인접행렬의 i번째 행이다.

[청구항 8] 제1항에 있어서,
상기 적어도 하나의 논리 X 연산자, 적어도 하나의 상기 논리 Z 연산자 및 상기 제2 안정연산자 생성자를 이용하여, 상기 적어도 하나의 얽힌 큐비트를 포함하는 복수의 큐비트에 대응되는 양자 오류 정정 부호를 생성하는 단계
를 더 포함하는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 방법.

[청구항 9] 적어도 하나의 얽힌 큐비트를 포함하는 복수의 큐비트에 대하여, 각 큐비트 간의 인접 관계를 나타내는 그래프 상태를 생성하는 그래프부;
상기 그래프 상태에 대응되며, 상기 복수의 큐비트의 오류를 검출하기 위한 복수의 안정연산자로 구성되는 제1 안정연산자 생성자를 생성하는 제1 생성자부; 및
상기 제1 안정연산자 생성자 및 상기 적어도 하나의 얽힌 큐비트에 기초하여, 코드워드의 위상플립연산에 이용되는 적어도 하나의 논리 Z 연산자, 코드워드의 비트플립연산에 이용되는 적어도 하나의 논리 X 연산자 및 상기 제1 안정연산자 생성자의 부분집합인 제2 안정연산자 생성자를 생성하는 제2 생성자부
를 포함하는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 장치.

[청구항 10] 제9항에 있어서,
상기 제2 생성자부는
상기 적어도 하나의 얽힌 큐비트에 기초하여, 상기 제1 안정연산자 생성자를 구성하는 상기 복수의 안정연산자 중 적어도 하나를 상기 적어도 하나의 논리 Z 연산자로 결정하고, 나머지로 상기 제2 안정연산자

생성자를 생성하고,
상기 적어도 하나의 논리 Z 연산자 및 상기 제2 안정연산자 생성자를 이용하여 상기 적어도 하나의 논리 X 연산자를 생성하는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 장치.

[청구항 11] 제10항에 있어서,
상기 제2 생성자부는
상기 제1 안정연산자 생성자를 구성하는 상기 복수의 안정연산자 중에서, 상기 적어도 하나의 얽힌 큐비트에 대응되는 위치에 비트플립연산에 이용되는 X 연산자를 포함하는 적어도 하나를 상기 적어도 하나의 논리 Z 연산자로 결정하고,
상기 적어도 하나의 논리 Z 연산자를 제외한 나머지로 구성되는 상기 제2 안정연산자 생성자를 생성하는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 장치.

[청구항 12] 제10항에 있어서,
상기 제2 생성자부는
상기 적어도 하나의 논리 Z 연산자에 포함된 상기 X 연산자를 큐비트의 위상플립연산에 이용되는 Z 연산자로 대체한 적어도 하나의 후보연산자를 생성하고,
상기 제2 안정연산자 생성자 중 상기 적어도 하나의 후보연산자와 동일한 위치에 상기 Z 연산자를 포함하는 안정연산자 및 상기 적어도 하나의 후보연산자를 이용하여 상기 적어도 하나의 논리 X 연산자를 생성하는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 장치.

[청구항 13] 제9항에 있어서,
상기 제1 생성자부는
상기 그래프 상태에 기초하여, 상기 복수의 큐비트 상호 간의 인접 여부를 나타내는 인접행렬을 생성하고,
파울리 연산자로 구성되며, 상기 인접행렬의 각 행에 대응되는 복수의 안정연산자를 산출하고,
상기 산출된 복수의 안정연산자를 포함하는 상기 제1 안정연산자 생성자를 생성하는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 장치.

[청구항 14] 제13항에 있어서,
상기 제1 안정연산자 생성자는 수학식 3에 의해 산출되는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 장치.
[수학식 3]

$$S = \begin{cases} X_i Z^{r_i} | I \quad (i=1,\ldots,n-c) \\ X_i Z^{r_i} | Z_j \quad (i=n-c+1,\ldots,n) \\ Z_i | X_j \quad (i=n-c+1,\ldots,n) \end{cases}$$

여기서, S는 상기 제1 안정연산자 생성자이고, X는 큐비트의 비트플립연산에 이용되는 연산자이고, Z는 큐비트의 위상플립연산에 이용되는 연산자이고, I는 큐비트의 항등 연산자이고, n은 상기 복수의 큐비트 중 논리적 큐비트의 개수이고, c는 상기 얽힌 큐비트의 개수이고, j는 i-(n-c)로 정의되는 값이고, r_i는 상기 인접행렬의 i번째 행이다.

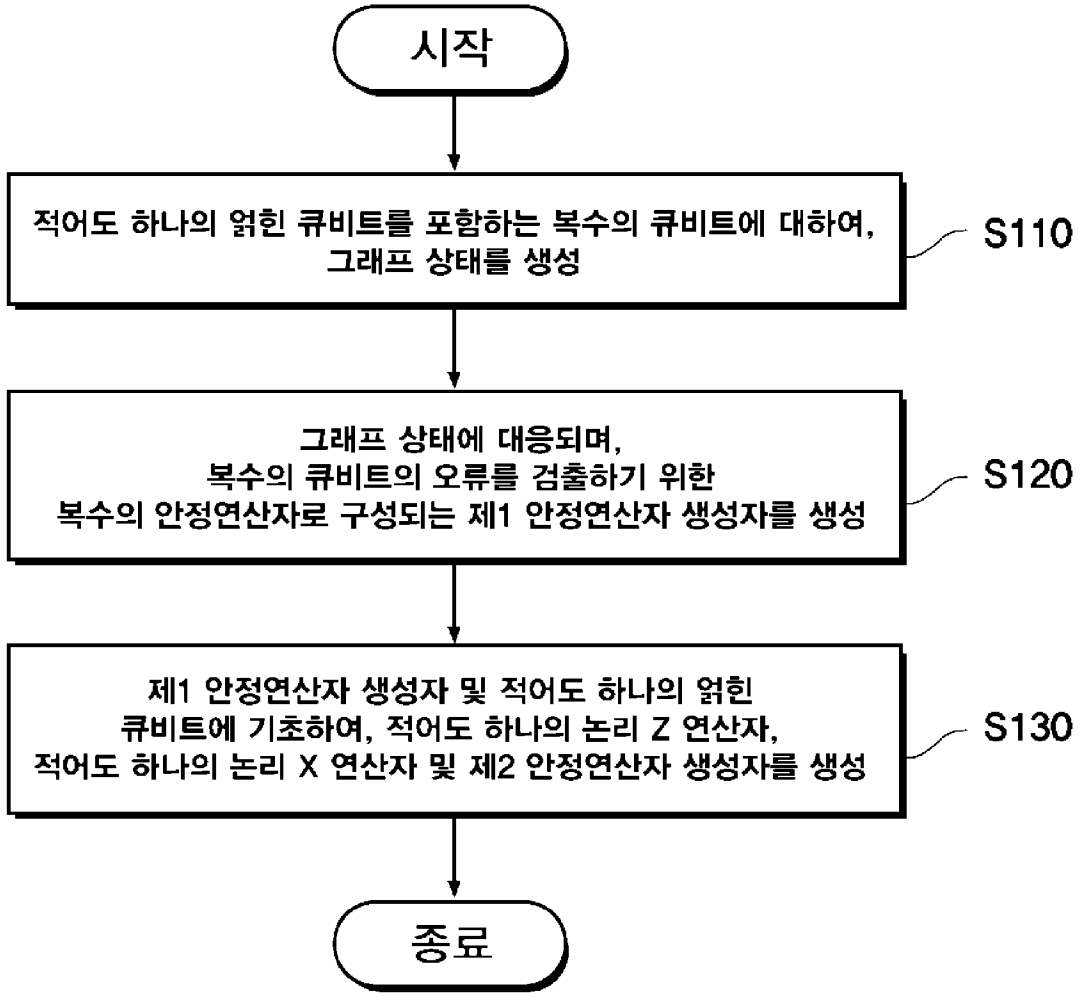
[청구항 15] 제9항에 있어서,

상기 적어도 하나의 논리 X 연산자, 상기 적어도 하나의 논리 Z 연산자 및 상기 제2 안정연산자 생성자를 이용하여, 상기 적어도 하나의 얽힌 큐비트를 포함하는 복수의 큐비트에 대응되는 양자 오류 정정 부호를 생성하는 ECC생성부

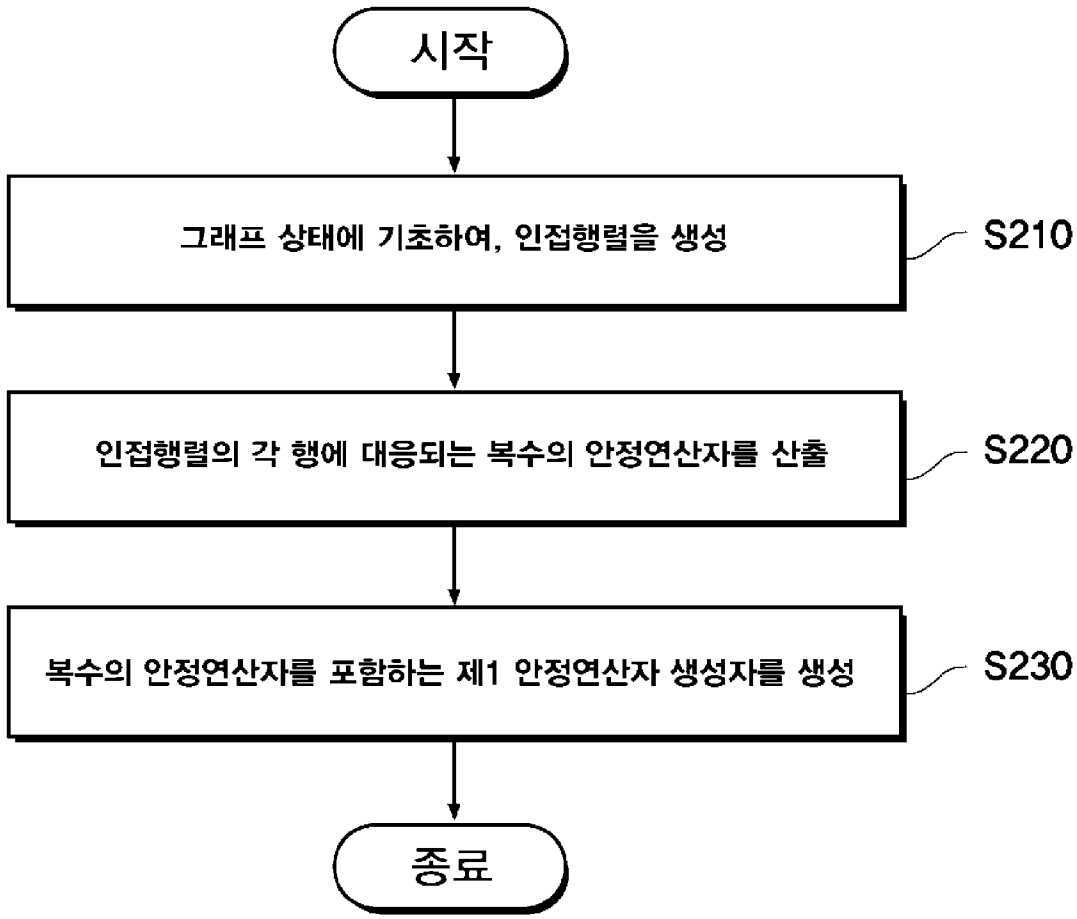
를 더 포함하는 것을 특징으로 하는 그래프 상태를 이용한 양자 오류 정정 부호의 생성 장치.

WO 2017/217577 PCT/KR2016/006809

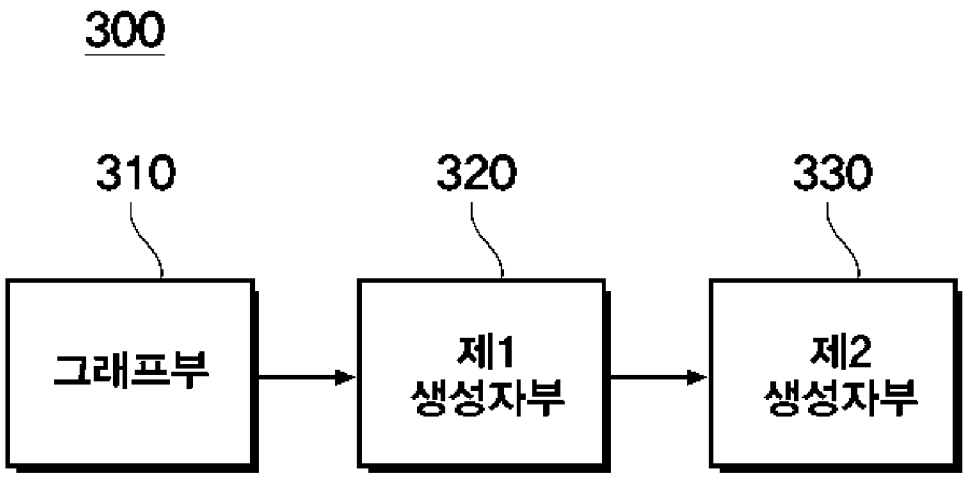
[도1]



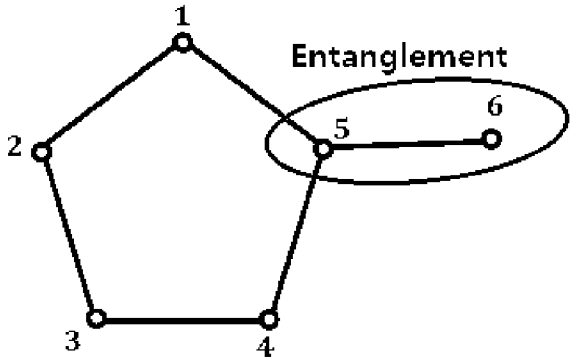
[도2]


시작
그래프 상태에 기초하여, 인접행렬을 생성
S210
인접행렬의 각 행에 대응되는 복수의 안정연산자를 산출
S220
복수의 안정연산자를 포함하는 제1 안정연산자 생성자를 생성
S230
종료

[도3]


300
310
320
330
그래프부
제1
생성자부
제2
생성자부

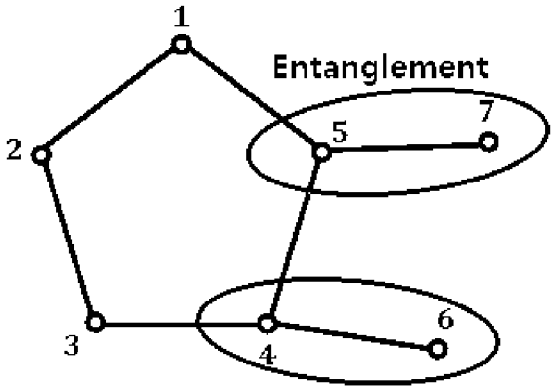
[도4]



[도5]

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

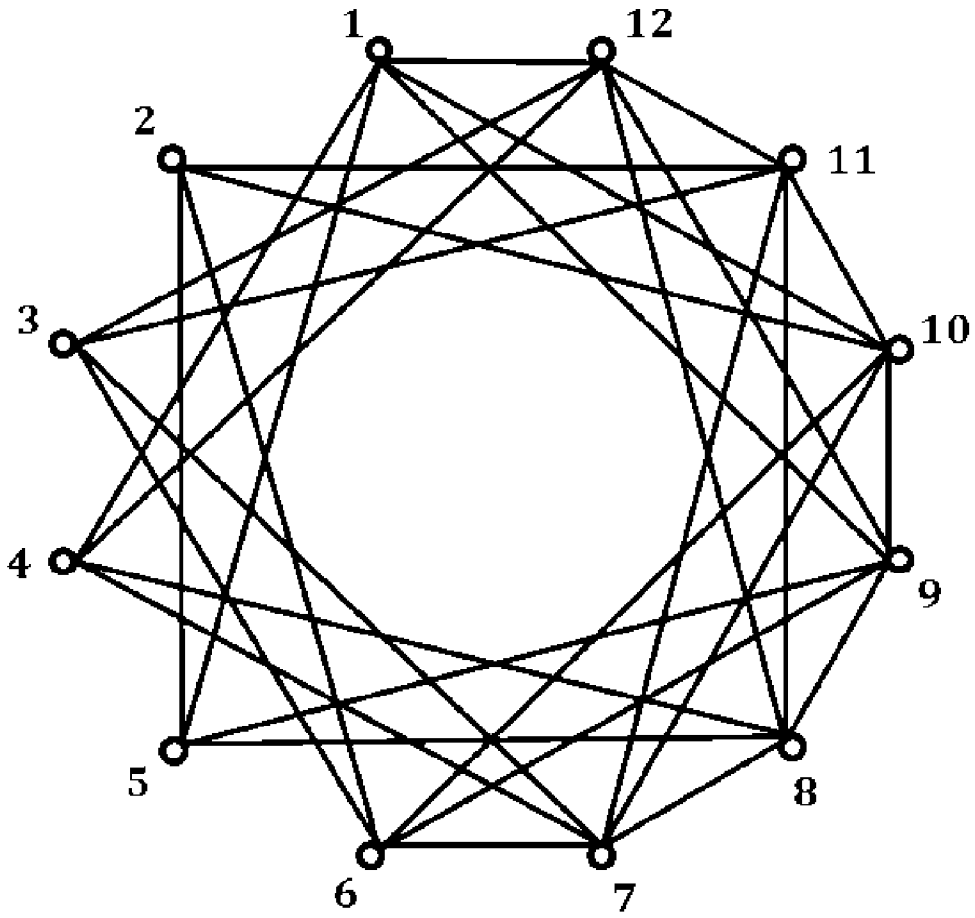
[도6]



[도7]

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

[도8]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2016/006809

A. CLASSIFICATION OF SUBJECT MATTER

H03M 13/29(2006.01)i, H03M 13/11(2006.01)i, G06N 99/00(2010.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H03M 13/29; G06F 17/50; G06F 17/16; G06F 11/10; H03M 13/03; H03M 13/11; G06N 99/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: entangled qubit(entangled qubit), adjacent(adjacent), stabilizer(stabilizer), graph state (graph state)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HEIN, M. et al., "Entanglement in Graph States and its Applications", arXiv: quant-ph/0602096v1, 11 February 2006 See pages 6, 15, 25, 34.	1-15
A	US 2010-0251049 A1 (GOTO, Hayato et al.) 30 September 2010 See paragraphs [0050]-[0172] and figures 1-16.	1-15
A	MORDECAI, Waegell, "A Bonding Model of Entanglement for N-qubit Graph States", arXiv:1406.0206v2 [quant-ph], 24 September 2014 See pages 1-17.	1-15
A	US 2015-0339417 A1 (THE REGENTS OF THE UNIVERSITY OF MICHIGAN) 26 November 2015 See paragraphs [0037]-[0078] and figures 1-10.	1-15
A	US 2014-0365843 A1 (ALCATEL-LUCENT USA INC.) 11 December 2014 See paragraphs [0033]-[0089] and figures 1-5.	1-15

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 FEBRUARY 2017 (16.02.2017)	**17 FEBRUARY 2017 (17.02.2017)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. +82-42-481-8578	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2016/006809

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2010-0251049 A1	30/09/2010	JP 04786727 B2	05/10/2011
		JP 2010-233066 A	14/10/2010
		US 8386899 B2	26/02/2013
US 2015-0339417 A1	26/11/2015	WO 2015-179753 A1	26/11/2015
US 2014-0365843 A1	11/12/2014	EP 3005572 A1	13/04/2016
		US 9286154 B2	15/03/2016
		WO 2014-197757 A1	11/12/2014

국 제 조 사 보 고 서

국제출원번호
PCT/KR2016/006809

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H03M 13/29(2006.01)i, H03M 13/11(2006.01)i, G06N 99/00(2010.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H03M 13/29; G06F 17/50; G06F 17/16; G06F 11/10; H03M 13/03; H03M 13/11; G06N 99/00

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: 얽힌 큐비트(entangled qubit), 인접(adjacent), 안정연산자(stabilizer), 그래프 상태(graph state)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	M. HEIN 등, 'Entanglement in Graph States and its Applications', arXiv:quant-ph/0602096v1, 2006.02.11 페이지 6, 15, 25, 34 참조.	1-15
A	US 2010-0251049 A1 (HAYATO GOTO 등) 2010.09.30 단락 [0050]-[0172] 및 도면 1-16 참조.	1-15
A	MORDECAI WAEGELL, 'A bonding model of entanglement for N-qubit graph states', arXiv:1406.0206v2 [quant-ph], 2014.09.24 페이지 1-17 참조.	1-15
A	US 2015-0339417 A1 (THE REGENTS OF THE UNIVERSITY OF MICHIGAN) 2015.11.26 단락 [0037]-[0078] 및 도면 1-10 참조.	1-15
A	US 2014-0365843 A1 (ALCATEL-LUCENT USA INC.) 2014.12.11 단락 [0033]-[0089] 및 도면 1-5 참조.	1-15

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2017년 02월 16일 (16.02.2017)	2017년 02월 17일 (17.02.2017)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
이은규
전화번호 +82-42-481-3580

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2016/006809

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2010-0251049 A1	2010/09/30	JP 04786727 B2	2011/10/05
		JP 2010-233066 A	2010/10/14
		US 8386899 B2	2013/02/26
US 2015-0339417 A1	2015/11/26	WO 2015-179753 A1	2015/11/26
US 2014-0365843 A1	2014/12/11	EP 3005572 A1	2016/04/13
		US 9286154 B2	2016/03/15
		WO 2014-197757 A1	2014/12/11