Graph state 기법을 이용한 6-큐비트 양자 오류 정정 부호 설계

신정환, 허 준
고려대학교

요 약

본 고에서는 그래프 상태(graph state)를 이용하여 양 자 오류 정정 부호를 설계하는 기법에 대해서 알아본다. 그래프 상태는 꼭짓점과 각 꼭짓점을 연결하는 변으로 구성된다. 그래프 상태에서 각 꼭지점은 실제 코드워드의 각 큐비트에 해당하며 꼭지 점을 연결하는 변은 양자 오류 정정 부호의 부호화 방식을 결정한다. 본 고에서는 그래프 상태의 특성을 알아보고 그래프 상태 기반 양자 오류 정정 부호 설계 기법을 이용하여 단일 오류를 검출할 수 있는 6-큐비트 양자 오류 정정 부호 설계 방법에 대해 알아본다.

Ⅰ. 서 론

1995년 Shor가 소개한 9-큐비트 양자 오류 정정 부호 [1] 이후 다양한 방식의 양자 오류 정정 부호 설계 기법이 연구되고 있다[2]-[7]. 양자 오류 정정 부호는 크게 additive 부호와 non-additive 부호로 구분할 수 있다. Additive 부호의 경우 고전 오류 정정 부호의 선형 부호와 유사한 특징을 가지고 있으며 체계적인 방법을 이용하여 양자 오류 정정 부호를 설계할 수 있는 장점을 가지고 있다. 이러한 체계적 구성 방법으로 인해 많은 양자 오류 정정 부호는 additive 부 호의 특징을 가지고 연구되고 있으며, 대표적인 양자 오류 정정 부호 설계 기법으로 stabilizer 부호를 생각할 수 있다. 특히 stabilizer 부호는 고전 선형 블록 오류 정정 부호로 부 터 양자 오류 정정 부호를 설계할 수 있는 방법을 제시한다. 반면, non-additive 부호의 경우 부호를 설계하는 과정이 체계적이지 못하지만 일반적으로 additive 부호에 비해 더 큰 코드워드 공간 또는 더 많은 오류 정정 능력 등 더 좋은 성능을 갖는 부호를 설계할 수 있다[8]-[12]. 최근 Codeword stabilized (CWS) [13] 양자 오류 정정 부호 설계 기법은 그래프를 이용하여 고전 오류 정정 부호로부터 양자 오류 정정 부호를 설계할 수 있는 기법이 제시하고 있다. CWS 기법을 이용할 경우 채널에서 발생하는 오류의 형태에 따라 고전 이진 오류 정정 부호를 정의할 수 있으며, 이를 이용하여 체계적인 방법으로 양자 오류 정정 부호의 코드워드를 구성할 수 있다. 하지만 CWS 부호를 이용하여 설계된 양자 오류 정정 부호는 부호의 minimum distance가 3 이하로 제한되는 특징을 가지고 있다. 이러한 단점을 극복하기 위해 얽힌 큐비트(entangled qubit)를 사용할 수 있는데 얽힌 큐비트를 이용한 CWS부호의 경우3이상의 양자 오류 정정 부호 설계가 가능하다. [14] 양자 오류 정정 부호를 설계하는 연구 중 그래프를 이용한 연구가 많이 진행되고 있다[15]-[17]. 위에서 언급한 CWS 부호 또한 그래프를 이용한 양자 오류 정정 부호이다. 그래프를 이용할 경우 부호의 코드워드 구성이 단순하며 코드워드에 관련된 연산자를 쉽게 구성할 수 있다. 또한 그래프의 변형을 통해 다양한 양자 오류 정정 부호의 구성이 가능하다. 따라서, 본 고에서는 그래프를 이 용하여 양자 오류 정정 부호를 설계하는 기법을 살펴본다. 자세하게는, 그래프와 그래프 상태에 대한 일반적인 내용을 살펴보고 CWS 기법을 이용하여 양자 오류를 이진 오류로 변환하고 이를 이용하여 양자 오류 정정 부호를 설계하는 과정을 살펴본다. 그리고 그래프 상태와 CWS 부호 기법을 이용하여 양자 오류 정정 부호를 설계하는 방법을 소개하고, 이렇게 설계된 부호가 단일 오류에 대한 검출 능력을 가지며 16개의 논리 상태를 인코딩 할 수 있음을 보여 준다.

Ⅱ. 본 론

양자 시스템은 양자 상태 (quantum state)로 나타낼 수 있으며, 양자 상태는 수학적으로 힐버트 공간 H위의 positive 연산자, density 행렬 ρ로 표현된다. density 행렬은 trace 연산을 취한 값이 1이며, 이를 이용하여 모든 양자 상태의 집합 $J(H)$을 수식으로 표현하면 다음과 같다.

$$J(H) = \{\rho \in B(H): \rho \geq 0, \mathrm{Tr}\rho = 1\}$$

이 때, $B(H)$는 H에 존재하는 모든 bounded 선형 연산자의 집

합을 나타낸다. Density 연산자는 양자 상태의 가능한 모든 측정에 대한 측정 확률과 그에 해당하는 결과 상태로 나타낼 수 있다.

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

ρ의 rank가 1일 때, 양자 상태를 순수 상태 (pure state)라고 하며, 그렇지 않은 경우 혼합 상태(mixed state)라 한다. 이는 간단한 방법으로 확인할 수 있는데, 순수 상태인 경우 $\mathrm{Tr}(\rho^2) = 1$이며, 혼합 상태의 경우 $\mathrm{Tr}(\rho^2) < 1$이다. 순수 상태일 경우 density 연산자는 두 벡터의 곱 연산 $|\psi\rangle\langle\psi|$이나 파동함수 $|\psi\rangle$로 나타낼 수 있다. 본 고에서는 2-level 시스템만을 고려하며, 따라서 순수 상태의 파동함수, 또는 큐비트를 서로 직교하는 두 양자 상태 $|0\rangle$과 $|1\rangle$을 이용하여 다음과 같이 나타낼 수 있다.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

이 때, $|\alpha|^2 + |\beta|^2 = 1$이다. $|0\rangle$과 $|1\rangle$은 파울리 행렬 σ_z의 고유벡터로 각 각 +1과 −1의 고유치를 갖는다. 2-level 시스템에 대해 파울리 연산자는 다음과 같다.

$$I = \sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

고전 시스템에 존재하지 않는 양자 시스템만의 고유한 특징 중 하나는 얽힘(Entanglement)이다. 양자 정보 이론에서 다중 양자 시스템은 시스템들의 tensor 연산 $\otimes$을 통해 나타낼 수 있다. 얽힘은 두 시스템이 서로 분리될 수 없는 상태로 존재함을 의미하며, 수식으로 나타내면 임의의 양자 상태 $|a\rangle$와 $|b\rangle$를 이용하여 아래와 같은 식을 만족하는 양자 상태가 존재하지 않는 경우를 의미한다.

$$|\psi\rangle = |a\rangle \otimes |b\rangle$$

이렇게 서로 얽혀 있는 상태를 얽힌 큐비트 (entangled qubit)라고 한다. Entanglement는 얽힌 큐비트의 얽혀 있는 정도를 나타내는 척도이며, 특별히 두 시스템이 최대로 얽힌 경우 ebit으로 표현한다. 대표적인 ebit으로는 Bell 상태 또는 EPR 상태가 있으며 다음과 같은 4가지 상태로 구성된다.

$$|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), |\Phi_-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), |\Psi_+\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

1. 양자오류정정부호

양자 오류 정정 부호는 큐비트의 전송, 연산, 저장기간 동안 발생할 수 있는 오류로부터 양자 정보를 보호하는 기법이다. Shor의 9-큐비트 양자 오류 정정 부호 이후 대부분의 양자 오류 정정 부호는 임의의 큐비트를 보호하기 위해 양자 정보의 논리 상태를 더 큰 공간의 물리 상태의 부분 공간으로 변환시키는 기법을 사용하고 있다. 가장 많은 연구가 진행되고 있는 대표적인 양자 오류 정정 부호는 안정자 부호 (stabilizer code)이다. 안정자 부호는 그룹 이론을 바탕으로 파울리 연산자 그룹의 Abelian 그룹 연산자와 Abelian 그룹 연산자의 공통 고유벡터를 이용하여 양자 정보를 보호하는 기법이다. 다른 양자 부호 기법에 비해 안정자 부호 기법이 주목을 받는 이유는 안정자 부호는 고전 오류 정정 부호를 이용하여 양자 오류 정정 부호를 구성할 수 있는 방법을 제시하기 때문이다. 실제 안정자 부호 중 하나인 CSS 부호[3][4] 의 경우 고전 선형 오류 정정 부호 C와 C의 dual 부호 $C^{\perp}$을 이용하여 양자 오류 정정 부호를 설계하는 기법을 보여준다.

$[[n, k, d]]$ 안정자 부호는 k개의 논리 큐비트를 n개의 물리 큐비트에 부호화하고, $t = \lfloor d-1 \rfloor$개의 오류를 정정할 수 있다. 안정자 부호의 코드워드 $|\psi\rangle$는 안정자 그룹 S의 +1 고유치를 갖는 고유벡터 이므로 다음과 같은 식을 만족하다.

$$S_i|\psi\rangle = |\psi\rangle, \quad \text{for } S_i \in S$$

안정자 그룹 S를 형성하는 가장 적은 수의 독립적인 연산자를 안정자 생성 연산자 (stabilizer generator)라고 하며 $[[n, k, d]]$ 안정자 부호의 안정자 그룹은 $m = n - k$개의 생성 연산자를 이용하여 형성된다.

$$S = \langle S_1, S_2, \cdots, S_m \rangle$$

$[[n, k, d]]$ 안정자 부호 k개 Z논리 연산자와 k개의 X논리 연산자를 가지며, 코드워드 공간은 생성 연산자와 논리 연산 자 Z의 +1고유치를 갖는 공통 고유벡터에 논리 연산자X를 수행함으로써 전개된다.

2. 그래프

그래프 $G = (V, E)$는 두 집합, V와 E로 구성되어 있다. 이 때, V의 각 원소를 꼭짓점이라고 하며 E는 V의 두 원소를 연결하는 변의 집합이다. 꼭짓점 $a, b \in V$가 서로 변으로 연결되어 있는 끝 점일 때, 두 꼭짓점은 인접해 있는 상태이며 이러한 꼭짓점 사이의 인접한 상태는 그래프의 인접 행렬 (adjacency matrix) Γ_G를 이용하여 나타낼 수 있다. 만일 꼭짓점 집합 $V = \{a_1, \cdots a_N\}$가 N개의 원소로 구성되어 있다면, Γ_G는 다음

과 같은 $N \times N$대칭 행렬이다.

$$(\Gamma_G)_{ij} = \begin{cases} 1 & \text{if } (a_i, a_j) \in E \\ 0 & \text{otherwise.} \end{cases}$$

그래프의 각 꼭짓점은 변에 의해 연결된 이웃한 꼭짓점을 가지고 있다. 꼭짓점 a와 이웃한 꼭짓점의 집합 (neighborhood) $N_a \subset V$는 $(a,b) \in E$을 만족하는 꼭짓점 b의 집합으로 정의된다. 〈그림 1〉은 간단한 링 그래프를 나타내고 있다. 이 그림에서 V는 총 6개의 원소로 구성되어 있으며 $E = \{(1,2),(2,3),(3,4),(5,6),(5,1)\}$이다. 따라서 이 경우 6×6 인접 행렬Γ_G은 다음과 같다.

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

3. 그래프 상태 (Graph state)

그래프 상태는 그래프 $G = (V, E)$를 바탕으로 구성되는 양자 상태로 힐버트 공간 $H_V = (\mathbb{C}^2)^V$에 존재하는 특정 순수 양자 상태이다[16][17]. 그래프 상태에서 그래프의 각 꼭짓점은 큐비트에 해당하며 각 꼭짓점은 다음과 같은 Hermitian 연산자를 고려할 수 있다.

$$K_G^{(a)} = \sigma_x^{(a)} \prod_{b \in N_a} \sigma_z^{(b)} \quad (1)$$

이 때, $\sigma_i^{(a)}$는 a꼭짓점에 해당하는 큐비트에서 수행되는 파울리 연산자를 의미한다. 그리고 이 연산자는 인접 행렬에 의해 다음과 같은 식으로 표현할 수 있다.

$$K_G^{(a)} = \sigma_x^{(a)} \prod_{b \in N_a} (\sigma_z^{(b)})^{\Gamma_{ab}} \quad (2)$$

$K_G^{(a)}$는 꼭짓점 a와 a의 이웃점 $b \in N_a$로 구성된 큐비트의 observable이며 $K_G^{(a)}$는 총 $|V|$개가 존재하고 각 연산자는 서로 commute한 관계에 있다. $K_G^{(a)}$는 꼭짓점 집합 V와 관련된 큐비트 시스템의 완벽한 Abelian observable 집합을 정의하게 된다. 따라서, $K_G^{(a)}$는 공통의 고유벡터, 그래프 상태를 갖게 되며, 그래프 상태는 힐버트 공간의 기저벡터를 구성하게 된다. 그래프 상태 중 +1의 고유치를 갖는 $K_G^{(a)}$의 고유벡터를 $|s\rangle$라고 하면, 그래프 상태 $|s\rangle$는 모든 꼭짓점 a에 대해 다음과 같은 관계를 만족한다.

$$K_G^{(a)}|s\rangle = |s\rangle$$

안정자 부호 [2]와 비교해서 생각해보면, $K_G^{(a)}$는 $|s\rangle$의 안정 연산자로 간주할 수 있으며, 따라서 다음과 같은 식으로 구성된 Abelian 그룹은 그래프 상태 $|s\rangle$의 안정자 그룹이 된다.

$$S_G = \langle \{K_G^{(a)}\}_{a \in V} \rangle$$

따라서, 안정자 그룹의 모든 원소는 아래와 같은 식을 만족한다.

$$S|s\rangle = |s\rangle, \quad S \in S_G$$

위와 같이 그래프 상태를 바탕으로 구성된 양자 오류 정정 부호는 그래프 부호라고 한다. 그래프 부호의 코드워드는 연속되는 유니터리 연산자를 $|x,+\rangle^{\otimes V}$에 적용하여 얻을 수 있다.

$$|s\rangle = \prod_{(a,b) \in E} U^{(a,b)} |x,+\rangle^{\otimes V} \quad (3)$$

이 때, $|x,+\rangle$는 σ_x에 +1 고유치를 갖는 고유벡터를 의미하고, $U^{(a,b)}$는 σ_z의 ± 1 고유벡터 방향으로의 정사영 연산자 $P_{z,\pm}$에 의해 다음과 같이 정의 된다.

$$U^{(a,b)} = P_{z,+}^{(a)} \otimes I^{(b)} + P_{z,-}^{(a)} \otimes \sigma_z^{(b)}$$

4. CWS 부호 기법

CWS 부호 기법 [13]은 additive 양자 오류 정정 부호와 non-additive 양자 오류 정정 부호를 설계할 수 있는 기법을 제공한다. 모든 CWS 부호는 standard form으로 표현될 수 있는데, standard form의 CWS 부호는 그래프 상태를 이용하여 기존의 이진 오류 정정 부호로부터 양자 오류 정정 부호를 구성할 수 있는 방법을 제시한다. 이 때, 그래프의 꼭짓점은 각 각 코드워드의 n 큐비트에 대응된다.

CWS 부호는 크게 word stabilizer와 word operator, base state로 구성된다. Word stabilizer는 파울리 그룹 P_n의 부분 공간으로 Abelian 그룹을 형성하며, base state는 word stabilizer 의 +1 고유치를 갖는 공통 고유벡터이다. CWS 부호의 코드워드 공간을 구성하는 기저 벡터는 base state에 word operator를 수행함으로 얻게 된다. Standard form의 CWS 부호에서 word stabilizer는 그래프를 이용하여 다음과 같은 형태의 연산자 집합으로 구성된다.

$$g_i = X_i Z^{r_i} \quad (4)$$

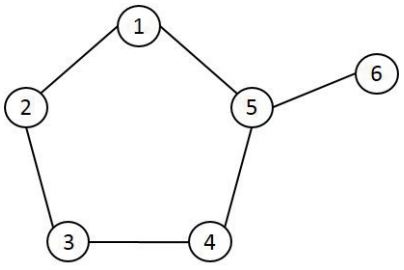

그림.1 6개의 꼭짓점을 연결하는 변으로 구성된 그래프

이 때, r_l는 그래프의 인접 행렬을 의미한다. 따라서, standard form에서 CWS 부호의 base state는 그래프 상태와 동일한 벡터이다. [18] CWS 부호의 코드워드 공간은 기저벡터의 집합으로 구성되며, 각 각의 기저벡터는 base state에 word operator를 적용하여 얻게 된다. 따라서, 코드워드 공간의 크기는 word operator의 개수에 의해 결정된다.

일반적으로 additive 부호의 경우 코드워드 공간의 크기는 2의 지수의 값을 갖는 반면 non-additive 부호의 경우 그렇지 않은 경우가 많다. n개의 물리 큐비트에 K크기의 코드워드 공간으로 구성된 minimum distance d인 non-additive 부호는 $((n, K, d))$로 표현한다. Non-additive 부호와 동일한 표현 방법을 이용하여 $[[n, k, d]]$ additive 부호를 나타내면 $((n, 2^k, d))$부호가 된다.

Word operator는 한 개 이상의 word stabilizer와 anti-commute하다. 따라서 word operator에 의해 구성된 벡터는 base state와 서로 직교한다. Word operator에 의해 구성된 벡터가 서로 직교하도록 word operator를 선택하는 것이 가능하며 따라서 word operator에 의해 구성된 서로 직교하는 벡터는 코드워드 공간의 기저벡터로 사용된다.

CWS 부호, 특히 standard form의 CWS 부호의 중요한 특징은 정정 가능한 어떤 오류 형태라도 Z연산자와 I연산자로만 구성된 오류 형태로 변환이 가능하다는 것이다. [13] 이런 변환에 의해 얻게 된 effective 오류는 두 종류의 파울리 연산자로 구성되어 있기 때문에 각 각의 effective오류는 이진 오류로 대응이 가능하다. 따라서 임의의 파울리 오류 $E = \pm Z^v X^u$와 이진 오류 사이의 관계는 다음과 같은 식으로 정의할 수 있다.

$$Cl_G(E = \pm Z^v X^u) = v \otimes \bigoplus_{l=1}^{n} u_l r_l$$

이 때, r_l은 그래프 인접 행렬의 l번째 행을 나타내며, u_l은 벡터 u의 l번째 비트를 의미한다. 예를 들어 $n = 4$이고 단순한 링 그래프로 정의된 CWS 부호를 고려해 보면, standard form 형태의 CWS 부호의 word stabilizer는 다음과 같다.

$$XZIZ \;\; ZXZI \;\; IZXZ \;\; ZIZX$$

이 때 양자 채널에서 오류 $E = XIII$가 발생한다면 E는 word stabilizer에 의해 다음과 같은 effective 오류로 변환된다.

$$E \cdot XZIZ \;=\; IZIZ$$

변환된 effective 오류는 Z와 I의 두 종류의 연산자로만 구성되어 있으며, Z와 I는 각 각 1과 0에 대응된다. 결론적으로 위의 양자 오류와 이진 오류 사이의 변환식을 이용하여 오류 $E = XIII$은 다음과 같이 이진 오류로 변환 된다.

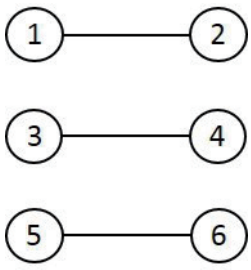

그림 2. 6-큐비트 그래프 상태.

$$Cl_G(E = XZIZ) \;=\; 0101$$

위의 양자 오류와 고전 이진 오류 사이의 대응 관계에 대한 정의를 이용함으로써 standard form의 CWS 부호는 아래에 오는 조건을 만족할 경우 그래프 G와 양자 오류 집합 $\mathcal{E}$에 대응하는 이진 오류 $Cl_G(\mathcal{E})$를 정정할 수 있는 고전 이진 오류 정정 부호 C_b에 의해 정의될 수 있다. 각 각의 $E \in \mathcal{E}$에 대해 word stabilizer에 의해 유도된 오류를 수정할 수 있는 고전 오류 정정 부호 C_b가 존재하고 아래의 조건을 만족할 경우 양자 오류 정정 부호를 구성할 수 있다.

$$\text{either} \quad Cl_G(E) \neq 0$$

$$\text{or, for each } i, \quad Z^{c_i} E = E Z^{c_i}$$

이 때, Z^{c_i}는 고전 이진 오류 정정 부호 C_b에 의해 구성된 word operator,

$$W = \{Z^c\}_{c \in C_b}$$

를 의미한다. 따라서 word operator는 고전 이진 오류 정정 부호로부터 전개될 수 있다.

5. 6-큐비트 양자 오류 정정 부호

Standard form의 CWS 부호가 갖는 effective 오류 변환은 standard form CWS 부호가 그래프를 바탕으로 구성되어 있기 때문이다. 식(1)과 식(2)로 표현되는 그래프 상태의 Hermitian 연산자는 standard form CWS의 word stabilizer 식(4)와 동일한 형태임을 확인할 수 있다. CWS 부호의 경우 대부분 링 그래프를 바탕으로 word stabilizer가 구성되어 있지만 standard form CWS 부호가 그래프 부호와 동일한 형태를 가지고 있기 때문에 다양한 형태의 그래프를 바탕으로 구성된 그래프 상태에 CWS 부호의 effective 오류를 적용하는 것이 가능하다. 이 경우 Word stabilizer는 그래프 G의 변의 집합 E에 따라 결정되기 때문에 E의 원소, 즉 그래프의 모양에 따라 실제 채널에서 발생하는 양자 오류는 다양한 형태의 effective 오류로 변환이

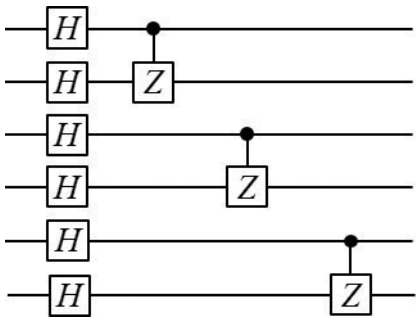

그림 3. Hadamard 게이트와 Controlled-Z 게이트로 구성된 6-큐비트 그래프 부호의 부호화 서킷

가능하다.

본 고에서 고려하는 그래프의 형태는 임의의 꼭짓점에 인접한 꼭짓점이 오직 하나인 경우로만 구성되어 있다. 이 경우, 임의의 꼭짓점 $a \in V$에 대해 이웃한 꼭짓점의 개수는 $|N_a| = 1$이다. 6-큐비트의 경우를 생각해보면 그래프의 모양은 〈그림 2〉와 같다. 그래프의 꼭짓점은 $|V| = 6$으로 구성되어 있으며, 변의 집합 E의 원소는 $\{(1,2)(3,4)(5,6)\}$로 구성된다. 식(1)과 식(2) 또는 식(4)에 따라 안정 연산자를 구성하면, 6-큐비트 그래프 상태의 안정 연산자는 다음과 같다.

$$\begin{matrix} XZIIII & IIXZII & IIIIXZ \\ ZXIIII & IIZXII & IIIIZX \end{matrix} \quad (5)$$

6-큐비트 그래프 상태 또는 6-큐비트 standard form CWS 부호의 base state는 식(3)을 이용하여 구할 수 있다. 이 때, 유니터리 연산자는 아래와 같이 정의된다.

$$U^{(1,2)} = |0\rangle\langle 0|^{(1)} \otimes I^{(2)}IIII + |1\rangle\langle 1|^{(1)} \otimes \sigma^{(2)}IIII$$

$$U^{(3,4)} = II|0\rangle\langle 0|^{(3)} \otimes I^{(4)}II + II|1\rangle\langle 1|^{(3)} \otimes \sigma^{(4)}II$$

$$U^{(5,6)} = IIII|0\rangle\langle 0|^{(5)} \otimes I^{(6)} + IIII|1\rangle\langle 1|^{(5)} \otimes \sigma^{(6)}$$

따라서 6-큐비트 그래프 상태의 부호화 서킷은 〈그림 3〉과 같이 구성할 수 있다. 6-큐비트 그래프 부호는 식(5)와 같이 독특한 형태의 word stabilizer를 가지고 있다. 이를 이용하여 채널에서 발생하는 모든 단일 오류를 Z와 I연산자로 구성된 이진 형태의 오류로 변환하면 다음과 같은 오류 집합을 얻을 수 있다.

$$\begin{matrix} Z_1 = ZIIIII & X_1 = IZIIII & Y_1 = ZZIIII \\ Z_2 = IZIIII & X_2 = ZIIIII & Y_2 = ZZIIII \\ Z_3 = IIZIII & X_3 = IIIZII & Y_3 = IIZZII \\ Z_4 = IIIZII & X_4 = IIZIII & Y_4 = IIZZII \\ Z_5 = IIIIZI & X_5 = IIIIIZ & Y_5 = IIIIZZ \\ Z_6 = IIIIIZ & X_6 = IIIIZI & Y_6 = IIIIZZ \end{matrix}$$

위의 오류 집합은 중복된 연산자를 가지고 있으며, 따라서 실제 채널에서 발생한 오류 중 코드워드에 영향을 미치는 오류는 아래와 같은 effective 오류의 집합과 등가 관계를 갖는다.

$$\begin{matrix} ZIIIII & IZIIII & IIZIII \\ IIIZII & IIIIZI & IIIIIZ \\ ZZIIII & IIZZII & IIIIZZ \end{matrix}$$

CWS 부호는 이진 오류로부터 word operator를 구할 수 있는 방법을 제시한다. 따라서, 위의 오류 집합으로부터, 관련된 이진 오류를 검출할 수 있는 고전 이진 오류 정정 부호를 구할 수 있다. 그리고 고전 이진 오류 정정 부호를 이용하여 word operator을 구하면 다음과 같은 연산자를 얻을 수 있다.

$$\begin{matrix} IIIIII & IIIZIZ & IIZIZI & IIZZZZ \\ IZZZZI & ZIIIZI & ZIIZZZ & ZIZIII \\ ZZIZZI & ZZZIIZ & ZZZZII & IZZIZZ \\ ZIZIII & IZIZII & ZIZZIZ & ZZIIZZ \end{matrix}$$

CWS 부호에서 코드워드 공간의 크기는 word operator와 동일하다. 따라서 6-큐비트 그래프 부호의 코드워드 공간의 크기는 16이 된다. 다시 말해 6-큐비트 그래프 부호는 [[6,4,2]] additive 부호이다. 양자 오류 정정 부호의 singleton bound

$$n - k \geq 2(d-1)$$

에 대입해 검토해 보면 [[6,4,2]]부호는 singleton bound를 만족하는 부호이다.

Ⅲ. 결 론

본 고에서는 양자 오류 정정 부호의 설계 기법에 대해 살펴보았다. 그래프에 대한 일반적인 내용을 살펴보았으며, 그래프 상태를 이용하여 안정자 연산자와 논리 연산자를 정의하고 이를 이용하여 양자 오류 정정 부호를 설계하는 방법을 소개하였다. 그래프 상태를 이용하는 대표적인 양자 오류 정정 부호 설계 기법으로 CWS 부호 설계 기법을 살펴보고, 양자 오류를 이진 오류로 변환하여 고전 오류 정정 부호와 그래프 상태를 이용하여 양자 오류 정정 부호를 설계하는 CWS 부호의 특징을 소개하였다. 그래프 부호와 CWS 부호의 특징을 이용하여 4개의 논리 큐비트를 6개의 물리 큐비트에 부호화 할 수 있는 양자 오류 정정 부호를 설계하였으며, 본 고에서 설계된 양자 오류 정정 부호가 singleton bound를 만족하는 양자 오류 정정 부호이며,

기존 기법으로 설계할 수 없었던 새로운 양자 오류 정정 부호임을 알았다. 하지만 본 고에서 설계된 양자 오류 정정 부호는 그 크기가 6 큐비트로 제한되어 있기 때문에 차후에 보다 큰 크기의 코드워드 큐비트 갖는 설계 기법에 대한 연구가 필요하다.

참 고 문 헌

[1] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," Phys. Rev. A, vol. 52, no. 4, pp. R2493-R2496, Oct. 1995.

[2] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, Caltech Ph.D. dissertation, Psadena, CA, May 1997.

[3] A. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," Phys. Rev. A, vol. 54, no. 2, pp. 1098-1105, Aug. 1996.

[4] A. Steane, "Multiple-Particle Interference and Quantum Error Correction," Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, vol. 452, no. 1954, pp. 2551-2577, 1996.

[5] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," Phys.Rev. A, vol. 56, pp. 33-38, Jul. 1997.

[6] A. Y. Kitaev, "Quantum Error Correction with Imperfect Gates," Quantum Communication, Computing, and Measurement, no. Chapter 19, pp. 181-188, 1997.

[7] A. Calderbank, E. M. M. Rains, P. W. Shor, and N. Sloane, "Quantum error correction via codes over GF(4)," IEEE Transactions on Information Theory, vol. 44, no. 4, pp. 1369-1387, Jul. 1998.

[8] M. Grassl and T. Beth, "A note on non-additive quantum codes," arXiv preprint quant-ph, 1997.

[9] E. M. M. Rains, R. H. Hardin, P. W. Shor, and N. Sloane, "Nonadditive Quantum Code," Phys. Rev. Lett., vol. 79, no. 5, pp. 953-954, Aug. 1997.

[10] M.Grassl and M.Rotteler, "Non-additive quantum codes from Goethals and Preparata codes," Information Theory Workshop, 2008. ITW '08. IEEE, pp. 396-400, May 2008.

[11] ——, "Quantum Goethals-Preparata codes," Information Theory, 2008. ISIT 2008. IEEE International Symposium on, pp. 300-304, Jul. 2008.

[12] S. Yu, Q. Chen, C.-Y. Lai, and C. H. Oh, "Nonadditive Quantum Error-Correcting Code," Phys. Rev. Lett., vol. 101, no. 9, p. 090501, Aug. 2008.

[13] A. Cross, G. Smith, J. A. Smolin, and B. Zeng, "Codeword Stabilized Quantum Codes," IEEE Transactions on Information Theory, vol. 55, no. 1, pp. 433-438, Jan. 2009.

[14] J. Shin, J. Heo, and T. A. Brun, "Entanglement-assisted codeword stabilized quantum codes," Phys. Rev. A, vol. 84, p. 062321, Dec. 2011.

[15] M. Van den Nest, J. Dehaene, and B. De Moor, "Graphical description of the action of local Clifford transformations on graph states," Phys. Rev. A, vol. 69, no. 2, p. 022316, Feb. 2004.

[16] M. Hein, J. Eisert, and H. J. Briegel, "Multiparty entanglement in graph states," Phys. Rev. A, vol. 69, p. 062311, Jun. 2004.

[17] S. Yu, Q. Chen, and C. H. Oh. (2007, Sep.) Graphical Quantum Error-Correcting Codes. Online available at http://arxiv.org/abs/0709.1780v1

[18] D. Schlingemann and R. F. Werner, "Quantum error-correcting codes associated with graphs," Phys. Rev. A, vol. 65, p. 012308, Dec. 2001.

[19] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Online available at http://www.codetables.de, 2007.

약 력

신 정 환

2005년 건국대학교 공학사
2007년 건국대학교 공학석사
2012년 고려대학교 공학박사
2012년~현재 고려대학교 BK21사업단 연구 교수
2013년~2015년 University of Southern California 방문 교수
관심분야: 양자 정보 이론, 통신 시스템

허 준

1989년 서울대학교 공학사
1991년 서울대학교 공학석사
2002년 University of Southern California 공학박사
1991년~1997년 LG전자 책임연구원
2003년~2007년 건국대학교 전자공학과 교수
2007년~현재 고려대학교 전기전자공학부 교수
관심분야: 이동통신 이론, 오류정정부호, 양자암호, 양자오류정정부호