편집위원 : 김동기, 임용재 (방송통신위원회)

양자 오류 정정 부호의 개요

허 준, 신정환
고려대학교

요 약

본고에서는 양자 정보 처리 시스템에서 사용되는 양자 오류 정정 부호에 대해서 알아본다. 양자 오류 정정 부호는 디지털 정보가 아닌 연속적인 값을 갖는 양자 정보의 오류를 수정하는 기법으로 기존의 고전 오류 정정 부호를 적용할 수 없는 양자 정보 시스템에서 사용되는 오류 정정 부호이다. 본 논문에서는 최근 가장 활발하게 사용되고 있는 안정 부호를 중심으로 양자 오류 정정 부호의 구성 및 기존 오류 정정 부호와의 관계를 살펴본다.

Ⅰ. 서 론

양자 역학이 시작된 이후 100년이 지난 지금 더 빠른 정보 처리를 위해 양자 컴퓨터를 기반으로 하는 양자 정보 시스템이 세계 각 국에서 연구되고 있다. 양자 정보 시스템은 기존 전산 시스템의 이진 정보에서 벗어나 연속적인 값을 갖는 양자 정보를 이용하는 시스템으로 다양한 분야에 적용 가능할 것으로 보여진다. 특히, 양자 컴퓨터의 가능성이 제시된 이후 1994년 피터 쇼어는 소인수 분해 과정에 양자 컴퓨터를 이용할 경우 고전 역학에 기반한 컴퓨터로는 수행할 수 없는 고속의 처리가 가능함을 보였다. 그 이후 그로버의 데이터 검색 알고리즘은 쇼어의 소인수 분해 알고리즘과 더불어 양자 정보의 병렬 처리 특성을 이용하여 양자 컴퓨터의 가능성을 보여주고 있다. 이러한 양자 시스템의 고속 데이터 처리는 기존 시스템으로는 해결하기 어려운 많은 문제들의 해결 수단이 되기도 하지만 복잡한 수학 문제에 기초한 기존 보안체계에는 상당한 위험으로 작용한다. 양자 컴퓨터를 이용할 경우 복잡한 보안키가 단시간에 해독될 수 있기 때문이다. 양자 컴퓨터가 가지고 있는 강력한 잠재력으로 인해 세계 각 국에서는 앞다투어 양자 정보 시스템을 연구하고 있다.

양자 알고리즘은 시스템의 연산 과정 중에 오류가 발생하지 않음을 가정하고 있다. 하지만 오류가 없는 양자 시스템을 구성하기는 상당히 어려운 일이다. 심지어 양자 정보는 저장되어 있는 순간에도 시간이 흐름에 따라 외부와 상호 작용하여 정보가 변형될 수 있다. 따라서 이러한 외부 환경과의 상호 작용 및 연산에서 발생할 수 있는 오류로부터 정보를 보호할 수 있는 기법이 필요하다. 양자 오류 정정 부호 기법은 양자 시스템에서 사용되는 오류 정정 부호 기법이다. 이미 기존 시스템에서 사용되는 훌륭한 오류 정정 부호가 많이 연구되어 있지만 근본적으로 양자 정보는 기존 이진 정보와 다른 특성을 가지고 있기 때문에 기존 오류 정정 부호를 양자 시스템에 적용하기는 쉽지 않다.

본 논문에서는 최근 가장 많은 연구가 진행되고 있는 안정 부호[1]를 중심으로 양자 오류 정정 부호의 구성을 살펴본다.

Ⅱ. 본 론

1. 양자 정보

양자 정보 시스템은 양자 비트(quantum bit), 줄여서 큐비트(qubit)를 정보의 기본 단위로 사용한다. 이는 고전 디지털 정보 시스템에서 정보의 최소 단위로 비트(bit)를 사용하는 것과 유사하다. 하지만 큐비트는 여러 측면에서 기존 비트와는 다른 특성을 가지고 있는데 그 중 가장 큰 차이점은 정보의 중첩이 가능하다는 것이다. 기존 이진 정보는 '0'과 '1'의 두 가지 상태를 가질 수 있으며, 두 상태 중 하나의 상태로 현재 값이 결정된다. 반면, 양자 정보는 '0'과 '1' 각 각의 상태로 존재할 수 있을 뿐만 아니라 '0'과 '1'이 동시에 존재하는 상태로도 존재할 수 있다. 다시 말해 큐비트는 두 가지 상태를 갖는 시스템에서 두 상태의 중첩된 형태로 표현된다. 간단한 예로 원자의 상태를 큐비트를 이용하여 나타내면 다음과 같다. 원자의 스핀 방향이 위로 향하는 경우를 '↑' 로, 스핀 방향이 아래로 향하는 경우를 '↓' 로 표시하면, 원자의 상태를 나타내는 큐비트는 디렉(Dirac)의 표현 식에 의해 다음과 같이 나타낼 수 있다.

$$|\psi\rangle = a|\uparrow\rangle + b|\downarrow\rangle$$

이 때, $|\cdot\rangle$은 벡터를 나타내며 a와 b는 각각 원자를 측정했을 때 측정 결과 스핀의 방향이 위로 향하는 경우와 아래로 향하는 경우에 해당하는 확률과 관련된 값이다. 엄밀히 말해 위 식에서 원자 상태를 측정했을 경우 스핀의 방향이 위를 향하는 값을 얻을 확률은 $|a|^2$이며, 측정 결과 스핀의 방향이 아래로 향할 경우의 확률은 $|b|^2$이다. 따라서 위 식에서 a와 b의 관계는 다음과 같다.

$$|a|^2 + |b|^2 = 1$$

원자의 상태를 나타내는 큐비트의 예에서 살펴본 것처럼 큐비트는 벡터 공간의 임의의 벡터로 정의되며 각 상태의 확률과 관련된 값은 복소수이다. 추가로 이 벡터 공간의 내적을 정의하면, 큐비트는 수학적으로 내적이 정의된 복소수 벡터 공간, 즉 힐버트 공간(Hilbert space)에 존재하는 임의의 벡터로 나타낼 수 있다. 앞의 원자의 예에서 $|\uparrow\rangle$와 $|\downarrow\rangle$는 2차원 힐버트 공간의 서로 직교인 기저 벡터를 의미하며, 일반적으로 $|0\rangle \equiv |\uparrow\rangle$와 $|1\rangle \equiv |\downarrow\rangle$로 나타낼 수 있다. 이를 이용하여 원자의 상태 $|\psi\rangle$를 다시 나타내면

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

와 같으며, 이 때 a와 b는 복소수이고, $|a|^2 + |b|^2 = 1$을 만족한다.

앞 원자의 예에서 원자의 스핀은 처음 두 방향의 중첩으로 이루어져 있지만 측정 후 상태는 각 방향의 확률에 따라 위와 아래의 방향 중 하나의 상태가 되는 것을 언급했다. 이는 양자의 상태, 또는 큐비트는 측정에 의해 측정 전의 상태와 측정 후의 상태가 다를 수 있음을 의미하며, 이러한 측정에 의한 정보의 붕괴는 양자 정보가 갖는 또 다른 특징 중의 하나이다. 임의의 양자 상태 $|\psi\rangle = a|0\rangle + b|1\rangle$을 벡터 $|0\rangle$과 벡터 $|1\rangle$방향으로 측정할 경우, 측정 후 상태는 각각 $|a|^2$와 $|b|^2$의 확률로 $|0\rangle$ 또는 $|1\rangle$이 된다.

양자 정보가 갖는 또 다른 특징은 얽힘 (Entanglement) 이다. 얽힘은 고전 정보가 갖지 못하는 양자 정보만의 특징으로 두 개 이상의 시스템에 걸쳐 있는 큐비트에 대해 한 시스템에서의 측정 결과가 다른 시스템의 측정 값을 결정하는 것을 의미한다. 다시 말해 두 시스템 AB 위에 있는 임의의 상태 $|\psi\rangle$에 대해 각 각의 시스템 A와 시스템 B에 있는 상태 $|a\rangle$와 $|b\rangle$로 분리되어 표현될 수 없는 경우, 즉 $|\psi\rangle = |a\rangle|b\rangle$로 나타낼 수 없는 경우 $|\psi\rangle$를 얽힌 상태라고 한다. 대표적인 얽힌 상태로는 EPR 상태 또는 Bell 상태가 있으며 다음과 같은 4가지 상태로 구성되어 있다.

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

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

위의 4가지 상태는 2-큐비트 상태이지만 두 개의1-큐비트 상태로 분리될 수 없는 것을 확인할 수 있다. Bell 상태에서 앞 큐비트 상태의 측정은 언제나 뒤에 있는 큐비트의 상태를 결정하게 된다. 첫 번째 Bell 상태의 경우를 살펴보면, 앞 큐비트의 측정 값이 '0'일 경우 뒤에 있는 큐비트는 측정하지 않아도 그 측정 값이 '0'으로 결정되며, 앞 큐비트의 측정 값이 '1'일 경우 뒤 큐비트는 '1'로 결정되는 것을 알 수 있다.

닫힌 계에서 양자 상태에 대한 연산자의 입력과 출력의 크기는 언제나 같아야 한다. 고전 정보의 경우 두 정보의 입력이 하나의 결과를 출력하거나 하나의 입력이 두 개의 정보로 출력될 수 있지만 (예를 들어 AND 연산자는 두 입력 값을 비교하여 하나의 값을 출력한다), 양자 연산은 언제나 입력과 출력의 크기가 동일해야 한다. 추가적으로, 닫혀 있는 계에서 양자 상태의 변화는 유니터리 연산자로 정의된다.

마지막으로 양자 정보가 갖는 또 다른 특징은 양자 정보는 복사가 불가능하다는 것이다. 이는 임의의 양자 정보를 복사할 수 있는 유니터리 연산자가 존재하지 않음을 의미한다.

2. 양자 오류 정정 부호

여러 양자 알고리즘은 연산과정에서 오류가 존재하지 않음을 가정하고 있다. 하지만, 양자 연산 과정의 오류는 피할 수 없는 현상이다. 뿐만 아니라 양자 채널을 이용한 통신에서도 채널에 의한 오류는 언제나 발생하며, 심지어 양자 정보는 정보가 저장되어 있는 순간에도 외부 환경과 반응하여 변형될 수 있다. 따라서 양자 정보 처리 및 통신에서는 발생 가능한 다양한 오류로부터 양자 정보를 보호 할 수 있는 기법이 필요하다.

기존 시스템에는 이미 다양한 오류 정정 기법이 존재한다. 하지만 이런 기존의 오류 정정 기법은 직접적으로 양자 시스템에 적용될 수 없다. 그 이유는 고전 오류와는 다르게 양자 정보에서 발생하는 오류는 연속적인 값을 취하기 때문이다. 또한 앞에서 살펴본 것처럼, 큐비트는 복사가 불가능하며 측정에 의해 정보가 붕괴되는 특징을 가지고 있다. 따라서, 양자 시스템에 적용할 수 있는 고유한 오류 정정 부호 기법이 필요하다.

Shor 부호

양자 오류 정정 부호는 양자 연산자 또는 양자 채널에서 발생하는 오류로부터 양자 정보를 보호하는 기술이다. 최초의 양자

오류 정정 부호는 1992년 Peter Shor에 의해 소개되었다 [4]. Shor는 자신의 논문에서9-큐비트를 이용하여 Pauli 채널에서 발생할 수 있는 단일 오류로부터 1-큐비트 정보를 보호할 수 있는 기법을 제시하였다. Pauli 채널은 채널에서 발생하는 오류 연산자가 Pauli 연산자로 정의된 오류 채널로 1-큐비트 시스템에 대한 Pauli 연산자는 다음과 같다.

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

각 연산자의 특징을 살펴보면, X연산자는 각 기저에 대해

$$X|0\rangle=|1\rangle,\quad X|1\rangle=|0\rangle$$

와 같은 연산을 수행하며, 고전 비트 플립 연산자와 유사한 결과를 보여준다. Z 연산자는 기저 사이의 페이즈에 영향을 주는 연산자로 그 결과는 다음과 같다.

$$Z|0\rangle=|0\rangle,\quad Z(\pm|1\rangle)=\mp|1\rangle$$

Y 연산자는 X 연산자와 Z 연산자가 연속적으로 수행된 것과 동일한 연산을 수행한다. Shor 부호는 각 오류에 대한 단계적인 오류 수정 과정을 통해 연속적인 오류로부터 정보를 보호하는 과정을 보여준다. 이러한 특징은 Shor 부호의 구조로부터 쉽게 접근할 수 있는데 Shor 부호의 구조를 살펴보면 비트 플립 오류를 수정할 수 있는 연산자와 페이즈 플립을 수정할 수 있는 연산자의 결합으로 구성되어 있는 것을 확인할 수 있다. 따라서, 3-큐비트 비트 플립 부호와 3-큐비트 페이즈 플립 부호를 통해 Shor 부호를 쉽게 이해할 수 있다.

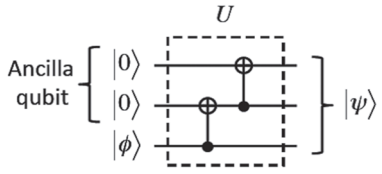


그림 1. 3-큐비트 비트 플립 부호의 부호화 서킷

(1) 3-큐비트 비트 플립 부호

3-큐비트 비트 플립 부호는 채널에서 발생하는 단일 X 오류로부터 정보를 보호할 수 있는 양자 오류 정정 부호이다. 3-큐비트 비트 플립 부호의 구조는 기존 오류 정정 부호 중 반복 부호와 유사한 모양을 가지고 있다. 3-큐비트 비트 플립 부호는 1개의 1-큐비트 정보를 3-큐비트 구성된 공간으로 부호화 하며, 부호화 과정은 다음과 같다.

$$|0\rangle\rightarrow|000\rangle,\quad |1\rangle\rightarrow|111\rangle$$

따라서 임의의 1-큐비트 $|\phi\rangle=a|0\rangle+b|1\rangle$는 부호화 과정을 통해 $|\psi\rangle=a|000\rangle+b|111\rangle$가 된다. 3-큐비트 비트 플립 코드에 의해 부호화된 코드워드는 단일 X 오류 채널을 통해 수신자에게 전송되는 과정에서 X 오류가 발생한 위치에 따라 아래의 4가지 경우 중 하나의 상태로 수신자에게 전송된다.

$$|\psi_0\rangle=a|000\rangle+b|111\rangle$$
$$|\psi_1\rangle=a|100\rangle+b|011\rangle$$
$$|\psi_2\rangle=a|010\rangle+b|101\rangle$$
$$|\psi_3\rangle=a|001\rangle+b|110\rangle$$

이 때, $|\psi_0\rangle$은 채널에서 오류가 발생하지 않은 경우를 나타내며, $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$은 각각 1번 째, 2번 째, 3번 째 큐비트에서 X 오류가 발생한 경우를 의미한다.

3-큐비트 비트 플립 부호의 복호 과정은 Projection 연산자를 통해 수행된다. 오류 채널을 통해 전송된 코드워드는 오류가 발생한 위치에 따라 서로 직교인 부분 공간 (subspace)에 존재하는 벡터가 된다. 따라서, 전송된 정보를 서로 직교인 부분 공간으로 투영함으로써 오류의 유무 및 발생한 위치를 확인 할 수 있다.

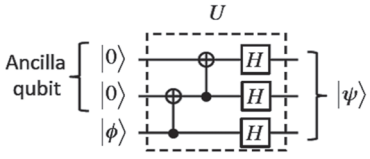


그림 2. 3-큐비트 페이즈 플립 부호의 부호화 서킷

실제 3-큐비트 비트 플립 부호의 Projection 연산자를 살펴보면 다음과 같다.

$$P_0=|000\rangle\langle 000|+|111\rangle\langle 111|$$
$$P_1=|100\rangle\langle 100|+|011\rangle\langle 011|$$
$$P_2=|010\rangle\langle 010|+|101\rangle\langle 101|$$
$$P_3=|001\rangle\langle 001|+|110\rangle\langle 110|$$

이 때, 각 연산자는 코드워드를 오류가 발생한 위치에 해당하는 공간으로 투영하는 연산을 수행한다.

3-큐비트 비트 플립 부호의 또 다른 복호 기법은 각 큐비트를 비교하여 오류가 발생한 위치를 확인하는 것이다. 오류가 없는 상태에서 코드워드의 각 큐비트는 서로 같은 상태로 구성되어 있다. 코드워드의 첫 번째 상태와 두 번째 상태는 '$|00\rangle$'과 '$|11\rangle$'로 서로 동일한 값을 갖는다. 만일 첫 번째 큐비트에 X 오류가

발생할 경우 첫 번째 상태와 두 번째 상태는 각 각 $|10\rangle$과 $|01\rangle$'로 변경되고, 이 때 각 위치의 상태는 서로 다른 값을 갖게 된다. 따라서, 각 위치의 큐비트가 동일한 상태인지 비교함으로써 오류의 발생 유무 및 위치를 확인 할 수 있다. ZZI와 IZZ는 코드워드의 각 큐비트를 비교하는 연산자이다. ZZI는 첫 번째 큐비트와 두 번째 큐비트를 비교하며 IZZ는 두 번째 큐비트와 세 번째 큐비트를 비교한다. 두 측정 연산자에 의한 연산의 결과는 오류가 발생한 위치에 따라 다르며 연산의 결과는 다음과 같다.

$$\langle\psi_0|ZZI|\psi_0\rangle=1,\ \langle\psi_0|IZZ|\psi_0\rangle=1$$
$$\langle\psi_1|ZZI|\psi_1\rangle=0,\ \langle\psi_1|IZZ|\psi_1\rangle=1$$
$$\langle\psi_2|ZZI|\psi_2\rangle=0,\ \langle\psi_2|IZZ|\psi_2\rangle=0$$
$$\langle\psi_3|ZZI|\psi_3\rangle=1,\ \langle\psi_3|IZZ|\psi_3\rangle=0$$

오류가 발생한 위치에 따라 두 연산자의 수행 결과는 서로 다른 패턴을 취하게 되며, 이는 고전 선형 오류 정정 부호의 신드롬 패턴과 유사한 형태임을 알 수 있다. 따라서 두 연산자에 의한 신드롬 패턴을 통해 코드워드에 발생한 오류의 유무 및 위치를 확인할 수 있으며, 각 신드롬에 해당하는 오류의 역 연산을 수행함으로써 정보를 복원하게 된다.

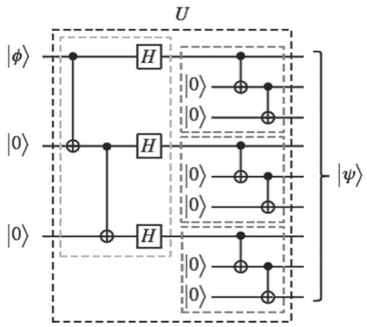


그림 3. Shor 부호의 부호화 서킷

(2) 3-큐비트 페이즈 플립 부호

3-큐비트 페이즈 플립 부호는 채널에서 발생하는 단일 Z 오류로부터 정보를 보호하는 양자 오류 정정 부호 기법이다. 3-큐비트 페이즈 플립 부호의 구성은 3-큐비트 비트 플립 부호와 유사하다. 3-큐비트 페이즈 플립 부호의 코드워드는 $|+++\rangle$와 $|---\rangle$로 구성되는 공간에 존재하며, 이 때 $|+\rangle$와 $|-\rangle$는 각 각 다음과 같은 상태를 의미한다.

$$|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\quad |-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

따라서 임의의 1-큐비트 상태는 3-큐비트 페이즈 플립 부호에 의해 $|\psi\rangle=a|+++\rangle+b|---\rangle$로 부호화 된다. $|+\rangle$ 상태와 $|-\rangle$ 상태는 Z 연산자에 의해 서로 플립 되는 관계를 가지고 있다. 이는 $|0\rangle$과 $|1\rangle$이 X 연산자에 의해 서로 플립 되는 것과 유사하다. 3-큐비트 페이즈 플립 부호의 경우 복호 연산은 XXI와 IXX에 의해 수행되며, 두 연산자는 채널에서 발생한 오류의 위치에 따라 서로 다른 신드롬 패턴을 보여준다.

Shor 부호의 부호화 과정은 3-큐비트 페이즈 플립 부호의 부호화 과정을 수행한 후 각 큐비트에 대해 3-큐비트 비트 플립 과정을 적용함으로써 수행된다. Shor 부호의 복호 과정은 채널에서 발생한 비트 플립 오류와 페이즈 플립 오류를 개별적으로 판단하고 각 오류를 수정함으로써 전체 오류를 수정한다. Shor 부호의 복호에 사용되는 측정 연산자는 총 8개의 연산자로 구성되어 있으며 다음과 같다.

$$S_1=ZZIIIIIII,\quad S_2=IZZIIIIII$$
$$S_3=IIIZZIIII,\quad S_4=IIIIZZIII$$
$$S_5=IIIIIZZI,\quad S_6=IIIIIIZZ$$
$$S_7=XXXXXXIII,\quad S_8=IIIXXXXXX$$

8개의 측정 연산자 중 S_1, S_2, S_3, S_4, S_5, S_6는 X 오류의 발생 유무와 위치에 대한 신드롬 패턴을, S_7, S_8은 Z 오류에 의한 신드롬 패턴을 보여준다.

Degenerate 부호

Shor 부호에서 첫 번째 큐비트에 발생하는 Z 오류와 두 번째 큐비트에 서 발생하는 Z 오류는 동일한 신드롬 패턴을 갖는다. 따라서, 첫 번째, 두 번째, 세 번째 큐비트에서 발생하는 Z 오류는 모두 동일한 복호 연산에 의해 오류를 정정할 수 있다. 뿐만 아니라 신드롬 패턴의 중복은 4, 5, 6 큐비트, 그리고 7, 8, 9 큐비트에서도 동일하게 작용한다. 이와 같이 서로 다른 오류에 대해 동일한 복호 연산을 통해 정보를 복원할 수 있는 특징을 degeneracy라고 하며, 이러한 특성을 갖는 부호를 degenerate 부호라고 한다. 앞에서 살펴본 것처럼 Shor 부호는 degeneracy 특성을 가지고 있는 degenerate 부호이다. Degenerate 부호는 기존 오류 정정 부호에서는 존재하지 않는 양자 오류 정정 부호만의 특징으로 서로 다른 오류에 대해 동일한 신드롬 패턴을 갖는 부호를 말한다. Degeneracy에 의해 양자 오류 정정 부호는 신드롬 패턴의 개수 이상의 오류를 수정할 수 있으며 이는 오류 정정 부호의 성능 향상을 의미한다. 하지만 이런 degenerate 특성 때문에 양자 오류 정정 부호의 성능은 쉽게 분석될 수 없다. 양자 오류 정정 부호의 성능 분석은 많은 경우 고전 오류 정정 부호의 분석 기법을 차용하여 수행된다. 따라서 고전 오류 정정 부호에 존재하지 않는 degenerate

특성은 고전 분석 기법을 이용한 양자 오류 정정 부호 분석의 한계를 의미한다.

안정 부호 (Stabilizer code)

안정 부호는 대표적인 양자 오류 정정 부호로 현재 가장 많은 연구가 진행 중인 오류 정정 부호이다. 그룹 이론(Group theory)을 바탕으로 형성된 안정 부호는 기존 선형 오류 정정 부호와 유사한 특징을 가지고 있으며, 많은 양자 오류 정정 부호가 안정 부호의 범주에 속한다. 앞에서 살펴본 3-큐비트 비트 플립 부호, 3-큐비트 페이즈 플립 부호, Shor 부호 또한 안정 부호에 속하는 오류 정정 부호이다.

안정 부호는 안정 연산자(stabilizer)로 정의된다. 안정 부호의 코드워드는 고유값(eigenvalue) '+1'을 갖는 안정 연산자의 공통 고유벡터(eigenvector) 이다. 따라서, 안정 부호의 안정 연산자 그룹을 S라고 하면 안정 연산자와 코드워드는 다음과 같은 관계를 만족한다.

$$S_i|\psi\rangle = |\psi\rangle$$

이 때, $S_i \in S$이다. 코드워드가 '+1' 고유값을 갖는 안정 연산자의 고유벡터 이기 때문에 코드워드는 안정 연산자의 연산에 의해 변화하지 않는다. 앞의 3-큐비트 비트 플립 부호의 예에서 코드워드 $|\psi\rangle = a|000\rangle + b|111\rangle$는 신드롬 측정 연산자 ZZI와 IZZ 에 의해 안정된 (stabilized) 된 상태이다.

$$ZZI|\psi\rangle = |\psi\rangle, \quad IZZ|\psi\rangle = |\psi\rangle$$

$|\psi\rangle$는 고유값 (eigenvalue)'+1'을 갖는, 측정 연산자 ZZI와 IZZ 의 고유벡터로 해석될 수 있다. 따라서, 3-큐비트 비트 플립 부호는 ZZI와 IZZ 로 구성되는 안정 연산자 그룹을 갖는 안정 부호이다.

안정 연산자 그룹은 그룹을 나타낼 수 있는 최소한의 연산자로 표시되며, 이러한 최소한의 연산자를 안정 연산자 생성자 (Stabilizer generator) 라고 한다. 생성자를 이용해 안정 연산자 그룹을 나타내면 다음과 같다.

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

안정 연산자 그룹의 모든 원소는 서로 교환법칙이 성립하는 연산자이다. 이를 수식으로 나타내면 다음과 같다.

$$[S_i, S_j] = 0$$

이 때, $[A,B] = AB - BA$를 의미한다. 연산자 사이의 교환법칙 성립은 안정 연산자와 오류를 구별하며, 안정 연산자와 오류 연산자 사이의 교환법칙 결과는 신드롬 패턴으로 사용된다.

논리 연산자 $\overline{X}$, $\overline{Z}$는 코드워드에 대해 X 또는 Z 연산자와 같은 역할을 하는 연산자이다. 코드워드는 코드워드 공간의 기준 벡터로부터 $\overline{X}$을 이용하여 형성될 수 있다. k-큐비트를 복호화 할 경우 논리 연산자는 각 각 k개의 연산자로 구성된다. 예를 들어 살펴보면, 3-큐비트 비트 플립 부호의 경우 정보 큐비트 $|\phi\rangle = a|0\rangle + b|1\rangle$에 대한 논리 연산자는 X와 Z 이다. 정보 큐비트가 코드워드로 부호화 된 후 코드워드에 대해 정보 큐비트의 논리 연산자와 같은 역할을 수행하는 연산자는 다음과 같다.

$$\overline{X}_1 = XXX \ , \quad \overline{Z}_1 = ZII$$

코드워드를 구성하는 기저 벡터는 코드워드 공간의 기준 벡터 $|000\rangle$와 논리 연산자 XXX를 이용하여 전개된다.

$$|111\rangle = XXX|000\rangle$$

연산자 $\overline{Z}_1$은 코드워드에 대해 Z 연산자와 같은 역할을 수행한다.

$$ZII|000\rangle = |000\rangle, \quad ZII|111\rangle = -|111\rangle$$

안정 연산자와 논리 연산자를 통해 안정 부호의 Normalizer를 정의할 수 있다. Normalizer는 연산자의 그룹으로 모든 안정 연산자와 교환법칙이 성립하는 연산자의 집합이다. 논리 연산자는 모든 안정 연산자와 교환법칙이 성립한다. 따라서 Normalizer는 안정 연산자와 논리 연산자를 통해 다음과 같이 나타낼 수 있다.

$$N = \langle S_1, S_2, \cdots, S_m, \overline{X}_1, \cdots, \overline{X}_k, \overline{Z}_1, \cdots, \overline{Z}_k \rangle$$

안정 부호에 의한 채널의 오류는 크게 3 종류로 구분될 수 있다. 첫 번째로는 안정 부호에 의해 검출 및 정정이 가능한 오류이다. 이 그룹에 속하는 오류 연산자는 생성자 중 임의의 연산자와 교환법칙이 성립하지 않으며 그 결과로 신드롬 패턴을 형성한다. 따라서, 생성된 신드롬 패턴을 이용해 오류를 정정하게 된다. 두 번째 오류 그룹은 검출은 가능하지만 정정은 불가능한 오류이다. 이러한 오류는 일부의 생성자와 교환법칙이 성립하지 않고 신드롬 패턴을 형성하지만 안정 부호의 오류 수정 능력을 넘어서는 오류이다. 세 번째 오류 그룹은 안정 부호의 모든 안정 연산자와 교환법칙이 성립하는 오류로써 오류가 발생한 경우에도 오류의 유무를 확인할 수 없다. 앞에서 설명한 normalizer는 안정 연산자와 교환법칙이 성립하는 연산자 그룹으로 normalizer의 모든 연산자가 세 번째 오류에 속하게 된다. Normalizer는 안정 연산자 그룹을 포함하고 있다. 하지만 안정 연산자는 코드워드를 변형시키지 않기 때문에 오류로 볼 수 없다. 이를 바탕으로 안정 부호의 오류 정정 능력을 살펴보면, 안정 부호의 minimum distance d는 $N-S$에 속하는 원소 중 가

장 작은 weight로 정의 된다.

안정 부호는 기존 선형 블록 부호와 유사한 특징을 가지고 있으며, 특정 조건을 만족하는 기존 선형 블록 부호로부터 안정 부호를 생성할 수 있다. CSS 부호는[5] 안정 부호로 해석할 수 있는 양자 오류 정정 부호로써 두 선형 블록 부호 C_1과 C_2가 $C_2 \subset C_1$ 조건을 만족하며, C_1와 $C_2^{\perp}$의 오류 정정 능력이 같을 경우 두 선형 블록 부호로부터 CSS 부호를 구성할 수 있음을 보여준다. 이 때, $C^{\perp}$는 C의 듀얼을 의미한다. 특히, Steane은 $C_1 = C$이고 $C_2 = C^{\perp}$인 선형 오류 정정 부호를 이용하여 1개의 오류를 정정 할 수 있는 7-큐비트 안정 부호를 구성하였다[6,7].

선형 블록 부호와 양자 오류 정정 부호의 관계는 양자 연산자의 바이너리 표현을 통해 더 쉽게 이해할 수 있다. 임의의 Pauli 연산자는 이진 벡터로 표현이 가능하다. X 연산자의 경우 $[0|1]$로 나타낼 수 있으며 Z는 $[1|0]$로 나타낼 수 있다. 이를 이용하여 임의의 Pauli 연산자를 표기하면 다음과 같다.

$$U = Z^u X^v \triangleq [u|v]$$

이 때, u와 v는 이진 벡터를 나타낸다. 안정 부호의 생성자를 이진 벡터를 이용하여 나타내면 이진 행렬이 되며 이를 체크 행렬이라고 한다. 그리고 이 때 각 행은 생성자 연산자에 해당하는 이진 벡터가 된다. 안정 부호의 체크 행렬은 심플레틱 내적(symplectic inner product)에 대해서 '0'을 만족한다. 이 때, 심플레틱 내적은 다음과 같이 정의된다.

$$[a|b] \odot [c|d] \equiv ad^T \oplus bd^T$$

심플레틱 내적의 결과가 '0'이 된다는 것은 각 행을 구성하는 연산자 사이의 관계가 서로 교환법칙을 만족함을 의미한다. 따라서 심플레틱 내적의 값이 '0'이 되는 이진 행렬을 구성함으로써 안정 부호의 생성자를 구할 수 있으며, 이로부터 안정 부호의 안정 연산자 그룹을 생성할 수 있다. 심플레틱 내적이 '0'이 되는 방법 중 하나는 안정 부호의 체크 행렬이 다음과 같을 때이다.

$$A = \begin{bmatrix} H & 0 \\ 0 & G \end{bmatrix}$$

이 때, H는 선형 블록 부호 C의 패리티 체크 행렬을, G는 C의 듀얼인 $C^{\perp}$의 생성 행렬을 의미한다. 듀얼 부호의 경우 생성 행렬이 원 부호의 패리티 체크 행렬과 동일하기 때문에 결과적으로 위 체크 행렬은 심플레틱 내적이 '0'이 된다. 이와 같은 선형 블록 부호의 듀얼 특성을 이용하여 안정 부호는 기존 선형 블록 부호로부터 양자 오류 정정 부호를 구성할 수 있는 기법을 제시한다.

Ⅲ. 결 론

양자 정보 시스템은 고전 정보 시스템이 가지고 있는 한계를 넘기 위한 새로운 시스템이다. 고전 시스템으로는 불가능한 많은 일이 양자 시스템으로는 가능하다. 양자 시스템의 가능성에 세계 각국은 앞다투어 새로운 양자 컴퓨터 개발에 박차를 가하고 있다. 양자 정보 시스템은 아직 기초적인 연구단계에 있다. 물리적인 구현에서 이론적인 내용까지 아직은 많은 문제를 해결해야 한다. 양자 정보는 저장에서 전송까지 외부의 영향으로부터 매우 취약하다. 따라서 정확한 정보 처리를 위해 양자 오류 정정 부호는 양자 시스템의 필수 불가결한 요소이다. 본 논문에서는 양자 정보의 특성을 살펴보고 양자 정보를 보호하기 위한 양자 오류 정정 부호를 간략하게 살펴보았다.

참 고 문 헌

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

[2] E. Hagley et al., "Generation of Einstein-Podolsky-Rosen Pairs of Atoms," Phys. Rev. Lett. 79, 1997.pp. 1 - 5.

[3] Michael A. Nielsen and Isaac L. Chuang, "Quantum Computation and Quantum Information," Cambridge University Press, 2000

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

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

[6] A. M. Steane, "Error Correcting Codes in Quantum Theory," Phys. Rev. Lett., vol. 77, pp. 793 - 797, Jul. 1996.

[7] 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.

[8] R. G. Gallager, "Low-density parity-check

codes,"IEEE Tram. on Inforinariorz Theory, vol.8, no.1, pp. 21-28, January 1962.

[9] P.W. Shor, Proceedings 35th Annual Symposium on Foundations of computer Science, IEEE Computer Society Press, Los Alamitos, CA, 1994, p. 124.

[10] Grover L.K., "A fast quantum mechanical algorithm for database search," Proceedings, 28th Annual ACM Symposium on the Theory of Computing, p. 212 (May 1996)

[11] S. Wieder, The Foundations of Quantum Theory, Academic Press, 1973.

[12] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-Graph Codes for Quantum Error-Correction," IEEE Trans. on Information Theory, vol. 50, no. 10, pp. 2315-2330, October 2004.

[13] H. Lou and J. Garcia-Frias, "Quantum Error-Correction Using Codes with Low-Density Generator Matrix," Proc. SPAWC'05, June 2005.

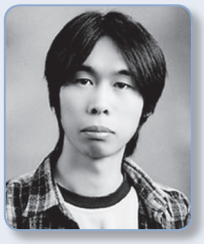
[14] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," Phys. Rev. A, vol. 55, no. 2, pp. 900-911, Feb. 1997.

[15] E. Knill, R. Laflamme, and L. Viola, "Theory of Quantum Error Correction for General Noise," arXiv.org, vol. quant-ph. 20-Aug-1999.

약 력

허 준

1989년 서울대학교 공학사
1991년 서울대학교 공학석사
2002년 University of Southern California 공학박사
2002년~2003년 하이닉스 반도체 (주) System IC comp 책임연구원
2003년~2007년 건국대학교 전자공학과 조교수
2007년~현재 고려대학교 전기전자전파공학부 교수
관심분야: 통신 시스템, 오류 정정 부호, 양자 정보 이론



신 정 환

2005년 건국대학교 공학사
2007년 건국대학교 공학석사
2012년 고려대학교 공학박사
2012년~현재 고려대학교 BK21사업단 연구 교수
관심분야: 양자 정보 이론, 통신 시스템