# 연속 변수를 사용한 양자 오류 정정 부호

손일권, 허 준
고려대학교

## 요 약

연속 변수 양자 오류 정정 부호는 전자의 스핀, 광자의 편광 등으로 나타내는 불연속 변수와는 다르게 빛의 진폭 및 위상처럼 연속적인 값을 가지는 양자 정보의 오류를 수정하는 기법이다. 본 논문에서는 안정 부호 형태를 기반으로 한 연속 변수 양자 오류 정정 부호의 구성을 살펴보고, 불연속 양자 오류 정정 부호와의 차이점을 알아본다.

## Ⅰ. 서 론

최근에 양자 역학에 기반을 둔 양자 정보 처리 기술들이 세계적으로 활발하게 연구되고 있다. 양자 정보 처리 기술은 기존의 이진 정보가 아닌 연속적인 값을 가지며 중첩이 가능한 양자 정보를 이용하며 병렬 처리가 가능하기 때문에 기존의 기술로는 처리할 수 없는 고속 연산이 가능하다. 1994년 피터 쇼어는 양자 정보의 병렬 처리 특성을 이용하여 소인수 분해 연산을 매우 빠르게 처리할 수 있음을 보였고[1], 이후 그로버의 데이터 검색 알고리즘[2] 또한 양자 정보 처리 기술이 기존의 컴퓨터가 수행할 수 없는 연산들이 가능함을 보였다. 이렇듯 양자 정보 처리 기술은 강력한 잠재력을 가지고 있지만, 기술의 근간이 되는 양자 정보가 외부의 간섭에 매우 취약하다는 단점이 존재하여, 기존의 정보 처리 시스템처럼 오류가 없는 시스템을 구성하는 것이 상당히 어렵다. 따라서 양자의 정밀한 상태가 유지 되지 않아도 사용될 수 있으며 관측 시 붕괴 된다는 양자 정보의 또 다른 특성을 이용하여 정보 전송 중에 도청되는 것을 방지하는 양자 암호 기술[3]이 최근에 큰 주목을 받고 있다.

이렇듯 양자 정보의 취약성으로 인하여 양자 암호 기술 이외의 양자 정보 처리 기술 구현에 많은 어려움이 있기 때문에 양자 오류 정정 부호의 역할이 매우 중요하다. 양자 오류 정정 부호는 외부의 간섭으로 인해 양자 상태가 붕괴되거나 전송, 처리 저장 중에 발생하는 오류를 수정하기 위한 기술이다. 양자 오류 정정 부호는 사용되는 양자 정보 형태에 따라 구분되며 각각의 형태는 불연속 변수와 연속 변수로 나눌 수 있다. 불연속 변수의 경우 전자의 스핀, 광자의 편광 등을 이용하여 구현하며, 연속 변수의 경우에는 빛의 진폭 · 위상과 같은 특성을 사용하여 구현한다. 현재 연구되고 있는 불연속 양자 오류 정정 부호는 이진 정보에서의 오류 정정 부호를 기반으로 발전하였으며 이와는 별도로 양자 고유의 속성을 사용한 양자 오류 정정 부호들 또한 연구되고 있다. 연속 변수의 경우 선행 연구된 불연속 변수 양장 오류 정정 부호를 바탕으로 연구되고 있으며 이를 통해 현재 연속 변수 안정 양자 오류 정정 부호와 연속 변수 얽힘 양자 오류 정정 부호 등이 연구 된 바 있다.

본 논문에서는 불연속 변수 안정 부호를 간략히 살펴보고 이를 바탕으로 연속 변수 안장 부호의 구성 방법을 살펴본다.

## Ⅱ. 본 론

### 1. 양자 정보

#### 1.1 불연속 변수 양자 정보

불연속 변수 양자 정보는 양자 비트(quantum bit), 줄여서 큐비트(qubit)를 정보의 기본 단위로 사용한다. 이는 기존의 디지털 정보인 비트처럼 두 개의 기본 상태를 가진다는 점은 유사하나 여러 측면에서 비트와는 다른 특성을 가진다. 비트의 경우 0 혹은 1 둘 중 하나의 값만 가질 수 있지만 큐비트의 경우 상태의 중첩이 가능하다는 것이 가장 큰 차이점이다. 즉 양자 정보는 0과 1 각각의 상태로 존재할 수 있을 뿐만 아니라 0과 1이 중첩 되어 있는 상태로도 존재할 수 있다. 간단한 예로 전자의 스핀을 사용하여 큐비트를 구성할 경우 전자의 스핀 방향이 위로 향하는 경우를 '↑'로, 스핀 방향이 아래로 향하는 경우를 '↓'로 나타낼 수 있다. 이를 디렉(Dirac) 표현에 따라 큐비트를 나타내면 다음과 같이 나타낼 수 있다.

$$|\psi\rangle = a|\uparrow\rangle + b|\downarrow\rangle \quad (1)$$

이때 $|\cdot\rangle$는 벡터를 나타내며 $a$, $b$는 각각의 스핀에 해당하는 확률과 관련된 값으로 전자로 구성한 큐비트의 상태가 '↑'일 확률이 $|a|^2$, '↓'일 확률이 $|b|^2$이다. 따라서 $a$와 $b$의 관계는 다음과 같다.

$$|a|^2 + |b|^2 = 1 \tag{2}$$

앞에서 설명한 전자의 예를 일반적인 경우로 나타내면 각 스핀은 2차원 힐버트 공간의 직교 기저 벡터라 할 수 있고 $|0\rangle \equiv |\uparrow\rangle$, $|1\rangle \equiv |\downarrow\rangle$로 나타낼 수 있다. 따라서 불연속 변수 양자 정보는 2차원 힐버트 공간상에 존재한다. 이를 통해 일반적인 큐비트 상태 $|\psi\rangle$를 다시 나타내면 다음과 같다.

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{3}$$

### 1.2 연속 변수 양자 정보

큐비트가 기존에 사용되던 비트 정보와 유사한 성질을 가지고 있으며, 큐비트를 사용해서 양자 전송[4](Quantum teleportation), 양자 소인수 분해, 양자 암호 키 등 양자 고유의 성질을 응용하는 기술들을 모두 구현할 수 있기 때문에 현재의 양자 정보 처리 기술들은 대부분 큐비트를 기반으로 연구되고 있다. 하지만 광자, 전자와 같은 불연속 변수 양자 정보는 생성, 검출이 매우 어렵다는 단점을 가지고 있다. 예를 들어 광자의 경우 단일 광자를 효율적으로 검출해 내는 기술은 매우 어려우며, 이러한 제한 조건들은 양자 정보 처리 기술의 발전에 있어서 큰 걸림돌이 되고 있다. 이에 반에 연속 변수 양자 정보는 기존의 광학 장비 및 기반 지식들을 양자 정보의 생성, 제어, 처리 등에 적용할 수 있다는 장점을 가지고 있다. 또한 양자 정보의 차원이 2인 큐비트와 다르게 실수 차원을 가지는 양자 상태를 사용하기 때문에 자원 활용에 있어서 연속 변수 양자 정보는 불연속 변수 양자 정보보다 효율적이라는 장점을 가지고 있다. 이러한 연속 변수 양자 정보는 양자 역학에서의 조화 진동자를 표현하는데 쓰이는 위치 $\hat{q}$와 운동량 $\hat{p}$을 사용하여 정보를 표현하며 각각의 형태[5]는 다음과 같다.

$$\hat{q} = \sqrt{\frac{\hbar}{2\omega}}(\hat{a} + \hat{a}^\dagger)$$
$$\hat{p} = -i\sqrt{\frac{\hbar\omega}{2}}(\hat{a} - \hat{a}^\dagger) \tag{4}$$

이 때 $\hat{a}$와 $\hat{a}^\dagger$는 각각 creation 연산자와 annihilation 연산자이다. 만약 빛을 통해 연속 변수 양자 정보를 구성한다면 $\hat{q}$는 전기장, $\hat{p}$는 자기장으로 설정할 수 있다. 따라서 앞서 설명한 불연속 변수처럼 정보를 표현하는데 쓰이는 성질이 2개인 것이 아니라 연속적인 실수의 값을 가지게 된다. 따라서 2차원 힐버트 공간상에 존재하는 불연속 변수 양자 정보와 다르게 연속 변수 양자 정보는 무한 차원의 힐버트 공간상에서 존재한다. 이는 연속 변수로써 정보를 표현하는 것이 불연속 변수를 사용하는 것보다 효율적으로 자원을 사용할 수 있게 하지만 동시에 연산량이 훨씬 더 많아지는 단점 또한 가지게 된다.

## 2. 양자 오류 정정 부호

1994년 Peter shor가 양자 소인수 분해 알고리즘을 통해 양자 정보 처리의 우수성을 처음 발표했을 때, 양자 정보는 외부의 간섭에 매우 취약하기 때문에 그 상태를 유지할 수 없어 양자 정보 처리 자체가 불가능하다는 인식이 널리 퍼져있었다. 따라서 이론적으로는 성능이 우수할 수 있으나 구현이 불가능할 것이라 생각하여 대부분의 사람들이 그 효용성에 있어서 많은 의구심을 가졌었다. 하지만 1995년 Peter shor가 최초의 양자 오류 정정 부호[6]를 발표함으로써 양자 정보 처리 기술의 발전이 이루어지게 되었고, 양자 정보 처리 기술의 발전에 따라 양자 오류 정정 부호의 중요성 또한 크게 부각 되었다.

기존의 디지털 시스템과 다르게 양자 정보는 복사가 불가능[7]하기 때문에 기존 디지털 시스템에서 사용하던 오류 정정 부호의 방식을 그대로 사용할 수 없다. 따라서 초기 양자 오류 정정 부호는 기존 오류 정정 부호를 활용하여 만들어졌지만 현재에는 양자 고유의 오류 정정 부호 기술이 연구되고 있다.

### 2.1 불연속 변수 양자 안정 부호

불연속 변수 양자 오류 정정 부호는 양자 정보에 발생하는 Pauli 오류를 정정할 수 있는 기술이다. Pauli 오류란 Pauli 연산자로 정의된 오류로 단일 큐비트 시스템에 대한 Pauli 연산자는 다음과 같다.

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$
$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{5}$$

각각의 연산자의 특성을 살펴보면, $X$연산자는 비트 플립(flip) 연산자로 각 기저에 미치는 영향은 다음과 같다.

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle \tag{6}$$

$Z$연산자는 위상(phase) 플립 연산자로 각 기저에 미치는 영향은 다음과 같다.

$$Z|0\rangle = |0\rangle, \quad Z|1\rangle = -|1\rangle \tag{7}$$

$Y$연산자는 $X$연산자와 $Z$연산자가 연속적으로 작용한 연산이다. 각각의 연산자는 서로 anti-commute한 관계이다. 즉 $\{A, B\} = AB + BA\ (A \neq B)$을 만족한다. 또한 각각의 연산

자는 이진 벡터와 대응 시킬 수 있다.

표 1. Pauli operator와 이진 벡터 간의 대응 관계

| $(\mathbb{Z}_2)^2$ | Pauli operator |
|---|---|
| 00 | $I$ |
| 01 | $X$ |
| 11 | $Y$ |
| 10 | $Z$ |

이를 통해 Pauli 연산자에서는 곱셈 형태의 연산이 이진 벡터 상에서는 modulo 2 연산으로 변환 될 수 있다.

안정 부호(Stabilizer code)는 현재까지 가장 많은 연구가 된 양자 오류 정정 부호이다. 안정 부호는 기존 디지털 시스템에서 쓰이던 선형 오류 정정 부호와 유사한 특징을 가지고 있으며, 현재 개발 되어 있는 대다수의 부호가 안정 부호에 속한다. 안정 부호는 안정 연산자(stabilizer) 그룹 S를 통해 구성된다. 안정 연산자는 안정 부호의 코드워드에 대해 '+1' eigenvalue를 가지며 안정 연산자는 서로 commute한 관계를 가지는 연산자이다. 즉 안정 부호의 코드워드는 안정 연산자의 eigenvector이며 코드워드와 안정 연산자의 관계는 다음과 같다.

$$S_i|\psi\rangle = |\psi\rangle \tag{8}$$

이 때 $S_i$는 안정 연산자 그룹의 원소이며($S_i \in S$) eigenvalue가 '+1'이기 때문에 안정 부호의 코드워드는 안정 연산자에 의해 변화하지 않는다. 안정 연산자 그룹 S는 그룹을 구성할 수 있는 최소의 안정 연산자 생성자(Stabilizer generator)를 통해 표현될 수 있다. 안정 연산자 생성자를 통해 안정 연산자 그룹을 나타내면 다음과 같다.

$$S = \langle S_1, S_2, \cdots S_m \rangle \tag{9}$$

논리 연산자 $\bar{X}$, $\bar{Z}$는 $X$, $Z$연산자가 일반 큐비트 상태에 대하여 수행하는 역할을 코드워드에 대해 수행하는 연산자이며 안정 연산자와 모두 commute한 관계를 가진다. 안정 부호의 경우 논리 $|0\rangle$ 벡터인 $|\bar{0}\rangle$와 $\bar{X}$를 통해 코드워드를 생성한다. 보호하고자 하는 정보가 k큐비트인 경우 논리 연산자 $\bar{X}$, $\bar{Z}$는 각각 k개가 존재하며 k개의 $\bar{X}$을 통해 $2^k$개의 안정 부호 코드워드를 구성할 수 있다.

안정 부호를 구성하는 단계는 다음과 같다. 양자 오류 정정 부호는 양자 상태가 복제가 불가능하기 때문에 기존의 오류 정정 부호처럼 k비트의 정보를 $n$비트로 확장할 수 없다. 따라서 k큐비트의 정보를 보호하기 위해서 $n$큐비트의 부호를 구성할 경우 미리 $n$큐비트 길이의 $|0\rangle^{\otimes n}$기저를 준비해야 한다. 이렇게 준비해둔 큐비트를 논리 $|0\rangle$인 $|\bar{0}\rangle$로 만들기 위해서 안정 연산자를 사용한다. 안정 연산자를 통해 $|\bar{0}\rangle$를 구성하는 방법은 다음과 같다.

$$|\bar{0}\rangle = \sum_{S_i \in S} S_i |0\rangle^{\otimes n} \tag{10}$$

$|\bar{0}\rangle$에 논리 연산자 $\bar{X}$를 연산해줌으로써 코드워드를 구성할 수 있다. 논리 연산자를 통해 코드워드를 구성하는 방법은 다음과 같다.

$$|\overline{c_1 c_2 \cdots c_k}\rangle = \overline{X_1}^{c_1}\overline{X_2}^{c_2}\cdots\overline{X_k}^{c_k}|\bar{0}\rangle \tag{11}$$

큐비트는 이진 정보의 형태이기 때문에 $c_i$는 $\{0, 1\}$ 중 하나의 값을 가지게 되고 0일 경우에는 는 작용하지 않고 1일 경우에는 작용하게 된다. 5 큐비트 안정 부호[8]를 예를 들면 안정 연산자 생성자는 다음과 같다.

$$XZZXI, IXZZX, XIXZZ, ZXIXZ \tag{12}$$

4개의 안정 연산자 생성자를 통해 총 16개의 안정 연산자가 구성되며 이를 통해 $|\bar{0}\rangle$을 구성하면 다음과 같다.

$$|\bar{0}\rangle = \sum_{S_i \in S} S_i |0\rangle^{\otimes 5}$$
$$= |00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle$$
$$- |11011\rangle - |00110\rangle - |11000\rangle - |11101\rangle - |00011\rangle$$
$$- |11110\rangle - |01111\rangle - |10001\rangle - |01100\rangle - |10111\rangle$$
$$+ |00101\rangle \tag{13}$$

5 큐비트 부호의 논리 연산자 $\bar{X}$는 $XXXXX$이고 이를 $|\bar{0}\rangle$에 적용하면 $|\bar{1}\rangle$을 구할 수 있고 그 형태는 다음과 같다.

$$|\bar{1}\rangle = \bar{X}|\bar{0}\rangle = XXXXX|\bar{0}\rangle$$
$$= |11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle$$
$$- |00100 - |11001\rangle - |00111\rangle - |00010\rangle - |11100\rangle$$
$$- |00001\rangle - |10000\rangle - |01110\rangle - |10011\rangle - |01000\rangle$$
$$+ |11010\rangle \tag{14}$$

이를 통해 5 큐비트를 사용하여 1 큐비트의 정보를 1개의 오류로부터 보호할 수 있는 ⟦5,1,3⟧부호를 구성할 수 있다.

### 2.2 연속 변수 양자 안정 부호

불연속 변수 양자 오류 정정 부호가 기존 디지털 시스템 상에서의 오류 정정 부호를 바탕으로 발전하였듯이 연속 변수 양자 오류 정정 부호는 선행 연구된 불연속 변수의 부호를 기반으로 연구되어 왔다. 연속 변수 양자 정보는 무한대 차원의 힐버트 공간상에 존재하기 때문에 그 연산 량이 불연속 변수 양자 정보에 비하여 훨씬 많아지므로 불연속 변수 부호 각각에 대응하는 연속 변수 부호가 모두 존재하지는 않는다.

연속 변수 양자 오류 정정 부호는 Generalized Pauli 오류를 수정할 수 있는 기술이다. Generalized Pauli 오류란 Heisenberg-Weyl 연산자로 정의된 오류로 단일 큐비트 시스

템에 대한 Heisenberg-Weyl 연산자는 다음과 같다.

$$X(t) \equiv \exp(i\pi t\hat{p}), \qquad Z(t) \equiv \exp(i\pi t\hat{q}) \tag{15}$$

이때 변수 t는 0 또는 1만의 값을 가지던 Pauli 연산자와 다르게 실수의 값을 가진다. 각각의 연산자가 단일 wave-packet에 미치는 영향은 다음과 같다.

$$X(t)|x\rangle = |x+t\rangle, \qquad Z(t)|x\rangle = e^{2i\pi tq}|x\rangle \tag{16}$$

불연속 변수와 마찬가지로 각각의 연산자는 벡터 형태로 표현될 수 있으나 벡터의 원소가 불연속 변수와 다르게 실수의 형태이며 곱셈의 연산이 modulo 2 연산이 아닌 일반 덧셈의 형태를 가진다.

불연속 변수 양자 오류 정정 부호와 마찬가지로 연속 변수 안정 부호는 가장 기본적인 부호라 할 수 있다. 불연속 변수 안정 부호를 통해 연속 변수 안정 부호를 구성하는 방법[9]은 다음과 같다. 불연속 변수의 안정 연산자 생성자를 통해 양자 오류 정정 부호의 parity check matrix를 구성할 수 있다. 예를 들어 앞서 살펴본 불연속 변수 $[\![5,1,3]\!]$ 부호의 parity check matrix를 구성하면 다음과 같다.

$$\left[\begin{array}{ccccc|ccccc} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right] \tag{17}$$

불연속 변수 부호의 안정 연산자 생성자를 통해 parity check matrix를 구하고, 이를 변환하여 연속 변수의 parity check matrix를 유도할 수 있다. 연속 변수는 정보의 값이 실수 범위 상에서 존재하기 때문에 안정 연산자 생성자 사이의 commutativity를 확인하기 위한 벡터 간의 연산이 modulo 2 연산이 아닌 일반 덧셈으로 바뀌게 된다. 따라서 parity check matrix 상의 원소의 값을 일부 수정해야 한다. 대부분의 경우 불연속 변수 양자 정보에서 을 통해 commute함이 만족 되었던 행들에서 일부 1 값의 부호를 -1로 바꾸어 주는 것만으로도 해결이 가능하다.

변환된 parity check matrix를 통해 연속 변수 안정 부호를 구성하는 방법은 다음과 같다. 불연속 변수 안정 부호와 마찬가지로 양자 정보는 복제가 되지 않기 때문에 미리 $n$-wave-packet의 $|0\rangle$상태를 준비한다. 준비한 $n$-wave-packet의 $|0\rangle$ 상태를 논리 $|\bar{0}\rangle$로 변환하기 위해 불연속 변수와 마찬가지로 $|\bar{0}\rangle = \sum_{S_i \in S} S_i|0\rangle^{\otimes n}$의 관계를 사용한다. 이때 안정 연산자 $S_i$는 미리 변환해둔 연속 변수 안정 부호의 parity check matrix를 통해 구성한다. 연속 변수 안정 부호 또한 $|\bar{0}\rangle$에 논리 연산자 $\bar{X}$를 연산해줌으로써 코드워드를 구성할 수 있다. 연속 변수 안정 부호의 논리 연산자 $\bar{X}$을 구하기 위해서는 안정 연산자와 마찬가지로 일반 덧셈 연산에서도 안정 연산자들과 $\bar{X}$가 commute하도록 변환해주어야 한다. 변환 된 $\bar{X}$와 연속 변수 안정 부호의 코드워드 간의 관계식은 다음과 같다.

$$\overline{|q_1 q_2 \cdots q_k\rangle} = \overline{X_1(q_1)X_2(q_2)} \cdots \overline{X_k(q_3)}|\bar{0}\rangle \tag{18}$$

위에서 예를 들은 $[\![5,1,3]\!]$ 부호를 연속 변수 안정 부호로 변환하려면 다음과 같은 단계를 거치게 된다. 첫째로 불연속 변수 안정 부호의 parity check matrix를 변환하면 다음과 같다.

$$\left[\begin{array}{ccccc|ccccc} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right] \tag{19}$$

이에 따라 연속 변수 안정 부호의 논리 연산자 $\bar{X}$를 구하면 다음과 같다.

$$\begin{aligned} \bar{X} &= X(-1)X(-1)X(1)X(1)\,X(1) \\ &\rightarrow (-1,-1,1,1,1,|0,0,0,0,0) \end{aligned} \tag{20}$$

코드워드의 기반이 되는 논리 $|\bar{0}\rangle$를 구하는 과정은 다음과 같다.

$$\begin{aligned} |\bar{0}\rangle &= \sum_{S_i \in S} S_i|0\rangle^{\otimes 5} \\ &= \int \cdots \int dt_1 \cdots dt_4\, e^{2i\pi q(t_1-t_4)} \times \\ &\quad |t_1+t_3, t_2+t_4, t_3, t_1+t_4, t_2\rangle \end{aligned} \tag{21}$$

위에서 구한 5-wave-packet 부호의 논리 연산자 $\bar{X}$을 사용하여 $|\bar{1}\rangle$를 구하는 과정은 다음과 같다.

$$\begin{aligned} |\bar{1}\rangle &= \bar{X}|\bar{0}\rangle = X(-1)X(-1)X(1)X(1)\,X(1)|\bar{0}\rangle \\ &= \int \cdots \int dt_1 \cdots dt_4\, e^{2i\pi q(t_1-t_4)} \times \\ &|t_1+t_3-1, t_2+t_4-1, t_3+1, t_1+t_4+1, t_2+1\rangle \end{aligned} \tag{22}$$

이를 통해 5-wave-packet을 사용하여 1-wave-packet의 정보를 1개의 generalized Pauli 오류로부터 보호할 수 있는 $[\![5,1,3]\!]$ 부호를 구성하였다.

## Ⅲ. 결 론

양자 정보 처리 기술은 병렬연산 및 얽힘 등과 같은 양자 고유의 성질을 이용하여 정보처리의 패러다임을 바꿀 수 있는 잠재력을 보여주고 있다. 특히 보안 분야는 가장 빠르게 상용화를 이루어 현재 몇몇 해외 기업에서 초기 단계의 제품을 내놓았다. 하지만 양자 정보 개발이 큰 영향을 미칠 것으로 기대되는 양자 통신이나 양자 컴퓨팅과 같은 분야에서는 아직 연구 수준 및 개발 단계가 초기 수준에 머물러 있다. 양자 상태가 외부 간섭에 매우 취약하여 각 분야의 개발에 어려움이 있기 때문에, 양자 오류 정정 부호는 양자 정보 처리 기술 구현에 가장 핵심 기술

이라 할 수 있다. 본 논문에서는 양자 정보를 불연속 변수와 연속 변수로 나누어 특성을 살펴보았고, 각각의 정보 형태에 따라 그 정보를 보호 할 수 있는 안정 부호 형태의 양자 오류 정정 부호를 살펴보았다.

## Acknowledgement

본 연구는 서울시 산학연 협력사업[WR080951, Bell Labs 서울 유치 / 광대역 컨버전트 네트워크 기반기술 및 응용서비스연구]의 연구 결과로 수행되었습니다. 이 논문은 2014년도 정부(교육과학기술부)의 재원으로 한국연구재단 기초연구사업의 지원을 받아 수행된 연구임(2011-0025328)

## 참 고 문 헌

[1] Peter W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," arXiv.org, vol. quant-ph. 27-Aug-1995.

[2] Lov K. Grover, "A fast quantum mechanical algorithm for database search," arXiv.org, vol. quant-ph. 29-May-1996.

[3] C. H. Bennett, G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in Proc. of IEEE Int. Conf. on Comp., Syst. and Sig. Proc., pp. 175-179, Bangalore, India, Dec. 1984

[4] Charles H. Bennett, Gilles Brassard, Claude Crepeau, Richard Jozsa, Asher Peres, William K. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky- Rosen Channels," Phys. Rev. Lett. vol. 70, num. 13, pp. 1895-1899 Mar. 1993

[5] Samuel L. Braunstein, Peter van Loock, "Quantum information with continuous variables," Rev. Mod. Phys, vol. 77, Apr. 2005

[6] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," Phys. Rev. A vol. 52, num. 4, pp. 2493-2496 May. 1995.

[7] Wootters, William; Zurek, Wojciech , " A Single Quantum Cannot be Cloned," Nature vol. 299 pp. 802-803, Oct. 1982.

[8] Daniel Gottesman, "Stabilizer Codes and Quantum Error Correction," arXiv.org, vol. quant-ph. 28-May- 1997.

[9] Richard L. Barnes, "Stabilizer Codes for Continuous-variable Quantum Error Correction," arXiv.org, vol. quant-ph. 13-May-2004.

### 약 력

손 일 권

2011년 고려대학교 전자전기전파공학부 졸업
2011년~현재 고려대학교 전자전기전파공학부 석박 통합 과정
관심분야: 통신 시스템, 양자 정보 이론

허 준

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