양자 정보 이론과 결함 허용 양자 컴퓨팅

신정환
(주)케이티

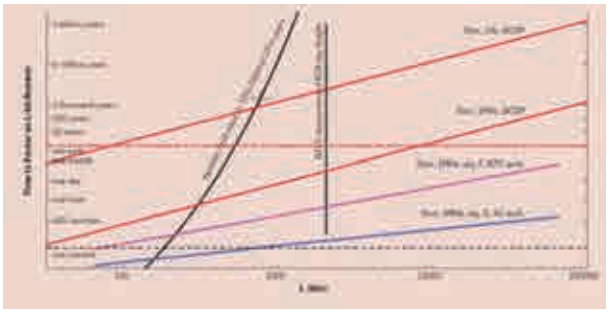
허 준
고려대학교

Ⅰ. 서 론

양자 컴퓨터는 양자 역학에 기반하고 있는 정보 처리 시스템이다. 양자 컴퓨터는 병렬 처리 및 간섭 등 기존 컴퓨터에 존재하지 않는 양자적 특성을 이용하여 고속의 연산 및 자연계 시뮬레이션 등 기존 컴퓨터가 처리할 수 없는 다양한 문제에 활용될 것으로 예상된다. 연산자(Gate) 기반 범용 양자 컴퓨터는 이론적으로 기존 컴퓨터로 구성 가능한 모든 시스템을 구성할 수 있지만, 그렇다고 해서 모든 분야에서 양자 컴퓨터가 기존 컴퓨터보다 더 좋은 성능을 보여주는 것은 아니다. 그럼에도 불구하고 특정 분야에서 양자 컴퓨터는 기존 정보 처리 시스템으로는 얻을 수 없는 결과를 보여준다. 대표적으로 1994년 벨 연구소의 연구원이였던 피터 쇼어에 의해 개발된 인수 분해 알고리즘은 양자 컴퓨터를 이용할 경우 기존 컴퓨터로는 불가능한 성능의 향상을 가져올 수 있음을 보고주고 있다.[1] 〈그림 1〉은 비대칭키 보안 알고리즘 RSA에 사용되는 인수 분해 처리 능력에서 기존 컴퓨터와 쇼어 알고리즘을 이용한 양자 컴퓨터의 성능을 이론적으로 비교한 그래프이다.[2] 그림에서 검은색 선은 기존 컴퓨터로 인수 분해를 했을 경우 RSA 키 길이에 따른 수행 시간을 보여주고 있으며, 그 붉은 색과 파란색 곡선은 다양한 양자 컴퓨터의 인수 분해 성능을 보여주고 있다. 키의 길이가 768인 RSA 알고리즘을 기준으로 살펴보면 기존 컴퓨터는 CPU 기준 3,300년의 시간이 걸리지만 양자 컴퓨터는 비록 이론적인 결과이지만 이상적인 경우 1초 만에 동일한 문제를 해결할 수 있는 것을 보여준다.

현재 많은 국가 및 기업들이 양자 컴퓨터 개발에 집중하고 있으며, 최근 D-wave, IBM, Google, Microsoft, Intel 등 여러 기업에서 양자 컴퓨터의 실현을 위한 다양한 결과를 발표하고 있다. 세계 최초의 상용 양자 컴퓨터를 판매한 곳은 캐나다의 D-Wave 이다. D-Wave

는 2011년 5월 11일 128-qubit 양자 프로세서를 탑재한 D-Wave One을 발표하였다. 이후 D-Wave Two, D-Wave 2X를 차례로 발표하고 2017년에는 2,048-qubit 양자 프로세서를 탑재한 D-Wave 2000Q를 발표하였다. D-Wave의 양자 컴퓨터는 최적화 문제에 특화된 양자 컴퓨터로 D-Wave Two의 경우 NASA와 Google이 인공지능 연구를 위해 도입하였으며, 폭스바겐은 2017년 D-Wave 2000Q를 이용하여 베이징 택시 10,000대에 대해 최적화 경로를 분석하는 실험을 통해 기존 컴퓨터로 45분이 걸리는 연산을 양자 컴퓨터를 이용하여 1초 이내에 완료하는 결과를 얻었다고 발표하였다. IBM은 초기부터 양자 컴퓨터를 연구한 기업으로 2016년 5월 5-큐비트로 구성된 양자 프로세서를 발표하였다. 그리고 2017년에는 16-큐비트, 50-큐비트의 양자 프로세서를 발표하였으며 2018년에는 20 큐비트 양자 프로세서로 구성된 상용 양자 컴퓨터를 공개하겠다고 발표했다.



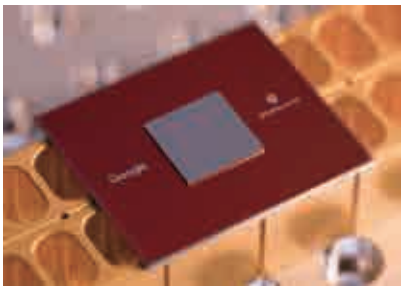
〈그림 1〉 양자 컴퓨터와 기존 컴퓨터의 인수 분해 성능 비교
("A Blueprint for Building a Quantum Computer" By Rodney Van Meter, Clare Horsman)

〈그림 2〉 양자 컴퓨터의 개발 과정

IBM 양자 컴퓨터는 'IBM Q'라는 이름의 프로젝트로 진행되고 있으며, 현재 누구나 온라인을 통해 IBM이 개발한 양자 컴퓨터를 이용할 수 있도록 공개하고 있다. IBM은 양자 컴퓨터를 웹브라우저에서 그래픽 또는 프로그래밍 기법 QASM으로 직접 프로그래밍할 수 있는 방법을 제공하고 있으며 동시에 양자컴퓨터 프로그램 툴 QISKIT과 API를 제공하고 있다. Google 또한 D-wave의 양자 컴퓨터를 이용한 연구와 함께 자체적으로 양자 컴퓨터를 제작하고 있으며 최근 72-큐비트 양자 프로세서 Bristle cone을 공개하였고, 양자 컴퓨터를 이용한 다양한 서비스를 준비하고 있다.

양자 정보 시스템의 가능성에도 불구하고 아직 양자 정보 시스템을 구성하기 위한 다양한 한계도 존재한다. 현재 양자 정보는 기존 정보 시스템에서 사용되는 정보에 비해 다루기 쉽지 않고 외부 시스템과 반응하여 쉽게 정보의 손실이 발생하기도 한다. 일반적으로 양자 컴퓨터에 사용되는 양자 알고리즘은 시스템의 연산 과정 중에 오류가 발생하지 않는 것을 가정하고 있다. 하지만 오류로부터 취약한 양자 시스템으로는 정확한 결과를 얻을 수 없을 것이며 따라서 이러한 외부 환경과의 상호 작용 및 연산에서 발생할 수 있는 오류로부터 양자 정보를 보호할 수 있는 기법이 필요하다. 양자 오류 정정 부호 기법은 양자 시스템에서 사용되는 오류 정정 부호 기법으로 결합, 또는 오류가 있는 양자 정보 시스템에서 정보를 보호하기 위해 필요한 핵심 기술이다.[3-9] 오류 정정 기법은 이미 기존의 다양한 정보 시스템에서 사용되고 있다. 하지만 근본적으로 양자 정보가 갖는 특성 때문에 기존 오류 정정 부호를 양자 시스템에 적용하기는 쉽지 않다.

본 고에서는 양자 역학에 기초를 두고 있는 여러 분야

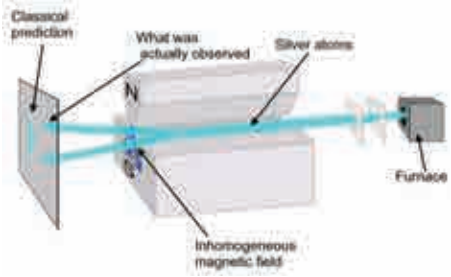


〈그림 3〉 72-qubit 양자 프로세서 (Bristle cone, Google)

중 특히 양자 정보 이론과 이를 바탕으로 결합 허용 양자 정보 시스템[10,11]을 구성하기 위한 양자 오류 정정 부호의 원리에 대해 소개하고자 한다.

Ⅱ. 양자 정보

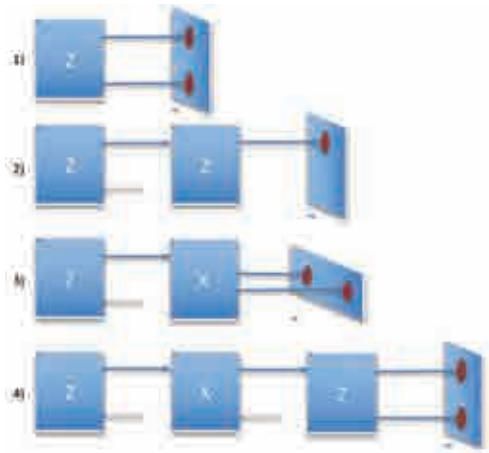
양자(Quantum)는 라틴어 'quantus'에서 유래한 말로 양을 나타내는 단어이다. 양자 역학은 미시적 세계에서 불연속적인 값을 갖는 작은 에너지 또는 물질의 성질을 다룬다. 예를 들어, 빛을 이루는 광자 하나, 물질을 구성하는 원자 하나가 양자 역학의 일반적인 대상이다. 이처럼 양자는 아주 작은 미시적인 세계의 특성을 나타내기에 우리가 직접적으로 경험하기는 쉽지 않으며, 미시적 물질의 성질은 고전 물리 현상과는 그 특성이 다르기 때문에 양자 상태의 모습은 고전 물리적 관점에서는 이상하게 보일 수 있다. 슈테른과 게를라흐가 1922년에 실시한 슈테른–게를라흐 실험은 이런 양자 역학의 특성을 잘 보여주는 실험이다. 슈테른과 게를라흐는 〈그림 4〉와 같이 은원자를 불균일한 자기장에 통과시켜 은원자의 자기 모멘트를 관측하는 실험을 실시하였다. 위 실험은 물리적으로 많은 의미가 있지만 양자 특성에만 초점을 맞춰 그 결과를 살펴보겠다. 실험을 간단히 설명하기 위해 은원자를 하나의 전자로 가정하면, 고전 물리학 관점에서 불균일한 자기장을 지나가는 전자는 자기장에 의해 자기장 방향으로 모든 구간에 걸쳐 연속적으로 관측될 것으로 예상된다. 하지만 실제 실험에서는 예상과는 달리 자기장 방향으로 양 끝에서만 원자가 검출되는 결과를 얻었다. 〈그림 5〉은 게를라흐가 1922년 2월 8일 보어에게 보낸 우편카드로 실험의 실제 관측 결과를 보여준다. 〈그림 3〉은 실제 실험 결과를 90도 돌린 사진으로 그림에서 왼쪽 사진은 불균일한 자기장을 걸어주지 않았을 경우를 나타내며 이때의 결과는 고전적 예상과 일치한다. 〈그림 5〉의 오른쪽은 사진은 실제 불균일한 자기장을 통과한 전자의 결과를 보여준다. 고전적 예상으로는 중간의 공백이 없는 연속적인 분포를 얻어야 하지만 실제 결과는 중간이 비어있는 불연속적인 모습을 보여준다. 이러한 결과를 통해 양자 상태는 불연속적인 값을 갖는 것을 알 수 있다. 〈그림 6〉은 슈테른–게를라흐의 실험을 간단히 나타낸 그림이다. 〈그림 6〉의 1)은 수직으로 형성된 불균일한 자기장에 전자를 통과 시키는 경우를 나타내며 그 결과로 위 또는 아래에서만 전자가 발견된 것을 나타낸다. 〈그림 6〉에서 "Z"는 수직 방향으로 걸쳐진 불균일한 자기장을 타나내고, "X"는 수평 방향으로 걸쳐진 불균일한 자기장을 의미한다. 〈그림 6〉의 2)는 수직 방향의 자기장을 통과한 전자 결과 중 위로 지나간 전자에 다시 수직 방향의 자기장을 걸어준 결과로, 직관적으로 알 수 있듯이 언제나 위쪽 방향의 결과만 얻을 수 있다. 〈그림 6〉의 3)은 수직 방향에서 위로 나온 원자를 다시 수평 방향의 자기장에 통과시킨 것으로 수평 방향에 대해 좌우로 불연속적인 값을 갖는 것을 알 수 있다. 이 실험으로 수직으로 통과한 전자는 수평 필터에 대해서는 좌, 우 두 성분을 포함하는 것으로 유추할 수 있다.〈그림 6〉의 4)는 슈테른– 게를라흐의 실험을 확장한 내용은 양자 상태의 독특한 성질을 보여준다. 〈그림 6〉의 4)에서는 수직 필터에서 위로 통과한 원자를 다시 수평 필터에 통과 시키고 그 결과 중 좌측으로 통과한 전자를 다시 수직 필터를 적용시켰다. 해당 실험의 고전적 해석은 처음 수직 필터에서 위로 통과한 결과만을 이용하였기 때문에 아래 방향의 성분은 사라졌고,



〈그림 4〉 슈테른–게를라흐 실험 장치 (출처: wikipedia)


〈그림 5〉 슈테른–게를라흐 실험 결과

따라서 마지막 수직 필터의 결과도 위로 나올 것으로 예상되지만 실제 실험에서는 1/2의 확률로 위, 아래로 검출되는 결과를 얻을 수 있었다. 처음 수직 필터에서 의해 사라졌을 것으로 생각되는 아래 방향의 결과가 마지막 수직 필터에서 다시 발생한 것이다. 그리고 이러한 결과는 두 수직 필터 사이에 위치한 수평 필터에 의해 발생하였다. 위에서 발생한 양자의 특징은 빛의 편광 특성과 유사한다. 빛이 편광판을 통과한 후의 결과를 관측해 보면 수직 편광판과 수평 편광판을 이용할 경우 두 편광판을 통과하는 빛을 관측할 수 없지만 두 편광판 사이에 대각선 편광판이 존재하는 경우 세 개의 편광판 사이로 통과하는 빛을 관측할 수 있다. 슈테른–게를라흐의 실험 결과로 유추해보면 전자, 또는 양자 상태에서 수직 성분은 수평 성분을 가지고 있으며 수평 성분은 다시 수직 성분을 포함하고 있다고 생각할 수 있다. 추가로 입력되는 양자 상태는 확률적으로 불연속적인 값으로 관측되며 사전에 그 관측 결과를 예측할 수는 없다. 양자 상태에서 수직 성분이 수평 성분으로 나누어지는 현상, 또는 수직 성분이 확률적으로 불연속적인 수평 성분으로 관측되는 성질을 중첩이라고 하며 이를 다시 말하면 수직 성분은 두 수평 성분의 중첩된 상태라고 할 수 있다. 수평 성분에 대해서도 수직 성분과 동일하게 수평 성분은 두 수직 성분의 중첩된 상태라고 말할 수 있다. 결과적으로 슈테른–게를라흐 실험에서 알 수 있는 양자 상태는 불연속적인 값을 가지며 동시에 불연속적인 값의 중첩이 가능한 특징을 가지고 있다.



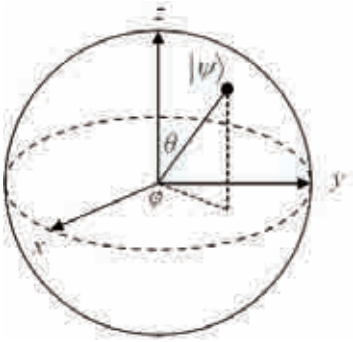
〈그림 6〉 다양한 슈테른–게를라흐 실험의 모형.
Z는 수직 방향으로의 불균일한 자기장을 나타내며 X는 수평 방향으로의 불균일한 자기장을 의미한다.

양자 정보 시스템은 불연속적이며 중첩 가능한 양자 상태를 이용한다. 양자 정보 시스템의 최소 정보 단위는 양자 비트(Quantum bit), 줄여서 큐비트(Qubit)이라고 하며 불연속적인 두 가지 상태 값을 가지고, 각 상태의 중첩이 가능하다. 위에서 살펴본 슈테른–게를라흐 실험의 전자를 예로 들면, 전자의 수직 관측 결과는 위로 향하는 경우, '↑'와 아래로 향하는 경우, '↓'의 두 가지 관측 결과를 갖고 있다. 또한 수평 자기장에 의한 관측 결과는 '→' 또는 '←' 이며, '→'를 수직 방향으로 관측했을 때 확률적으로 '↑' 또는 '↓'를 얻을 수 있으므로 '→' 상태는 '↑'와 '↓'가 중첩된 상태라고 말할 수 있다. 따라서 전자는 양자 정보 큐비트의 물리적 모델로 간주할 수 있다. 고전 디지털 시스템에서 정보의 최소 단위 bit는 는 0과 1이라는 두 개의 정보를 나타낼 수 있다. 하지만 0과 1이 동시에 존재하는 상태를 나타내지는 못한다. 따라서 고전 bit은 양자 정보로 사용될 수 없다.

양자 상태는 복소수 공간의 벡터를 이용하여 수학적으로 정의할 수 있다. 슈테른–게를라흐 실험에서 전자의 관측 결과를 예로 살펴보면, '↑' 상태를 벡터 $|\uparrow\rangle$로, '↓' 상태는 벡터 $|\downarrow\rangle$표기할 수 있으며 각각은 다음과 같은 벡터를 의미한다.

$$|\uparrow\rangle \equiv \begin{bmatrix}1\\0\end{bmatrix}, \quad |\downarrow\rangle \equiv \begin{bmatrix}0\\1\end{bmatrix}$$

'→' 상태를 수직 자기장으로 측정했을 경우 1/2의 확률로 '↑' 또는 '↓'를 얻을 수 있다. '↑' 상태의 경우에도 수



〈그림 7〉 Bloch sphere. 단일 양자 상태는 크기가 1인 벡터로, 반지름이 '1'인 구의 표면에 존재하는 한 점으로 나타낼 수 있다.

평 자기장 방향으로 측정했을 때 동일하게 1/2의 확률로 '→' 또는 '←'를 얻을 수 있다. 이런 중첩 상태를 앞에서 정의한 벡터식을 이용하여 나타내면 아래와 같이 표시할 수 있다.

$$|\uparrow\rangle = a|\rightarrow\rangle + b|\leftarrow\rangle$$

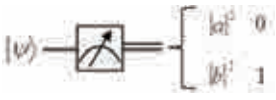
이 때, a와 b는 복소수이며 $|a|^2$와 $|b|^2$은 각각 '→'와 '←'가 관측될 확률을 의미한다. 실험에서 각 상태가 발견될 확률은 1/2이었기 때문에 이 경우 a와 b는 $1/\sqrt{2}$로 동일한 값을 갖는다. 전개의 편의를 위해 $|\uparrow\rangle$를 $|0\rangle$으로, $|\downarrow\rangle$를 로 대체하여 위 내용을 바탕으로 일반적인 양자 상태를 식으로 나타내면 다음과 같다.

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

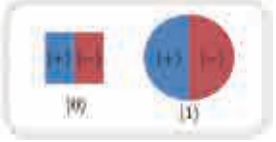
이 때, a와 b는 복소수이며 $|a|^2$와 $|b|^2$는 양자 상태를 관측했을 경우 각 상태가 관측될 확률을 의미하므로 $|a|^2 + |b|^2 = 1$를 만족해야 한다. 따라서, 양자 상태는 수식적으로 크기가 '1'인 벡터로 나타낼 수 있으며 〈그림 7〉와 같이 크기가 '1'인 임의의 단일 큐비트는 반지름이 '1'인 구의 표면에 존재하는 한 점으로 해석할 수 있다. 이 때 큐비트를 표현하는 반지름 '1'인 구를 Bloch sphere라고 한다. 슈테른-게를라흐 실험에서 수직 방향 자기장을 위로 통과한 전자 $|\uparrow\rangle$는 다시 수평 방향 자기장에 의해 $|\leftarrow\rangle$또는 $|\rightarrow\rangle$로 변환되며 전자의 각 상태 $|\uparrow\rangle$또는 $|\leftarrow\rangle$, $|\rightarrow\rangle$는 Bloch sphere의 표면에 있는 한 지점으로 나타낼 수 있다. 이처럼 연산 또는 시간 경과에 의한 양자 상태의 변화는 반지름 '1'인 구의 표면의 이동으로 나타낼 수 있으며 이러한 양자 상태의 변화는 유니터리 연산으로 기술할 수 있다. 따라서, 외부에 영향을 받지 않는 양자 시스템에서 양자 상태의 변화 또는 양자 정보의 연산은 유니터리 연산자로 정의된다.

– 양자 상태 측정 (Measurement)

슈테른-게를라흐 실험에서 불균일한 자기장에 들어가는 전자의 자기 모멘텀은 측정 후 확률에 따라 위, 아래 방향 중 하나의 상태로 결정된다. 빛의 편광의 경우 대각 편광을 수직 편광이나 수평 편광으로 측정한 후 다시 처음과 직교한 편광판을 거칠 경우 빛이 투과하지 않는 것을 통해 수직 편광 또는 수평 편광의 측정에 의해 두 편광 중 하나로 결정되었다는 것을 알 수 있다. 이러한 예와 같이 양자 상태, 또는 큐비트는 측정에 의해 측정 전의 상태와 측정 후의 상태가 다를 수 있다. 이러한 측정에 의한 정보의 붕괴는 양자 정보가 갖는 또 다른 특징 중의 하나이다. 일반적으로 양자 상태는 측정에 의해 정보가 붕괴되며 측정에 의해 붕괴된 정보는 원래의 상태로 되돌릴 수 없다. 〈그림 8〉은 양자 상태의 측정 또는 관측 과정을 회로로 나타낸 것으로 그림에서 곡선과 화살표를 포함한 네모 박스는 측정 과정, 즉 측정 연산자를 의미한다. 수직 자기장을 통과한 전자를 관측했을 경우 위쪽에서 관측되는 경우를 '0'이라 하고, 아래쪽에서 관측되는 경우를 '1'이라고 하면 임의의 큐비트 $|\psi\rangle = a|0\rangle + b|1\rangle$를 수직 자기장 방향으로 관측했을 경우 각각 $|a|^2$와 $|b|^2$의 확률로 '0'과 '1'을 얻을 수 있다. 일반적으로 임의의 양자 상태 $|\psi\rangle = a|0\rangle + b|1\rangle$에 대해 '$a$'와 '$b$'의 값을 알 수는 없다. '$a$'와 '$b$'는 관측 결과 $|a|^2$와 $|b|^2$의 확률로 관측된다는 것을 의미하여 각 상태가 $|a|^2$와 $|b|^2$의 확률로 존재하고 있다는 것을 나타내지는 않는다. 측정에서의 확률에 대해 기존 디지털 정보와 양자 상태를 비교하기 위해 〈그림 9〉과 같은 실험을 생각해 볼 수 있다. 속이 보이지 않는 상자에 원과 네모가 있고 각 각은 다시 파란색과 빨간색이 동일한 크기로 나누어져 있다고 가정해 보자. 이때 원의 면적과 네모의 면적은 상자에서 원이나 네모가 나올 확률을 의미한다. 상자에서 파란색이 나올 경우를 생각해보면 원 또는 네모의 면적과는 상관없이 언제나 1/2의 확률로 파란색을 얻게 된다. 빨간색의 경우도 원이나 네모의 확률과는 상관없이 1/2의 확률로 파란색과 동일함을 쉽게 알 수 있다. 동일한 실험을 양자 상태를 이용하여 진행하는



〈그림 8〉 측정 연산자를 이용한 큐비트 측정. 단일 큐비트의 측정 결과 $|a|^2$와 $|b|^2$의 확률로 '0'과 '1'이 관측됨



〈그림 9〉 양자 정보와 고전 정보

경우를 생각해 보자. 〈그림 9〉에서 |+>와 |−>는 각각 |→>와 |←>를 나타내며 |0>와 |1>과의 관계를 나타내면 다음과 같다.

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

|0>과 |1>을 |+>, |−>방향으로 관측했을 경우 |+>상태 또는 |−>상태가 나올 확률은 1/2로 동일하다. 〈그림 9〉에서 원과 네모를 각 각 |0>과 |1>상태라고 하면, 전체 상자는 임의의 양자 상태 $|\psi\rangle = a|0\rangle + b|1\rangle$로 생각할 수 있다. 이때, '$a$'는 원의 크기, '$b$'는 네모의 크기에 대응하는 값이다. 임의의 양자 상태 $|\psi\rangle = a|0\rangle + b|1\rangle$를 |+>, |−>로 정리하면 $|\psi\rangle = (a+b)/\sqrt{2}|+\rangle + (a-b)/\sqrt{2}|-\rangle$와 같고, 이는 $|\psi\rangle$를 |+>, |−>방향으로 측정하는 경우 |+>상태, |−>상태가 각각 $|a+b|^2/2$와 $|a-b|^2/2$의 확률로 관측되는 것을 의미한다. 고전 정보의 경우 원과 네모의 확률에 상관없이 파란색과 빨간색이 동일한 확률로 발생한 것과 달리 양자 상태의 경우 'a'와 'b'의 값에 따라 파란색과 빨간색이 나올 확률이 달라지는 것을 알 수 있다.

2. 결함 허용 양자 컴퓨팅

양자 상태는 외부 환경과의 상호 작용으로 인해 쉽게 그 정보가 변형되며, 양자 정보 연산 과정에 사용되는 연산자에서도 많은 오류가 발생한다. 현재 개발된 양자 컴퓨터는 대부분 초전도체를 이용하고 있으며 양자 컴퓨터를 운영하기 위해 절대 온도 0도에 가까운 환경을 유지하고 있다. 양자 컴퓨터가 발전함에 따라 양자 상태를 유지하고 양자 정보에 연산을 취하는 과정이 보다 정교해 지겠지만 완벽하게 무결한 양자 컴퓨터를 만들기는 쉽지 않다. 일반적으로 양자 알고리즘은 완벽한 양자 컴퓨터를 가정으로 구성되어 있다. 따라서 양자 컴퓨터에 오류가 있는 경우 양자 알고리즘으로 정확한 값을 얻을 수 없다. 결함 허용 양자 컴퓨팅은 양자 컴퓨터에 일정 수준의 오류가 존재하다라도 신뢰도 있는 양자 시스템을 구축하기 위한 방법을 제시하며, 결함 허용 양자 컴퓨터를 구성하기 위해 양자 오류 정정 부호 기법을 이용하고 있다.

양자 오류 정정 부호 기법은 양자 정보 시스템에서 발생하는 오류로부터 정보를 보호하는 기술이다. 양자 정보는 외부의 영향을 받기 쉬우며 양자 연산 과정도 오류가 발생할 수 있기 때문에 정확한 연산을 위해서는 양자 오류 정정 기법이 필수적으로 요구된다. 이미 기존 정보 시스템에는 다양한 오류 정정 기법이 존재하지만 양자 정보와 양자 정보에 발생하는 오류가 기존 정보 시스템과 차이를 가지고 있어 기존 오류 정정 기법을 양자 정보 시스템에 직접 적용할 수는 없다. 앞에서 살펴본 것과 같이 양자 정보는 측정에 의해 원래 상태가 새로운 상태로 변화, 또는 붕괴되기 때문에 기본적으로 연산 과정 도중에 정보를 관측할 수 없다. 또한 양자 정보에서 발생하는 오류는 연속적인 값을 가지고 있어 기존 디지털 시스템에서 발생하는 불연속 오류와는 특성이 다르다. 마지막으로 양자 정보는 복사가 불가능하다. ㅍ라서 정보의 복사 및 정보의 측정을 이용하는 기존 오류 정정 부호는 양자 오류 정정 기법으로 사용될 수 없으며 양자 정보의 특성을 고려한 새로운 오류 정정 기법이 필요하다.

최초의 양자 오류 정정 부호는 1995년 Peter Shor에 의해 소개되었다[3]. Shor는 자신의 논문에서 9개의 큐비트를 이용하여 단일 Pauli 오류로부터 1개의 정보 큐비트를 보호할 수 있는 기법을 제시하였다. Pauli 오류는 연산 과정에서 발생하는 오류가 Pauli 연산자로 정의된 오류이다. 1−큐비트 시스템에 대한 Pauli 연산자를 행렬을 이용하여 나타내면 다음과 같다.

$$\sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \sigma_Y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$$

각 Pauli 연산자의 특징을 살펴보면, σ_X연산자는 양자 상태 |0>과 |1>에 대해 아래와 같은 연산을 수행한다.

$$\sigma_X|0\rangle = |1\rangle, \ \sigma_X|1\rangle = |0\rangle$$

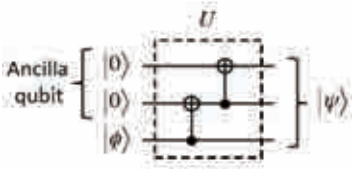
이는 고전 비트 플립 연산자와 유사한 결과를 보여준다. σ_Z연산자는 위상에 영향을 주는 연산자로 그 결과는 다음과 같다.

$$\sigma_Z|0\rangle = |0\rangle, \ \sigma_Z|1\rangle = -|1\rangle$$

임의의 큐비트 $|\psi\rangle = a|0\rangle + b|1\rangle$에 σ_Z오류가 발생하는 경우 $|\psi\rangle$는 다음과 같은 결과를 얻게 된다.

$$\sigma_Z|\psi\rangle = a|0\rangle - b|1\rangle$$

σ_Y연산자는 σ_X연산자와 σ_Z연산자가 연속적으로 수행



〈그림 10〉 3-큐비트 비트 플립 부호의 부호화 서킷

된 것과 동일한 연산을 수행한다.

$$\sigma_Y = i\sigma_Z\sigma_X$$

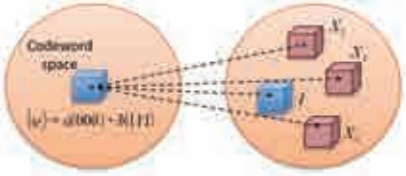
Shor 부호는 연산 과정에서 발생하는 Pauli 오류에 대해 단계적인 오류 수정 과정을 거쳐 연속적인 오류로부터 정보를 보호하는 과정을 보여준다. 이러한 특징은 Shor 부호의 구조로부터 쉽게 접근할 수 있는데 Shor 부호의 구조를 살펴보면 비트 플립 오류를 수정할 수 있는 3-큐비트 비트 플립 부호와 페이즈 플립 오류로부터 정보를 복원할 수 있는 3-큐비트 페이즈 플립 부호의 결합으로 구성되어 있다. 따라서, 3-큐비트 비트 플립 부호와 3-큐비트 페이즈 플립 부호를 통해 Shor 부호를 쉽게 이해할 수 있다.

– 3-큐비트 비트 플립 부호

3-큐비트 비트 플립 부호는 연산 과정에서 발생하는 단일 σ_X오류로부터 정보를 보호할 수 있는 양자 오류 정정 부호이다. 〈그림 10〉은 3-큐비트 비트 플립 부호의 부호화 과정을 보여준다. 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.

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

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 연산 과정에



〈그림 11〉 Pauli 오류 σ_x에 의해 서로 직교 공간으로 매핑되는 3-큐비트 비트 플립 부호의 코드워드

발생한 단일 σ_X오류의 위치에 따라 아래의 4가지 경우 중 하나의 상태가 된다.

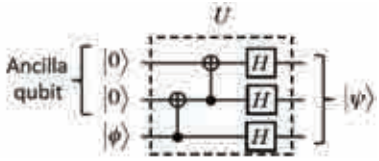
$$|\psi_0\rangle = a|000\rangle + b|111\rangle$$
$$|\psi_1\rangle = a|100\rangle + b|011\rangle$$
$$|\psi_2\rangle = a|010\rangle + b|101\rangle$$
$$|\psi_3\rangle = a|001\rangle + b|110\rangle$$

이 때, $|\psi_0\rangle$은 연산 과정에서 오류가 발생하지 않은 경우를 나타내며, $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$ 은 각각 1번 째, 2번 째, 3번 째 큐비트에서 σ_X오류가 발생한 경우를 의미한다. 위에서 오류에 영향을 받은 각 상태를 살펴보면 각각은 서로 직교하는 벡터임을 알 수 있다. 〈그림 11〉은 오류에 의해 서로 직교하는 공간으로 전개된 양자 상태를 보여준다. 서로 다른 오류에 의해 처음 상태가 서로 직교하는 상태로 전개되는 특성을 이용하여 3-큐비트 비트 플립 부호는 Projection 연산자를 이용해 오류의 유무 및 오류가 발생한 위치를 확인한다. 오류가 발생한 코드워드는 오류가 발생한 위치에 따라 서로 직교인 부분 공간(subspace)에 존재하는 벡터이다. 따라서, 전송된 정보를 서로 직교인 부분 공간으로 투영함으로써 오류의 유무 및 발생한 위치를 확인 할 수 있다. 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 σ_X오류가 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 확인할 수 있다. $\sigma_Z\sigma_Z\sigma_I$와 $\sigma_I\sigma_Z\sigma_Z$는

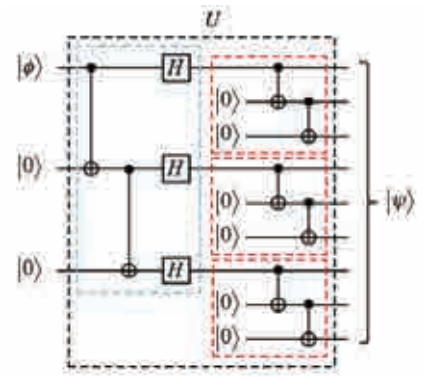


〈그림 12〉 3-큐비트 페이즈 플립 부호의 부호화 서킷

코드워드의 각 큐비트를 비교하는 연산자이다. $\sigma_Z\sigma_Z\sigma_I$는 첫 번째 큐비트와 두 번째 큐비트를 비교하며 $\sigma_I\sigma_Z\sigma_Z$는 두 번째 큐비트와 세 번째 큐비트를 비교한다. 오류가 발생한 위치에 따라 두 연산자의 수행 결과는 서로 다른 패턴을 취하게 되며, 이는 고전 선형 오류 정정 부호의 신드롬 패턴과 유사하다. 따라서 두 연산자에 의한 신드롬 패턴을 통해 코드워드에 발생한 오류의 유무 및 위치를 확인할 수 있으며, 각 신드롬에 해당하는 오류의 역 연산을 적용해 정보를 복원하게 된다.

– 3-큐비트 페이즈 플립 부호

3-큐비트 페이즈 플립 부호는 연산 과정에서 발생하는 단일 σ_Z오류로부터 정보를 보호하는 양자 오류 정정 부호 기법이다. 〈그림 12〉에서 보여주는 것과 같이 3-큐비트 페이즈 플립 부호의 구성은 3-큐비트 비트 플립 부호와 유사하다. 3-큐비트 페이즈 플립 부호의 코드워드는 $|+++\rangle$와 $|---\rangle$로 구성되는 공간에 존재한다. 따라서 임의의 1-큐비트 상태는 3-큐비트 페이즈 플립 부호에 의해 $|\psi\rangle = a|000\rangle + b|111\rangle$로 부호화 된다. $|+\rangle$ 상태와 $|-\rangle$ 상태는 σ_Z연산자에 의해 서로 플립되는 관계를 가지고 있다. 3-큐비트 페이즈 플립 부호의 경우 복호 연산은 $\sigma_X\sigma_X\sigma_I$와 $\sigma_I\sigma_X\sigma_X$에 의해 수행되며, 두 연산자는 발생한 오류의 위치에 따라 서로 다른 신드롬 패턴을 보여준다.



〈그림 13〉 Shor 부호의 부호화 서킷

– Shor 부호

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 연산 과정에서 발생한 비트 플립 오류와 페이즈 플립 오류를 개별적으로 판단하고 각 오류를 수정함으로써 전체 오류를 수정한다. 〈그림 13〉에서 파란색 점선으로 구성된 서킷은 페이즈 플립 부호와 동일한 인코딩 서킷으로 구성되어 있으며 붉은색 상자는 비트 플립 부호와 동일한 인코딩 서킷을 보여준다. Shor 부호의 복호에 사용되는 측정 연산자는 총 8개의 연산자로 구성되어 있으며 8개의 측정 연산자는 σ_X와 σ_Z 오류의 발생 유무와 위치에 해당하는 신드롬 패턴을 보여준다.

Ⅲ. 결 론

양자 정보 시스템은 양자 역학을 바탕으로 양자 정보가 갖는 고유한 특성을 이용하여 고전 정보 시스템이 가지고 있는 한계를 넘는 새로운 시스템이다. 고전 시스템으로 해결하기 어려운 많은 일들이 양자 시스템으로는 가능할 것으로 생각되고 있으며 자연계 시뮬레이션 등 기존 시스템으로 불가능한 다양한 문제를 해결할 수 있는 방법을 제시하고 있다. 이러한 양자 시스템의 가능성에 주목한 세계 각국은 현재 새로운 양자 컴퓨터 개발에 박차를 가하고 있으며 최근에는 괄목할만한 성과가 나오기 시작하고 있다. 양자 정보 시스템은 아직 시작 단계에 있다. 물리적인 구현에서 이론적인 내용까지 아직은 많은 문제를 해결해야 한다. 특히 양자 정보는 저장에서 전송까지 외부의 영향으로부터 매우 취약하다. 따라서 정확한 정보 처리를 위해 양자 오류 정정 부호는 양자 시스템의 필수 불가결한 요소이다. 본 고에서는 양자 정보의 특성을 살펴보고 결합 허용 양자 컴퓨터를 구성하기 위한 방법으로 양자 정보를 보호하기 위한 양자 오류 정정 부호를 간략하게 살펴보았다.

참고문헌

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

[2] Van Meter, R., &Horsman, C. (2013). A blueprint for building a quantum computer. Communications of the ACM, 56(10), 84-93.

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

[4] 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.

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

[6] 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.

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

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

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

[10] Kitaev, A. Y. (1997). Quantum Error Correction with Imperfect Gates. Quantum Communication, Computing, and Measurement, (Chapter 19), 181-188.

[11] Shor, P. W. (1996). Fault-tolerant quantum computation. Foundations of Computer Science, 1996. Proceedings., 37th Annual Symposium on, 56-65.

신정환

- 2005년 2월 건국대학교 공학사
- 2007년 2월 건국대학교 공학석사
- 2012년 8월 고려대학교 공학박사
- 2013년 10월~2015년 10월 University of Southern California 방문교수
- 2012년 8월~2016년 5월 고려대학교 BK21사업단 연구교수
- 2016년 5월~2017년 9월 고려대학교 스마트양자연구센터 연구교수
- 2017년 9월~현재 (주)KT 융합기술원 책임연구원

〈관심분야〉
양자 정보 이론, 통신 시스템

허 준

- 1989년 2월 서울대학교 공학사
- 1991년 2월 서울대학교 공학석사
- 2002년 8월 University of Southern California 공학박사
- 2002년 8월~2003년 2월 하이닉스 반도체(주) System IC comp 책임연구원
- 2003년 3월~2007년 2월 건국대학교 전자공학과 조교수
- 2007년 3월~현재 고려대학교 전기전자전파공학부 교수

〈관심분야〉
통신 시스템, 오류 정정 부호, 양자 정보 이론