情 報 保 護 學 會 誌
第 14 券 第 3 號, 2004. 6

양자 정보처리

안 도 열*

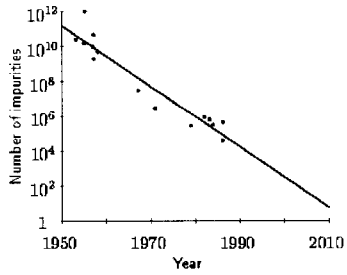
요 약

2010년경에는 칩의 고집적화로 집적회로를 구성하는 소자들에서 양자현상은 불가피 할 것으로 예상되며 오히려 이러한 양자현상을 잘 이용하여 연산이나 정보전송에 이용하기 위한 연구가 바람직 할 것으로 판단된다. 이러한 예측에 따라 비교적 최근에 양자역학을 이용한 정보처리, 특히 양자컴퓨터에 대한 관심이 증대되고 있다. 본 고에서는 이러한 양자 컴퓨팅 기술의 개요와 현황, 국내외적인 연구경쟁의 동향, 그리고 앞으로의 발전 전망에 대하여 논의하고자 한다.

Ⅰ. 서 론

21세기는 대용량 초고속 정보처리 기술에 바탕을 둔 정보화 사회가 될 것이라는 것은 주지의 사실이다. 이러한 추세를 나타내어 잘 나타내어주는 현상이 인터넷 및 가상현실에 기초한 멀티미디어의 확산이다. 이러한 정보처리기술의 근간은 컴퓨터와 통신이며 이들은 대규모 집적회로에 바탕을 두고 있다. 더 많은 정보를 더 빨리 처리하기 위하여 집적회로는 점점 더 소형화를 이루고 있으며, 인텔의 설립자인 Gordon Moore에 의하면 집적회로에 들어가는 트랜지스터의 수는 약 2년마다 배로 증가한다는 Moore의 법칙을 따르게 된다[1]. 이 법칙에 따르면 약 2020년경에는 칩의 고집적화로 소자의 크기가 20 나노미터에 접근하게 되어 양자현상을 피할 수 없게 된다. 또한 Robert Kyeses[2]는 한 비트의 정보를 저장하는 데 필요한 전자의 수를 시간의 흐름에 대하여 분석하였으며 그 결과는 아래 〔그림 1〕과 같다.

위의 〔그림 1〕은 bipolar 트랜지스터의 베이스에 도핑된 불순물의 숫자와 해당연도를 점찍은 것으로 한 개의 정보를 저장하기 위해 필요한 전자의 개수를 보여준다고 생각할 수 있다. 이 그림에 의하면 다음 20년 내에 1개의 원자에 1개의 비트를 저장할 수 있는 수준에 도달할 수 있으리라 예상할 수 있다. 위에서 열거한 두 가지 경향을 보면 집적회로를 구성하는 소자들에서 양자현상은 불가피 할 것으로 예상되며 오히려 이러한 양자현상을 잘 이용하여 연산이나 정보전송에 이용하기 위한 연구가 바람직 할 것으로 판단된다.



〔그림 1〕 한 비트의 정보를 저장하기 위해 필요한 전자의 수

이러한 예측에 따라 비교적 최근에 양자역학을 이용한 정보처리, 특히 양자컴퓨터[3,4]에 대한 관심이 증대되고 있다. 양자컴퓨터는 기존의 컴퓨터로는 풀기 어려운 계산들을 비교적 빠른 시간 내에 풀 수 있을 것으로 예측되고 있다. 여기서 말하는 시간이란 계산이 진행되는 동안을 말하는데 기존의 컴퓨터로는 이 우주가 끝날 때까지 계산을 해야 만이 풀리는 문제도 있을 수 있다. 양자컴퓨터는 이런 어려운 문제들을 현실적으로 풀 수 있는 가능성을 제시해 주고 있다. 많은 계산과정을 필요로 하는 문제의 한 예로 소인수분해 문제[5]가 있다. 소인수분해가 중요한 이유는 인터

* 서울시립대학교 전기전자 공학부 교수 (dahn@uos.ac.kr)

넷 등에 많이 쓰이고 있는 암호체계가 바로 이 소인수 분해에 기초를 두고 있기 때문이다. 현재 잘 알려진 소인수분해 알고라즘은 O(exp{(64/9)1/3(ln lnN) 2/3 })의 단계를 필요로 한다. 그러므로 이 알고리즘은 입력크기인 logN의 지수 승에 비례하는 컴퓨터 시간을 필요로 한다. 한 예로 1994년 RSA129로 알려진 129 digit number를 소인수분해 하는 데에 이 알고리즘에 기초하여 1600여대의 워크스테이션을 병렬 연결하여 문제를 해결하는 데 무려 8개월이나 걸렸다. 250 digit 라면 800,000년이 걸릴 것이며, 1000 digit라면 10^{25}년이 걸릴 것이다. 이것은 우주의 나이보다 더 많은 시간이다. 큰 숫자에 대한 소인수분해의 어려움은 공개키 방식의 암호화에 있어서 필수적인 것이었다. 은행에서 이용하는 암호코드 는 약 250 digit의 소인수분해에 의존하고 있다.

반면에 양자컴퓨터에서 사용할 수 있는 소인수분해 알고리즘의 경우는 오직 $O(\log N^{2+x})$ 의 단계를 필요로 한다. 이것은 대략 입력크기의 4승 정도가 된다. 따라서 1000 digits를 소인수 분해하는데 단지 수만 단계만 필요하며 충분히 빠른 (Pentium PC 정도의 속도를 갖는) 양자컴퓨터가 존재한다면 수 시간 내에 풀릴 수 있는 문제가 된다. 이것은 소인수분해에 근거를 둔 공개키 암호시스템 (public key crypto system)이 더 이상 유효하지 않을 수도 있음을 예측하게 한다.

II. 양자 컴퓨터의 기초

Quantum computation은 양자역학의 중첩의 원리에 의해 수행된다[6]. 간단한 quantum system은 스핀 1/2의 입자이다. 이것의 basis는 스핀다운 $|\downarrow\rangle$과 스핀업 $|\uparrow\rangle$은 각각 $|0\rangle$과 $|1\rangle$로 표현될 수 있다. 그러한 입자의 상태는 다음과 같이 기술 된다.

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

각 계수의 제곱인 $|\alpha|^2$ 와 $|\beta|^2$ 는 입자가 그에 해당하는 상태에 있을 확률을 말한다. 기존의 컴퓨터의 1비트인 0와 1은 1개의 값(value)을 나타낸다. quantum computer에서 1비트에 대응하는 것은 "quantum bit" ("qubit")이며 이것은 $|0\rangle$과 $|1\rangle$의 중첩된 상태이다. 1 byte는 8개나 16개의 qubit들이 모여 이루어진다. 이것을 스핀 1/2인 입자가 k개 있을 경우로 일반화시키면 2k의 가능한 bit-string에 대응하는 2k개의 basis states가 존재하게 된다. 이 basis vector들로 Hilbert space가 전개된다. k가 증가함에 따라 힐버트 공간의 차원은 지수적으로 증가한다. 어떤 의미에서 보면 양자컴퓨팅은 매우 작은 시스템이면서도 그 안에 존재하는 무한히 큰 벡터 공간을 이용하는 것이다. 양자컴퓨터는 중첩상태인 큐비트에 unitary operation을 수행하여 결과(output)를 만들어낸다. Unitary operation이 중첩된 상태벡터에 작동한다는 것을 제외하면 기존의 디지털컴퓨터의 작동과 비슷하다.

한 예로 8개의 큐비트로 된 상태를 생각하자. 각각의 큐비트는 $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ 상태에 있다고 하자. 이때 큐비트에 대한 측정(measurement)결과는 $|0\rangle$또는 $|1\rangle$이 각각 확률 0.5로 나타날 수 있다. 8개의 qubit로 구성된 이 레지스터는 매번 측정 시 측정결과가 0부터 255까지 같은 확률로 나올 수 있다. 따라서 완벽한 random number register라고 할 수 있을 것이다. 레지스터는 0부터 255까지 모든 숫자를 한 번에 나타낼 수 있고 결과를 측정했을 때만 단 한 개의 값이 도출된다. 이 8 bit register는 0부터 255까지 모든 숫자를 표현할 수 있으며 양자컴퓨터는 단 한 번에 모든 숫자의 연산을 수행할 수 있다. 이것을 "quantum parallelism"이라 한다. 양자 컴퓨터는 "processor"를 딱 한 번 지나면서 모든 숫자(0-255)에 대한 계산을 수행 할 수 있다. 반면에 기존의 디지탈 컴퓨터는 0부터 255까지 각각의 숫자를 한 번에 한 개씩 수행할 수 있으므로 양자컴퓨터에 비해 더 많은 과정을 거쳐야 함을 알 수가 있다. 한 예로, 64비트 컴퓨터의 경우 한 번에 1개의 64비트 숫자를 처리할 수 있지만 양자컴퓨터는 모든 64비트 수자들을 단 한번에 처리한다. 즉 2^{64}개의 연산을 단 한 번에 수행할 수가 있다.

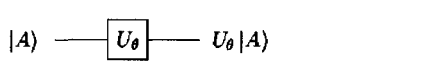
이제 양자 비트를 위한 임의의 논리게이트를 어떻게 구성하는지를 생각해 보자. 우선 one bit unitary operation으로 시작하여 Controlled NOT를 구성할 수 있다. 이들의 조합만으로도 양자비트를 위한 Toffoli 게이트[7]를 만드는데 충분하다. 단 한 개의 양자비트를 생각하자. 즉 벡터 $|0\rangle$와 $|1\rangle$을 고려해 보자. 그러면 2×2 matrix에 대응하는 가장 일반적인 unitary transformation은 다음과 같은 꼴이다.

$$U_\theta \equiv \begin{pmatrix} e^{i(\delta+\sigma+\tau)}\cos(\theta/2) & e^{-i(\delta+\sigma-\tau)}\sin(\theta/2) \\ -e^{i(\delta-\sigma+\tau)}\sin(\theta/2) & e^{i(\delta-\sigma-\tau)}\cos(\theta/2) \end{pmatrix}$$

위에서 특별히 $\delta=\sigma=\tau=0$ 으로 택하자. 이 연산자를 이용하여 우리는 다음과 같이 비트를 on off 시킬 수 있다.

$$U_\pi|0\rangle=-|1\rangle \text{ 그리고 } U_\pi|1\rangle=|0\rangle$$

위의 minus sign은 phase factor일뿐 실제 게이트들의 논리적 operation에 영향을 끼치지 않으므로 제거시켜도 상관없다. 위의 one-bit computation을 양자회로로 도식화하면 다음과 같다.



또 다른 중요한 1비트 게이트는 $U_{-\pi/2}$ 이다.

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

여기서 $q=2k$이다. 이 컴퓨터는 이제 0부터 $2k-1$까지 매우 큰 숫자의 중복상태 a를 그 상태로 갖게 된다. 이제 한 쌍의 비트 열 $|a;0\rangle$를 어떤 함수 $f(a)$로 얻어지는 한 쌍의 $|a;f(a)\rangle$로 매핑 시키는 unitary operation을 만들 수 있다고 가정하자. 그러면 중첩된 states에 작용하는 unitary operator는 다양한 입력 값 a에 대해서 다음과 같이 $f(a)$를 병렬로 계산해 낼 수 있다.

$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a;0\rangle \rightarrow \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a;f(a)\rangle$$

지금까지 우리는 힐버트 공간내의 단위벡터들의 중첩을 이용하여 주어진 정보를 처리하는 방법에 대하여 알아보았다.

1935년에 Einstein, Podolsky, Rosen (EPR)[8]은 entangled quantum system의 성질에 대하여 연구하던 중, 공간적으로 떨어져 있는 pair들간의 상관관계가 상대론적 인과율과 어긋나게 되는 현상을 발견하였다. 1960년대에 Bell[9]은 이 현상에 대하여 연구를 진행하여 entangled pair의 reality는 비국소현상 (nonlocal event)임을 보여주었다. 1990년대에 들어서 IBM의 Bennett등에 의하여 이들 얽힌 쌍의 비국소적 특성을 이용하면, 주어진 입자의 양자상태를 공간적으로 떨어져 있는 제 3자가 재현해 낼 수 있음을 보였다[10]. 이 현상을 소위 양자전송(quantum teleportation)이라고 부르는 데, 공상과학영화에서 보는 것처럼 실제 물체를 전송하는 것하고는 다르다. 우리는 이 양자전송현상을 이용해서 큐비트를 물리적 전송채널 없이 양자컴퓨터내의 게이트들간에 전송하는 데 사용할 수 있다. 한 예로 Alice 가 임의의 상태 $|\Psi\rangle=\alpha|0\rangle+\beta|1\rangle$를 공간적으로 떨어져 있는 Bob에게 전송하려 한다고 가정해자. Alice는 이를 위하여 entangle 된 입자 2와 입자 3을 준비해야 한다.

$$|\phi_{23}\rangle=\frac{1}{\sqrt{2}}[|1\rangle\otimes|0\rangle-|0\rangle\otimes|1\rangle]$$

Alice는 이들 입자들과 본래의 입자 $|\Psi\rangle$를 entangle 시킨후 입자 2를 보유하고 나머지 입자 3을 Bob에게 보낸후, 남아있는 입자계를 측정하고 그 측정결과를 통상적인 통신방식을 이용하여 Bob에게 보낸다. Bob은 Alice의 측정결과와 입자 3의 양자상태의 역변환을 거쳐서 $|\Psi\rangle$의 상태를 알게 된다. 이 과정에서 Alice가 갖고 있던 원래의 상태는 파괴된다.

Ⅲ. 문제점

양자컴퓨터를 구현하게 위해서는 우선적으로 컴퓨터 로직을 구현할 수 있는 양자게이트와 게이트의 입력이나 결과를 저장할 수 있는 양자 레지스터의 구현이 우선적으로 필요로 한다. 그리고 이러한 양자게이트나 양자 레지스터가 완전한 구동을 하기 위해서는 주변의 노이즈로부터 완전히 차단된 상태의 환경을 만들어야 한다. 실제적인 양자컴퓨터는 주변의 노이즈로부터 완전히 차단시키는 것이 불가능하여 항상 오동작할 수 있는 요인을 안고 있다. 그래서 양자컴퓨팅에서의 에러 보정을 위한, 다양한 양자에러 보정코드(QECC)[11,12]나 Decoherence Free Subspace (DFS)[13,14]를 이용한 코딩 등 많은 이론적인 방법들이 제안이 되었다. 이러한 방법들은 한 개의 에러 free인 qubit를 구현하기 위해서는 여러 개의 qubit를 이용해야 하는 등의 주어진 resource의 효용성에 어느 정도의 문제점을 안고 있다. 또 다른 방법으로는 주어진 양자상태를 유지하는데 있어서 QECC나 DFS에 처럼 redundancy를 이용하지 않고, 양자상태에 능동적으로 rf-펄스를 가해서 decoherence를 줄이는 방법이 있다[15]. 이것은 rf-펄스를 가한 경우

의 양자레지스터의 진화연산자를 정확히 계산하여 decoherence를 일으키는 항들이 많은 수의 충분히 짧은 펄스를 가한 경우 어떻게 행동하는지 살펴보므로써 가능하다.

양자계를 다루는데 있어서 decoherence는 피할 수 없는 현상이고 신뢰할 수 있는 양자컴퓨터를 구현하기 위해서는 우선적으로 양자계의 decoherence mechanism를 파악해야한다. 특히 양자게이트에서의 decoherence는 양자컴퓨터의 구현에 있어서 결정적으로 중요한 요소이므로 이의 이해가 반드시 필요하다. 지금까지 여러 가지의 양자게이트 모델들이 제안되어 있는데 그것의 decoherence에 대한 연구는 정성적인 수준에 머물러 있거나, 특별한 model를 도입해서 연구하는 정도이다. 앞으로 여러 양자게이트에서의 다양한 decoherence 현상에 대한 보다 정량적인 연구가 수행되어져야 할 것이다. 특히 양자게이트에서의 intrinsic decoherence와 nonlinear decoherence 등에 대한 연구가 필요하다[16].

Ⅳ. 양자게이트의 구현

양자 컴퓨터에 대한 알고리즘이 제안된 이후에, 양자정보 처리를 위한 기본 단위인 양자 소자의 개발에 많은 관심이 모아지고 있다. 현재까지 양자소자의 모델로, 갇혀진 이온, 원자핵의 스핀등을 이용한 것들이 제안되었다. 우선 지금까지 제안된 여러 가지 양자컴퓨터에 대해 간단히 알아보고 장단점을 비교해 보기로 한다[4].

1. Photon quantum computer

포톤의 분극이나 공간상의 위치를 양자화 시켜 큐비트를 구현하며, unitary transformation은 phase shifter, beam splitter, 또는 비선형 Kerr 효과를 이용하며, 상태벡터는 단광자를 발생시켜 얻는다. 단점으로는 크기가 크며, 비선형 Kerr효과가 큰 배질을 찾기가 힘들다는 점이다.

2. Cavity Quantum Electrodynamics

큐비트의 구현방법은 위와 동일하며, 수개의 원자가 구속된 Fabry-Perot QED Cavity를 phase shifter 및 beam Splitter와 함께 양자게이트로 사용하는 점이 photon quantum computer와 다르며, 단점으로는 스케일링이 곤란하고 크기를 줄이기 힘들다는 점이다.

3. Ion Trap

Trap 된 원자의 진동모드와 핵자기상태를 큐비트로 이용하며, 게이트의 역할은 레이저 펄스로 Jaynes-Cummings 상호작용을 유발시켜 원자의 상태를 제어한다. 단점으로는 진동모드의 수명이 극히 짧고, 이온의 기저상태를 만들기가 힘들다는 점이다.

4. NMR

분자의 수소고리에 있는 원자의 핵자기스핀을 큐비트로 이용하며, 외부에서 인가된 자장이 양자게이트의 역할을 한다. 현재 양자컴퓨터의 가능성을 보여주기 위해 가장 많이 연구된 분야중의 하나이다. 단점으로는 pure state를 만들기가 어렵고 스케일링이 거의 불가능하다는 점이다. 이외에도 조셉슨 쿠퍼쌍을 이용한 큐비트 등이 제안되었다.

최근에는 양자점을 이용한 양자소자 구현은 반도체를 이용한 나노구조를 만들 수 있는 기술이 발전하면서 많은 연구가 이루어지고 있다. 이를 위해서, 양자비트에 대한 기초를 정하고 그에 대한 제어방법과 controlled NOT gate같은 기능을 수행할 수 있는 모델을 양자점을 이용하여 구현하고자 하는 것이다. 이를 위해 여러 가지 모양의 양자점의 에너지 준위를 계산하고, 이 에너지 상태에 전자가 갇혀 있을 때, 우리가 원하는 상태로 전자를 제어할 수 있는지를 수치적인 방법을 통해 시험해 볼 수 있다.

양자점의 기저상태는 다른 상태와 잘 분리되어있기 때문에 전자가 그 곳에 채워지면 오랜 시간동안 coherence를 유지할 수 있어서 좋은 양자 비트의 기초로써 사용될 수 있다. 따라서 두 개의 양자점을 이용하면 그 곳을 채우는 전자의 위치로써 $|0\rangle$와 $|1\rangle$상태를 정의할 수 있다. 전자를 제어하기 위해서는 빛을 사용하는 방법을 이용하였다. 즉 양자점의 크기를 적당히 잘 조절하면, 기저상태뿐만 아니라 처음 들뜬 상태까지 양자점에 생기게 된다. 여기에 빛을 쏘여 주거나 초고주파 신호를 인가하면 전자는 기저상태에서 들뜬 상태로, 또는 들뜬 상태에서 기저상태를 옮아가게 된다. 이 성질을 잘 이용하면 외부의 섭동에 의해 양자점에 구속된 전자의 위치뿐만 아니라 위상까지도 조정할 수 있다. 이와 같은 구조를 사용했을 때 나타날

수 있는 문제점은 첫 번째로 원자의 떨림에 의해 나타나는 양자상태의 동요이다(decoherece). 특히 LA phonon에 의한 decohrence가 가장 커서 1 psec당 한 번 정도 전자가 산란되는 것으로 예측된다. 그러나 이러한 산란은 단지 전자가 들뜬 상태에서만 일어나므로 충분히 큰 세기의 빛을 사용한다면 해결될 수 있는 문제임이 밝혀졌다. 두 번째는 양자점의 크기를 정확히 조절해야 한다는 것이다.

위와 같이 양자점에 기초한 양자게이트의 구현을 위하여 필요한 양자점 들을 에칭으로 선택하고 나노게이트들을 양자점 근처에, 주어진 설계에 맞추어 적층할 수 있는 패터닝 기술이 필요하다. 현재 양자정보처리 연구단에서는 20nm급의 나노 게이트와 5nm내외의 크기를 갖는 양자점들을 구현할 수가 있다. 하지만 실제로 qubit을 구현하고 quantum gate의 동작을 확인하기 위해서는 양자점들의 간격이 수 나노미터내외가 되어져야 하는 데, 통상적인 self-assembly 공정을 이용해서는 이 정도의 간격을 갖는 양자점 들의 성장이 매우 힘든 것으로 나타났다. 이를 극복하기 위해서 우리는 양자점 들을 GaAs층과 InAs층을 번갈아 쌓으면서 양자점들을 수직으로 배열하는 적층구조를 시도하였다[20]. 이 경우 양자점들 간의 평균간격은 나노미터정도가 되어 양자점에 구속된 전자들간의 양자역학적인 상호간섭이 가능한 것으로 판단된다. 이때 구속된 양자상태들간의 간격이 50-60 마이크로 전자볼트가 됨을 알 수 있었다. 양자상태들간의 간격이 매우 작으므로 20 mK에서 10 tesla 이상의 자기장 상태 하에서 pulse RF측정을 한 결과 구속된 전자들의 스핀 분극이 생겨남을 발견하였다[21]. 이는 반도체 양자점을 이용해 qubit을 구현할 수가 있다는 점을 시사해 주는 것으로 앞으로 반도체구조를 이용해 quantum gate와 quantum computer의 구현이 가능할 수 있다는 것을 암시해 준다.

V. 앞으로의 전망

지금까지 우리는 양자컴퓨터가 어떻게 해서 논리적 연산을 수행하고 계산을 하는 지에 대하여 생각해 보았다. 전에 언급했던 quantum parallelism을 이용하는 알고리즘을 사용하면, 매우 긴 수열의 주기를 아주 효율적으로 찾을 수 있다는 것을 최근에 Shor가 증명하였다. 이 결과는 앞에서 언급한 소인수분해에 바로 적용할 수 있으며, 양자컴퓨터의 첫 번째 응용이 암호해독과 관련될 것이라는 예측을 하게 만들어 주었다. 양자컴퓨터의 비약적인 속도의 향상을 가능하게 하는 중요한 요소가 바로 quantum parallelism이라고 할 수 있다. Shor의 연구이후 과학 선진국에서는 모두 국가적 차원에서 지원하고 있다. 이 분야 연구비는 1995년부터 지수 적으로 증가하고 있는데 미국의 경우 1999년에 공식적인 지원비만 2000만 불이었다. 미국의 경우 국익 차원에서 국방성을 비롯하여 CIA, NSA 등에서 더 많은 지원이 있으며 이 돈들은 비 공개되어 있는 경우가 많다. 유럽 쪽은 말할 것도 없고 일본, 이스라엘, 인도, 중국, 호주 등도 국가적 차원에서 지원하고 있으며 호주의 경우 올해의 연구비가 천만불 단위라고 한다.

현재는 Shor 알고리즘과 Search 알고리즘이 양자컴퓨터를 이용하였을 때 기존의 컴퓨터보다 획기적으로 속도를 향상시킬 수 있는 유일한 알고리즘이지만 여러 연구자들이 또 다른 알고리즘을 찾고 있는 중이다. Quantum parallelism이 속도 향상에 효과가 있기 위한 전제 조건이 있다. 풀려고 하는 문제의 구조가 매우 많은 해답을 갖는 구조이어서는 안 된다. 따라서 NP-Problems처럼 복잡한 문제를 양자컴퓨터로 풀려고 한다면 성공하지 못할 것이다.

실제로 양자컴퓨터를 구현하는 데 있어서의 어려운 점은 다음과 같다. 양자컴퓨터의 연산은 작은 원자스케일의 시스템내의 Hilbert Space라는 수학적인 공간에서 이루어진다. 양자컴퓨팅(quantum computation)은 초기의 잘 정의된 상태에서 복잡한 마지막 상태까지의 궤적을 알아내는 것과 관련이 있다. 그런 궤적을 계속 추적하는 것은 가능하기는 하지만 상당히 어렵다[22]. 또한 문제가 되는 것은 양자컴퓨터가 섭동(perturbation)에 대해 대단히 민감하다는 것이다. 이것은 연산상의 궤적을 이탈시키게 한다. 섭동의 원인은 외부의 노이즈에 의해 생긴다. 그러나 외부의 노이즈에 대하여 양자컴퓨터을 고립화 시키는 데에 대한 근본적인 제한은 없다. 양자 로직 게이트들은 최근에 들어 구현되기 시작하였으며, 이제 세 개 이상의 양자 시스템을 동시에 연결하는 것을 연구하고 있는 실정이지만 가까운 시일 내에 수십 개의 qubit을 처리할 수 있는 quantum computer는 만들 수 있을 것으로 예측된다. 특히 올해 미국물리학회장이 21세기 물리학의 주요연구과제로 꼽았으며 세계 주요 언론에서도 양자컴퓨터 기술이 21세기 인류 문명에 중요한 부분이 될 것으로 간주하고 있다.

참 고 문 헌

[1] G. E. Moore, Electronics, 38, 114 (1965).
[2] R. W. Keyes, IBM. J. Res. Dev., 32, 24 (1988).
[3] J. Preskill, Lecture Notes for Physics 229 : Quantum Information and Computation, http://www.theory.caltech.edu/people/preskill/ph229 (1998).
[4] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge, Cambridge University Press, 2000).
[5] P. W. Shor, Proc. 35th Ann. Symp. Found. Comp. Sc., 1994.
[6] R. P. Feynman, Int. J. Theor. Phys. 21, 467 (1982).
[7] E. Fredkin and T. Toffoli, Int. J. Theor. Phys. 21, 219 (1982).
[8] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. 47, 777 (1935).
[9] J. S. Bell, Physics1, 195 (1964).
[10] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. 69, 2882 (1992).
[11] C. H. Bennett and P. W. Shore, IEEE Trans. Inf. Theory 44, 2724 (1998)
[12] W. Y. Hwang, D. Ahn and S. W. Hwang, Phys. Rev. A63, 022303 (2001)
[13] P. Zanardi and M. Rasetti, Mod. Phys. Lett. B11,1085 (1997).
[14] W. Y. Hwang, H. Lee, D. Ahn and S. W. Hwang, Phys. Rev. A62, 62305 (2000).
[15] K. Kim, H. Lee, D. Ahn, and S. W. Hwang, J. Korean. Phys. Soc. 37, 496 (2000).
[16] D. Ahn, J. H. Oh, K. Kimm and S. W. Hwang, Phys. Rev. A61, 052310 (2000).
[17] J. H. Oh, D. Ahn, and S. W. Hwang, Phys. Rev. A62, 052306 (2000).
[18] C. K. Hyon et al., Appl. Phys. Lett. 77, 2607 (2000).
[19] B. H. Choi et al., Appl. Phys. Lett. 78, 1403 (2001).
[20] 안도열, 창의적연구진흥사업 양자정보처리연구 2차년도 연구보고서 (2000).
[21] D, Ahn et al., Phys. Rev. Lett., to be submitted.
[22] D. Ahn et al., Phys. Rev.A 66, 012302 (2002).

〈著 者 紹 介〉

안 도 열 (Do-Yeol Ahn)

1983년 : 서울대학교 전자공학과 학사
1985년 : 서울대학교 전자공학과 석사
1988년 : University of Illinois at Urbana-Champaign 전기공학박사
전 IBM Thomas J Watson 연구소 연구원
전 포항공대 교수, 전 LG종합기술원 수석연구원
현재 : 서울시립대학교 전기전자 공학부 교수