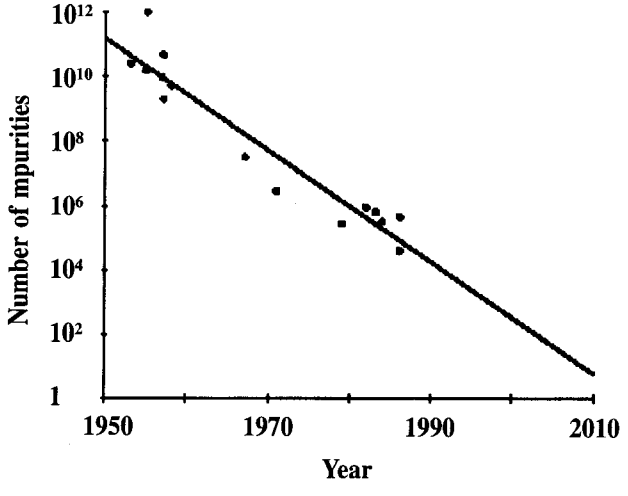
양자전산

안 도 열
서울시립대학교 양자정보처리연구단
dahn@uoscc.uos.ac.kr

1. 서론

다가오는 21세기는 대용량 초고속 정보처리 기술에 바탕을 둔 정보화 사회가 될 것이라는 것은 주지의 사실이다. 이러한 추세를 나타내어 잘 나타내어주는 현상이 인터넷 및 가상현실에 기초한 멀티미디어이 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 말하였다. 이 법칙에 따르면 약 2020년경에는 칩의 고집적화로 양자현상을 피할 수 없게 된다. 또한 Robert Kyeses는 한 비트의 정보를 저장하는데 필요한 전자의 수를 시간의 흐름에 대하여 분석하였으며 그 결과는 아래 그림과 같다.



위의 그림은 bipolar 트랜지스터의 베이스에 도핑된 불순 물의 숫자와 해당연도를 점찍은 것으로 한 개의 정보를 저장하기 위해 필요한 전자의 갯수를 보여준다고 생각할 수 있다.

위의 그림에 의하면 다음 20년내에 1개의 원자에 1개의 비트를 저장할 수 있는 수준에 도달할 수 있으리라 예상할 수 있다. 위에서 열거한 두가지 경향을 보면 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. 양자컴퓨터는 기존의 컴퓨터로는 풀기 어려운 계산들을 비교적 빠른 시간내에 풀 수 있을 것으로 예측되고 있다. 여기서 말하는 시간이란 계산이 진행되는 동안을 말하는데 기존의 컴퓨터로는 이 우주가 끝날 때까지 계산을 해야만이 풀리는 문제도 있을 수 있다. 양자컴퓨터는 이런 어려운 문제들에 많은 희망을 주고 있다. 많은 계산과정을 필요로하는 문제의 한 예로 소인부분해 문제를 검토하자. 소인수분해가 중요한 이유는 인터넷등에 많이 쓰이고 있는 암호체계가 바로 이 소인수 분해에 기초를 두고 있기 때문이다. 자연수 N을 소인수분해 한다고 하자. 예로 51688 = 23×7×13×71를 생각해 볼 수 있다. 어떤 알고리즘이 얼마나 빨리 문제를 풀수 있는가를 알기위해서는 입력에 대해 알고리즘이 완료될 때 까지의 step의 횟수를 계산하는 것이 필요하다. N 을 소인수분해 할 경우 입력값은 N이며 입력의 크기는 log N이다. 효과적인 알고리즘은 실행속도가 입력크기의 다항식으로 나타나야 한다.

현재 잘 알려진 소인수분해 알고리즘은 O(exp[(64/9)1/3(ln lnN)2/3}]) 의 단계를 필요로 한다. 그러므로 이 알고리즘은 입력크기인 logN의 지수승에 비례해서 많은 시간이 걸린다. 예를 들면 1994년 RSA129로 알려진 129 digit number를 소인수분해 하는데에는 이 알고리즘을 이용하여 세계에 있는 1600여대의 워크스테이션을 병렬연결하여 8개월이 걸렸다. 250 digit 라면 800,000년이 걸릴것이며, 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.

최근에 양자컴퓨터에서 사용할 수 있는 소인수분해 알고리

즘이 개발되었는데 오직 O(log N^{2+x})의 단계를 필요로 한다. 이것은 대략 입력크기의 4승정도가 된다. 따라서 1000 digits를 소인수분해하는데 단지 수만 단계만 필요하며 충분히 빠른 (Pentium PC 정도의 속도를 갖는) 양자컴퓨터가 존재한다면 수시간내에 풀릴 수 있는 문제가 된다. 이것은 소인수분해에 근거를 둔 공개키 암호시스템 (public key cryptosystem)이 더 이상 유효하지 않을 수도 있음을 예측하게 한다.

어떻게해서 이런 획기적인 향상이 가능한지 알기위해 가장 기본적인 양자역학 실험을 검토해 보자. 이중 슬릿 실험은 양자역학적 행동을 관찰하는 가장 대표적인 실험이다. 광원에서 포톤, 전자 또는 다른 입자들을 방출하여 2개의 슬릿에 도달한다. 이 입자들은 unitary evolution을 하여 나중에 위치가 측정된다. 우리는 두 슬릿이 모두 열려있을 때 간섭패턴을 관찰할 수 있으며 한 개가 슬릿이 닫혀 있으면 간섭무늬는 사라지게 된다. 어떤 의미에서는 입자가 두 개의 슬릿을 동시에 parrallel하게 통과한다고 할 수 있다. 만일 unitary evolution이 연산에 대응하는 것이라면 그 양자 시스템은 병렬로 계산을 수행하는 것으로 볼 수 있다.

2. 양자컴퓨터의 기본원리

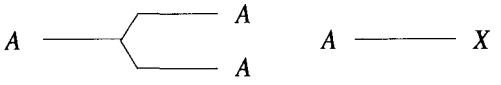
그렇다면 기존의 컴퓨터를 원자수준에서 만드는 것이 왜 그렇게 어려운 것인가? 기존의 컴퓨터의 사이즈를 최소화 하는데 가장 큰 문제는 열의 발산(dissipation of heat)이다. 1961년에 란다우는 열의 발산에 기초한 컴퓨터의 물리적 한계를 연구하였. 놀랍게도 그는 계산의 필요한 거의 모든 오퍼레이션들이 가역적 (reversible)으로 실행될 수 있음을 보일수 있었다. 이것은 곧 열을 발산하지 않고 실행될 수 있는 것을 의미한다. 디바이스가 가역적이기 위한 첫 번째 조건은 그것의 입력과 출력이 어느쪽에서도 서로 검색가능해야 한다. 이것을 "논리적 가역성"이라 한다. 논리적 가역성뿐만 아니라 디바이스가 거꾸로 실행될 수 있다면 "물리적 가역성"이라 부르고 그렇게 되면 열역학 제2법칙에 의해 열을 발산하지 않게 된다. Classical, reversible computation의 연구결과는 양자컴퓨터의 개발의 기초가 되었다.

양자컴퓨터에서 프로그램들은 입력의 unitary evolution에 의해 실행된다. 입력이란 state of system을 말한다. 모든 unitary operator들은 서로 가역의 관계가 있으므로 양자컴퓨터 에서는 항상 계산과정을 거꾸로 할 수 있다.

양자컴퓨터를 이해하기 위하여 먼저 계산에 사용되는 기본적인 논리요소를 검토해보고 기존의 컴퓨터가 어떻게 해서 계산을 하는데 있어서 적당한가를 살펴 보자. 합리적인 computation은 Boolean 수식으로 쓰여진 것이며, 모든 Boolean 수식은 고정된 논리게이트들의 집합으로 구성되어있다. AND, OR 그리고 NOT 등은 가장 기본적인 게이트 집합이다. 위의 기본 게이트로 임의의 논리게이트의 조합을 만들 수 있는 기계가 바로 universal computer이다. 게이트들에 대한 진리표가 다음 그림과 같다.

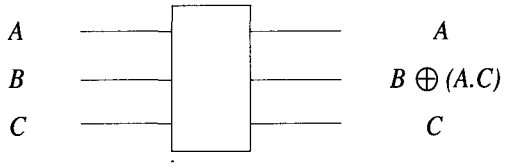
A	B	AND	OR	XOR	NOT *B*
0	0	0	0	0	1
0	1	0	1	1	0
1	0	0	1	1	1
1	1	1	1	0	0

위의 게이트들중에 AND, OR, XOR는 논리적으로 가역적이지 못하다. 왜냐하면 다대일(many-to-one) 연산이기 때문이다. 위의 논리 게이트들을 가역적으로 만들기위한 논의를 하기전에 기본 게이트와는 다른 비표준적 게이트를 검토해보자.
위의 (a)는 가역적이며 (b)는 지우기전에 정보를 백업해둔다면 가역적으로 실행될 수 있다.



(a) FANOUT (b) ERASE

다음으로는 어떤 계산에서도 이용될 수 있으며 또한 가역적인 "Toffoli gate"를 알아 보자.



Toffoli gate의 출력은 각각의 경우에 따라 다양한 게이트로 분해될 수 있다.

$$B \oplus (A.C) = \begin{cases} A.C, & \text{for } B=0 \quad \text{(AND)} \\ A \oplus B, & \text{for } C=1 \quad \text{(XOR)} \\ \overline{B}, & \text{for } A=C=1 \quad \text{(NOT)} \\ A, & \text{for } B=0,\ C=1 \quad \text{(FANOUT)} \end{cases}$$

위에서 A.B는 AND gate, A ⊕ B는 XOR gate, A는 NOT gate이다. 이 게이트는 AND, XOR.NOT, FANOUT을 입력에 따라 수행하므로 범용적이라 할 수 있다. 란다우에 의해 지적되었듯이 Toffoli gate프로시저는 ERASE가 없음으로 인해서 문제가 생긴다. 즉 점점 더 많은 게이트를 이용함에 따라 더많은 "junk(잡동사니)"비트들이 생성된다. 각각의 게이트에서 가

역성을 유지하기위해 입력값을 저장해야 하기 때문이다. 기존의 비가역적인 컴퓨터 대신에 가역적인 논리회로로 이루어진 컴퓨터는 다음과 같을 것이다.

f : a -----> (a, j(a). f(a))

여기서 j(a)는 많은 정크비트를 말한다. Bennett는 다음과 같은 방법으로 junk비트들을 중간과정을 추가함으로써 거꾸로 계산할때의 문제점을 해결하였다.

$$\begin{aligned} f : a &\rightarrow (a, j(a), f(a)) \\ \text{FANOUT} : (a, j(a), f(a)) &\rightarrow (a, j(a), f(a), f(a)) \\ \text{f+} : (a, j(a), f(a), f(a)) &\rightarrow (a, f(a)), \end{aligned}$$

위에서 f는 계산을 의미하고 f+는 역계산을 의미한다. 먼저 f가 계산되어 원하는 결과와 junk비트가 생성된다. 그리고 나서 FANOUT게이트가 그 결과를 복사한다. 그리고나서 거꾸로 계산을 실행함으로써 마지막으로 원래의 함수 f를 도출해낸다. 거꾸로 실행시 junk비트들을 제거하고 실제의 output 한 개를 제거할 수 있다.

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

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

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. 즉 qubit ==> $a|0\rangle + b|1\rangle$ a,b:정규화된 상수 이다. 1 byte는 8개나 16개의 qubit들이 모여 이루어진다. 이것을 스핀 1/2인 입자가 k개 있을때로 일반화 시키면 2k의 가능한 bit-string에 대응하는 2k개의 basis states가 존재하게 된다. 이 basis vector들은 Hilbert space를 전개하게 된다. k가 증가함에 따라 Hilber space의 차원은 exponential하게 증가한다. 어떤 의미에서보면 quantum computation은 매우 작은 시스템이면서도 그안에 존재하는 바로 이 무한히 큰 사이즈를 이용하는 것이다. quantum computer는 중첩상태인 byte에 unitary operation을 수행하여 결과(output)를 만들어낸다. unitary operation은 중첩된 states에 작동한다는 것을 제외하면 기존의 디지탈컴퓨터의 작동과 비슷하다. 한 예로 8개의 qubit로 된 1byte를 생각하자. 각각의 qubit는 $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ 상태로 있다고하자. 각각의 qubit에 대한 측정(measurement)결과는 $|0\rangle$또는 $|1\rangle$이 각각 확률 0.5로 나타날 수 있다. 8개의 qubit로 구성된 이 레지스터는 매번 측정시 측정결과가 0부터 255까지 같은 확률로 나올 수 있다. 따라서 완벽한 random number register라고 할 수 있다. 레지스터는 0부터 255까지 모든 숫자를 한 번에 나타낼 수 있고 측정했을때는 단 한 개의 값이 도출된다. 이 8 bit register는 0부터 255까지 모든 숫자를 표현할 수 있으며 quantum computer는 단 한 번에 모든 숫자의 연산을 수행할 수 있다. 이것을 "quantum parallelism"이라 한다. 부연하면 입력은 0부터 255까지의 서로 다른 수의 중첩으로 되어 있다는 것이다. quantum computer는 "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 처리할수 있지만 양자컴퓨터는 모든 64비트 숫자들을 단한번에 처리한다. 즉 2^{64}가지의 숫자를 모두 처리한다. 즉 거의 십억개가 넘는다.

이제 양자 비트를 위한 임의의 논리게이트를 어떻게 구성하는지를 생각해 보자. 우선 one bit unitary operation으로 시작하여 XOR(single tow bit)를 구성할 수 있다. 이들의 조합만으로도 양자비트를 위한 Toffoli 게이트를 만드는데 충분하다. 단 한개의 양자비트를 생각하자. 즉 벡터 $|0\rangle$과 $|1\rangle$을 고려해 보자. 그러면 2×2 matrix에 대응하는 가장 일 반적인 unitary transformation은 다음과 같은 꼴이다.

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

위에서 특별히 $\delta = \sigma = \tau = 0$으로 택하자. 이 연산자를 이용하여 우리는 다음과 같이 비트를 on off 시킬수 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 상관 없다. 위의 one-bit computation을 양자회로로 도식화하면 다음과 같다.

$$|A\rangle \text{ ——[}U_\theta\text{]—— } U_\theta|A\rangle$$

또다른 중요한 1비트 게이트는 $U_{-\pi/2}$이다.

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

이것은 스핀다운인 입자를 동일한 확률의 up과 down으로 투사시키는 역할을 한다. 스핀 1/2인 입자 k개가 초기상태에서

모두 스핀 다운인 경우를 생각해보자. 각가의 입자에다가 이 게이트를 가한다면 길이가 k인 모든 가능한 있을수 있는 비트열의 superposition을 얻게 된다.

$$|0> \rightarrow \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a>),$$

여기서 q=2k이다. 이 컴퓨터는 이제 0부터 2k-1까지 매우큰 숫자의 중복상태에 있는 a이다. 이제 한쌍의 비트열 |a;0>를 어떤함수 함수 f(a)에 대한 한쌍의 |a;f(a)>로 매핑시키는 unitary operation을 만들 수 있다고 가정하자. 그러면 중첩된 states에 작용하는 unitary operator는 다양한 입력값 a에대해서 f(a)를 (병렬적으로 수없이 많은 횟수에 걸쳐) 계산해 낼 수 있다.

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

이를 가능하게하는 unitary operator를 어떻게 구성하는가를 알기 위해서는 먼저 XOR게이트를 알아야만 한다. 두 개의 입자로 구성되어 있는 시스템의 basis state를 다음과 같은 벡터로 표현하자.

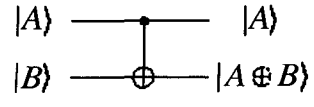
$$|00> = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01> = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|10> = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11> = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

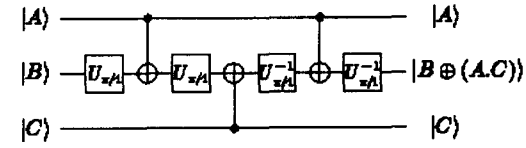
그러면 XOR게이트는 다음과 같은 unitary operator로 표현할 수 있다.

$$U_{\mathrm{XOR}} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

위의 연산자의 작용에 대해서 첫 번째 입자의 상태는 두 번째 입자의 상태를 flip하기 위한 조건적인 게이트 역할을한다. 진리표 Table 1에 주어진 XOR의 결과를 비교해 보면 동일함을 알수 있다. 양자 XOR게이트를 도식적으로 표현하면 다음과 같다.



Toffoli 게이트는 3개의 입력과 3개의 출력이 필요하다. 양자역학적으로 이것은 3개의 입자가 충돌하는 scattering process에 해당된다. 하지만 다행히도 두 입자의 scattering process로 구성될 수 있다고 한다. XOR 게이트와 U_θ 게이트로 Toffoli 게이트를 다음과 같이 구성할 수 있다.



XOR 게이트는 양자컴퓨터에서 모든 논리적 operation를 위해서도 유용할 뿐만 아니라 임의의 unitary transformation을 구성하는데 이용된다.

다음에는 스핀들을 조작하는 간단한 양자컴퓨터를 논의한다. 양자컴퓨터 코드를 작성하는 방법을 논의하고 예를 들겠다. 스핀이 1/2인 수천개의 입자가 초기에 모두가 스핀다운이듯이 잘 정의된 상태라고하자. classical computer는 1개의 스핀이나 여러쌍의 스핀들을 입력받아 그것들을 서로 조작하게 된다. 즉 one bit operation인 U 나 two bit인 XOR을 수행한다. 각각의 쌍에대해 기존의 컴퓨터 프로그램의 명령에 따라 스핀들은 반복된 처리를 받는다. 여기서 주의할점은 스핀들은 중간단계에서는 절대로 관측되어서는 안된다. quantum superposition 상태를 중간에 변경 시켜서는 안된다. 또한 어떤것도 스핀의 방향을 파괴하거나 그것들의 unitary evolution을 방해해서는 안된다. 일단 잘 정의된 싸이클이 완료된 이후에야 스핀들은 측정되게 된다. 스핀들의 측정된 방향들이 계산의 output이 된다. 그러면 과연 컴퓨터 코드는 어떻게 짤 것인가? 컴퓨터 언어는 어떤 모습을 가질것인가? 양자컴퓨터에서 가장 심각한 어려움은 모든 연산이 완전히 가려진상태에서 수행된다는 것이다. 즉 양자 정보를 중간에 엑세스할수 없고 끝까지 기다려야만 한다. 이것은 곧 기존의 언어에서처럼 양자변수(quantum variable)에 대한 조건분기를 사용할 수 없다는 것이다. 예를 들면 루프의 횟수는 양자변수에 무관하게 정확한 횟수로 반복되어야 한다. 각각의 조건분기는 각각의 경우에 따라 매번 반복되도록 쪼개져야만 한다. 또한 양자비트들에 적용된 각각의 수행문은 논리적인 가역성을 유지해야만 한다. 따라서 | a > = n과 같은 문장은 안되고 초기에 0으로 초기화된 변수에 | a > = | a > + n 처럼 증가시켜야만 한다.

3. 양자전송과 양자전산

지금까지 우리는 힐버트 공간내의 단위벡터들의 중첩을 이용하여 주어진 정보를 처리하는 방법에 대하여 알아보았다. 1935년에 Einstein, Podolsky, Rosen(EPR)은 entangled quantum

system의 성질에 대하여 연구하던중, 공간적으로 떨어져 있는 pair들관의 상관관계가 상대론적 인과율과 어긋나게 되는 현상을 발견하였다. 1960년대에 Bell은 이 현상에 대하여 연구를 진행하여 entangled pair의 reality는 비국소현상(nonlocal event)임을 보여주었다. 1990년대에 들어서 IBM의 Bennett등에 의하여 이들 entangled pair의 nonlocality를 이용하면, 주어진 입자의 양자상태를 공간적으로 떨어져 있는 제3자가 재현해 낼 수 있음을 보였다. 이 현상을 소위 양자전송(quantum teleportation)이라고 부르는 데, 공상과학영화에서 보는 것 처럼 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 $|\Psi> = \alpha|0> + \beta|1>$를 공간적으로 떨어져 있는 Bob에게 전송하려 한다고 가정해자. Alice는 이를 위하여 entangle 된 입자 2와 입자3을 준비해야 한다.

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

Alice는 이들 입자들과 본래의 입자 $|\Psi>$를 entangle 시킨후 입자2를 보유하고 나머지 입자3을 Bob에게 보낸후, 남아있는 입자계를 측정하고 그 측정결과를 통상적인 통신방식을 이용하여 Bob에게 보낸다. Bob은 Alice의 측정결과와 입자3의 양자상태의 역변환을 거쳐서 $|\Psi>$의 상태를 알게 된다. 이과정에서 Alice가 갖고 있던 원래의 상태는 파괴된다.

4. 앞으로의 전망

지금까지 우리는 양자컴퓨터가 어떻게해서 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 미국에서는 국방성이 주축이 되어 많은 예산을 양자컴퓨터 연구에 투입하고 있다. 현재는 Shor 알고리즘과 Search 알고리즘이 양자컴퓨터를 이용하였을 때 기존의 컴퓨터보다 획기적으로 속도를 향상시킬수 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 매우많은 해답을 갖는 구조이어서는 안된다. 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 이루어 진다. 양자전산(quantum computation)은 초기의 잘 정의된 상태에서 복잡한 마지막상태까지의 궤적을 알아내는 것과 관련이 있다. 그런 궤적를 계속 추적하는 것은 상당히 어렵다. 또한 문제가 되는 것은 양자컴퓨터가 섭동(perturbation)에 대해 대단히 민감하다는 것이다. 이것은 연산상의 궤적를 이탈시키게 한다. 섭동의 원인은 외부의 노이즈에 의해 생긴다. 그러나 외부의 노이즈에 대하여 양자컴퓨터을 고립화 시키는 데에 대한 근본적인 제한은 없다. 미국 로스 알라모스 국립 연구소의 연구팀들은 최근, 양자 컴퓨터가 계산 중의 오차를 보정해 낼 수 있음을 밝혔다. 아직도 어떤 과학자들은, 아주 약간의 잡음이라도 큐비트들 사이의 섬세한 얽혀짐을 파괴할 수 있고 따라서 큐비트들의 상태가 망가지므로 실용적 수준의 양자 컴퓨터는 불가능할 것이라고 주장한다. 그런데 Raymond Laflamme 를 비롯한 로스 알라모스의 과학자들에 의해, 7개의 큐비트들로 이루어진 큐바이트 (qubyte)에 대한 신뢰할 만한 계산을 수행하면서 또한 큐비트들 중의 하나가 망가질 가능성을 보정하는 알고리듬이 개발되어 주목을 받고 있다. 하지만, 실험적 수준의 양자 컴퓨터는 갈 길이 멀다. 양자 로직 게이트들은 최근에 들어 구현되기 시작하였으며, 이제 세 개 이상의 양자 시스템을 동시에 연결하는 것을 연구하고 있는 실정이다. 하지만 가까운 시일내에 수십개의 qubit을 처리할 수 있는 quantum computer는 만들 수 있을 것으로 예측된다. 아마도 20년 후에는 기존의 집적회로의 구성단위의 크기가 원자스케일로 줄어들 것이고 양자컴퓨터의 시대가 그때부터 시작될 것이다.

필자소개

안도열 박사는 서울대학교 전자공학과를 졸업(B.S '83, M.S '85)한 뒤 국비유학생으로 도미하여 1988년 University of Illinois at Urbana-Champaign에서 전기공학박사학위를 받았다. 1988년 일리노이대학으로부터 Ross Martin Award와 Robert T. Chien Memorial Award를 수상하였다. 졸업 후에는 IBM Thomas J Watson 연구소 연구원, 포항공대 교수, LG종합기술원 수석연구원 등을 역임한 후 현재 서울시립대학교 전자전기 공학부 부교수로 재직 중에 있으며 1998년부터는 과학기술부에서 주관하는 창의적연구진흥사업에 선정되어 양자정보처리연구단을 책임지고 있다. 주 연구분야는 양자전자공학과 반도체 이론이며, 최근에는 양자전산분야의 연구를 수행하고 있다. 현재까지 국제학술지 및 학술회의에 90여편의 논문을 발표하고, 6건의 미국특허를 보유하고 있으며 IEEE Senior Member이다. 1999년에는 Who's Who in the Asia500에 선정되기도 했다.