情 報 保 護 學 會 誌
第 14 券 第 3 號, 2004. 6

공개키 암호 체계와 Shor 알고리듬

이 순 칠*

요 약

양자알고리듬들 중 쇼의 알고리듬은 공개키 암호체계의 근간을 이루는 소인수분해를 고전알고리듬보다 훨씬 빨리 처리할 수 있다. 고전컴퓨터로 N자리 수를 소인수분해 하는데 걸리는 시간은 $\exp[(\ln N)^{1/3}(\ln\ln N)^{2/3})]$에 비례하지만 쇼의 양자풀이법을 사용하면 약 $(\ln N)^3$ 보다 적은 시간이 걸린다. 이 알고리듬의 핵심은 양자계의 중첩이라는 성질을 이용해서 푸리에 변환을 모든 데이터에 대해 병렬적으로 동시에 처리함으로서 주기를 빠르게 찾는다는 것이다. 이러한 양자전산의 이점은 모든 연산이 중첩된 상태에 독립적으로 작용한다는 자연계의 선형성에서 비롯된다. 고전컴퓨터에서도 병렬처리를 하지만 양자적 병렬처리를 고전컴퓨터의 병렬처리로 대신할 수는 없다. N비트로 나타내지는 2^N개의 숫자에 대해 동시에 병렬처리 하는데 양자컴퓨터는 한대면 되지만 고전컴퓨터는 2^N대가 필요하므로 비트수가 증가하면 필요한 고전컴퓨터의 수가 비현실적으로 증가하기 때문이다. 이 알고리듬의 수행으로 얻어지는 결과는 확정적인 것이 아니며 확률적으로 옳은 답을 얻는다. 어떤 수가 약수가 되는지 아닌지는 금방 확인해 볼 수 있으므로 서너 번 이와 같은 시행착오 과정을 거쳐 옳은 답을 얻는다 해도 문제가 되지는 않는다.

Ⅰ. 서 론

양자전산(Quantum computation)이란 양자역학계의 특징인 불확정성, 중첩, 얽힘(entanglement), 간섭 등을 이용하여 지금까지와는 근본적으로 다른 방식으로 정보를 처리하는 일련의 기술을 의미한다. 이는 반도체 소자의 크기가 점점 작아짐에 따라 양자적 특성을 점점 더 많이 고려해야 한다는 식의 소극적인 의미에서 벗어나, 고전계가 가지지 못하는 이러한 특성들을 적극 이용하여 고전적인 컴퓨터, 즉 우리가 지금 사용하고 있는 컴퓨터로는 풀 수 없었던 문제를 해결하는 완전히 새로운 정보처리기술이다.

양자전산의 역사는 컴퓨터에서 행해지는 연산들의 가역성에 대한 논란으로 거슬러 올라간다. 현재 우리가 사용하고 있는 컴퓨터들에서 행해지는 연산은 모두 비가역적이다. 비가역적인 연산은 필연적으로 열을 발생시킨다. 이 사실에 주목하고 있던 베네트(Bennett)는 1973년 비가역적인 튜링기계와 같은 연산을 수행할 수 있는 가역적 튜링기계를 제안하였다[1]. 그 후 베니오프(Benioff)는 시간가역성을 가지고 있는 양자계로 가역적 연산을 할 수 있음을 지적하였고[2], 재미있는 일화들로 우리나라 독자들에게도 이제는 꽤 친숙한 천재 물리학자 파인만은 1982년 처음으로 양자컴퓨터의 개념을 도입하였다[3]. 이 논문에서 파인만은 고전적인 컴퓨터로는 양자계를 효율적으로 시늉낼 수 없으나 양자컴퓨터가 있으면 가능하다는 점을 지적하였다. 구체적인 양자튜링기계 모델은 3년 후 도이치(Deutsch)에 의해 제안되었다[4]. 도이치는 이 때, 양자컴퓨터에서 훨씬 빨리 수행되는 양자 알고리듬도 하나 같이 발표하였다. 이 풀이법은 처음으로 양자컴퓨터의 효용을 증명한 것이었기는 하지만 실제적인 쓸모가 별로 없는 풀이법이었기에, 그 후 10년간 사람들은 양자컴퓨터가 근사한 것 같기는 한데 그걸 해서 뭐하냐는 반응을 보였다.

이러한 반응에 쐐기를 박고 양자전산이 폭발적인 관심을 끌게 된 계기가 된 것은 1994년 벨연구소의 쇼(Shor)가 발표한 소인수분해 풀이법[5]과 1997년의 핵자기공명에 의한 양자컴퓨터의 실제 구현이었다. 소인수분해 풀이법은 쓸모가 너무 넘쳐서 3년 후 같은 연구소의 그로버(Grover)에 의해 발표된 데이터 검

* 한국과학기술원 물리학과 교수 (soonchillee@kaist.ac.kr)

색풀이법[6]과 함께 전 세계에서 쓰이고 있는 현대암호를 모두 깰 수 있는 잠재력을 가지고 있었다. 그래서 과학 선진국들의 정부는 일제히 긴장하여 국가차원의 연구지원을 서두르기 시작했으며 쇼는 응용수학에서 필드 상에 해당한다는 너발리나 상을 수상하는 등 역사에 남을 인물이 되었다.

알다시피 소인수분해는 공개키 암호체계의 근간을 이루는데, 쇼의 알고리듬은 이 소인수분해를 고전알고리듬보다 훨씬 빨리 처리할 수 있다. 고전컴퓨터로 N자리 수를 소인수분해 하는데 걸리는 시간은 $\exp[(\ln N)^{1/3}(\ln\ln N)^{2/3})]$에 비례하지만 쇼의 양자풀이법을 사용하면 약 $(\ln N)^3$ 보다 적은 시간이 걸린다.

큰 수 n을 소인수분해하는 한 가지 방법은 임의로 선정한 난수 x에 대해 $x^a \bmod n$, 즉 x^a을 n으로 나눈 나머지가 a에 대해 주기적이라는 사실[7]을 이용하는 것이다. 이 주기가 r이라면 $x^r=1 \bmod n$이라는 뜻이므로, r을 찾았는데 운 좋게 짝수였다면 (운이 나빴다면 다음 날 다른 x로 다시 시도한다.)

$$(x^{r/2}+1)(x^{r/2}-1)=0 \mod n$$

과 같이 인수분해 된다. 이 식은 $x^{r/2}=\pm 1 \bmod n$ 이 되는 특수한 경우만 아니라면 n과 $(x^{r/2}+1)$, 혹은 $(x^{r/2}-1)$이 공약수를 가졌음을 뜻한다. 두 수의 최대공약수는 유클리드의 소거법으로 빠른 시간에 구할 수 있으므로 결과적으로 주기만 구할 수 있으면 n의 약수를 쉽게 구한다. 주기는 나머지들을 푸리에 변환하여 찾을 수 있다. 문제는 고전컴퓨터로 푸리에 변환을 할 때 비트수가 많아지면 시간이 매우 오래 걸린다는 점인데, 쇼의 알고리듬은 바로 이 푸리에변환을 양자계의 중첩이라는 성질을 이용해서 순식간에 해치우고 주기를 빠르게 찾는 해법이다. 이 알고리듬을 이해하기 위해서는 양자물리의 기본규칙을 몇 가지 알아야 한다. 이 규칙들은 상식적으로 받아들이기 어려운 것들이기는 하지만 알아야할 규칙은 몇 가지 밖에 없다. 이 규칙들을 모르면 아무리 자세히 알고리듬을 설명해도 이해할 수 없으므로 양자물리에 대해 충분한 지면을 할애하기로 한다.

II. 양자물리의 기본 가설

양자전산이 고전전산과 가장 다른 점은 0과 1을 나타내는 상태들이 중첩이 가능하다는 점과 연산은 유니타리 연산만 가능하다는 점이다. 고전컴퓨터에서 0과 1을 나타내기 위해 전압이 0볼트인 상태와 5볼트인 물리적 상태를 사용하는 것처럼 양자컴퓨터에서도 이 두 숫자를 나타내기 위해 두 가지 물리적 상태를 사용해야 한다. 양자전산에서는 비트에 해당하는 상태를 양자비트라는 뜻으로 큐빗(qubit)이라고 부르기도 하는데, 스핀이 위로 향한 상태와 아래로 향한 상태, 광자의 두 가지 편광방향, 혹은 불편하지만 원자의 기저상태와 첫 번째 들뜸 상태 등 어떤 두 개의 양자상태도 큐빗으로 사용될 수 있다.

그런데 이 상태들이 중첩이 된다는 것은 도대체 무슨 의미일까? 고전컴퓨터의 0볼트와 5볼트 상태를 생각하고 있으면 이 말은 도저히 이해할 수 없다. 0볼트면 0볼트고 5볼트면 5볼트이지 두개의 전압이 중첩된다는 것은 전혀 개념이 성립되지 않는다. 우리가 익숙한 고전적인 상태에서는 이 말이 옳다. 하지만 양자물리의 규칙이 지배하는 미시세계에서는 그렇지 않다. 사실은 물리학자들도 중첩된 상태에 대해 어떻게 이해해야 하는지 잘 모른다. 그럼에도 불구하고 이런 생각을 하게 된 역사적 사고과정을 잠시 살펴보면 이해에 도움이 된다.

지금부터 100여 년 전, 19세기가 끝나고 20세기가 시작할 무렵 물리학자들은 장차 먹고 살 걱정을 하고 있었다 한다. 하찮은 몇 가지 문제만 제외하고는 자연이 완벽하게 이해되어 더 이상 연구할 것이 없다고 생각했기 때문이다. 그런데 이 "하찮은" 실험들 중 흑체복사, 광전효과 등 몇 가지는 파동이 입자의 성질을 가진다고 가정해야만 설명이 되었다. 파동이 입자의 성질을 가진다는 가설이 유행하기 시작하자 드브로이는 역으로, 입자들도 모두 파동의 성질을 지닐 것이라는 이론을 박사학위 논문으로 발표했다. 그랬더니 사람들은 말도 안 된다는 반응을 보였고, 속설에 의하면 왕족이었던 드브로이는 할 수 없이 학위심사위원회에 압력을 넣어서 박사학위를 받았다고 한다. 그 후 이 가설은 실험적으로 증명이 되었고 드브로이는 노벨 물리학상을 받았다.

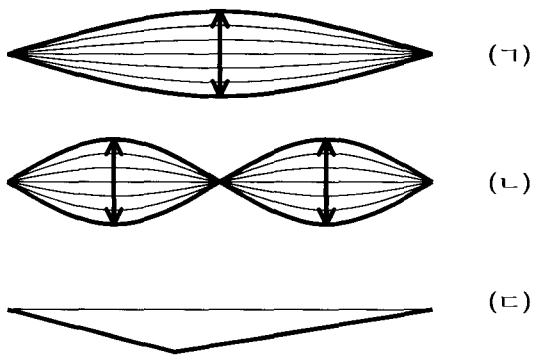
우리가 물리문제를 풀 때 결국 얻고자 하는 것이 무엇인가? 역학문제를 푸는 목적은 입자의 위치를 시간의 함수로 구하자는 것이다. 이것만 구하면 시간에 대해 미분해서 속도도 알 수 있으므로, 시간에 백년을 넣으면 그 입자가 백년 후에 우주 공간 내에서 가지는 위치와 속도를 알게 되며, 우주 안의 모든 입자들의 위치를 시간의 함수로 구해서 마이너스 백만 년을 집어넣으면 공룡이 살던 시대의 우주 모습도 이론상 완

벽히 알게 된다. 한편 파동을 연구할 때 우리가 얻고자 하는 궁극적 정보는 시간과 위치의 함수로 나타내진 파동의 진폭, 즉 크기다. 파동은 파형을 가지고 있으며 그것이 일반적으로 움직이기 때문이다. 입자의 운동은 뉴턴 방정식을 따라야 하며 파동의 크기는 파동방정식을 따라야 한다. 이것이 양자역학이 나타나기 이전의 물리가 세상을 기술하는 방식이었다.

그런데 입자가 파동의 성질을 지니고 파동도 입자의 성질을 지니고 있다면 도대체 세상만물을 어떤 방식으로 기술해야 할까? 입자의 위치는 시간이라는 한 개의 독립변수의 함수이고 파동의 크기는 시간과 위치라는 두개의 독립변수의 함수인데, 삼라만상이 파동과 입자의 성질을 모두 가진다면 더 간단한 식으로 복잡한 현상을 설명할 수는 없으므로 파동으로 세상을 기술할 수밖에는 없겠다. 이렇게 해서 어윈 슈레딩거는 물질을 나타내는 파동, 즉 물질파가 따라야하는 파동방정식을 만들었고 그 업적으로 노벨상을 탄 것은 물론 역사에 확실히 이름을 새겼다. 이 방정식은 슈레딩거 방정식라고 해서 상대성이론의 $E=mc^2$과 함께 현대물리학을 상징하는 수식이 되었으며 물질파를 표시하는 그리스문자 프사이(ψ)는 물리학에서 가장 많이 사용하는 문자가 되었다.

세상을 물질파로 기술하게 되면서 가지게 된 첫 번째 의문은 당연히 '파동함수가 무엇을 의미하는가' 였는데, 닐스 보어 및 몇몇 양자역학의 대가가 '물질파의 크기(의 제곱)은 입자가 그 시간에 그 위치에서 발견될 확률이다'라고 해석하였다. 파동의 크기를 확률로 해석하는 가설은 우리가 생각할 수 있는 가장 그럴 듯한 논리이며 이해가 가지 않는 바가 아닌데, 양자역학에서 정말 이상한 가설은 중첩과 측정에 관한 가설이다. 이해를 돕기 위해 파동의 기본성질인 중첩에 대해 잠시 이야기하기로 하자.

물질파이건, 파도 같이 우리가 일상생활에서 관찰하는 파동이건, 파동의 가장 중요한 성질은 여러 개의 파가 겹쳐질 수 있다는 것으로서 빛의 굴절, 간섭, 회절, 반사 등등 빛의 모든 성질들이 이로서 설명된다. 우리가 으뜸화음을 듣는 것은 도, 미, 솔 세음의 주파수를 가진 파동들이 겹쳐져서 공기를 통해 우리 귀를 진동시키는 현상이다. 피아노나 기타를 치면 줄이 아무렇게나 진동하는 것이 아니고 그림의 (ㄱ)이나 (ㄴ)과 같이 줄의 길이에 딱 맞는 파장을 가진 진동만 일으키며 소리를 낸다. 이런 진동을 그 줄의 고유진동이라고 부르는데, 그림(ㄱ)과 같은 모양으로 진동할 때 '도'음이 난다면 (ㄴ)과 같은 모양으로 진동하면 높은 '도'음이 들린다. 일상생활에서 관찰되는 줄의 진동 모습은 대부분 (ㄱ)과 같은 모습이지만 처음에 (ㄴ)의 외곽선과 유사한 모습을 잘 만들어 진동을 시작시키면 (ㄴ)과 같은 진동도 일으킬 수 있다. 이는 '도'에 조율된 줄로 높은 '도'소리를 만들어내는 작업이므로 물론 쉽게 일어나는 일은 아니나 가능하다.



줄의 진동 모습

실제로 피아노나 기타 줄을 치면 (ㄱ)이나 (ㄴ)과 같은 방식으로만 현이 진동하는 것이 아니고 일반적으로 (ㄱ), (ㄴ) 등의 고유진동들이 적당히 조합된 진동이 일어난다. 피아노 건반이 현을 때릴 때나 우리가 기타 줄을 튕길 때는 (ㄱ)이나 (ㄴ)과 같은 모양으로 줄 모양을 만들어 진동을 시작시키는 것이 아니고, 예를 들어 (ㄷ)과 같은 형태로 처음 진동을 시작시키는데 이런 진동 모습은 (ㄱ), (ㄴ) 등과 같은 고유진동들의 조합이기 때문이다. 물론 (ㄴ)성분보다는 (ㄱ) 성분이 훨씬 많기 때문에 높은 '도'가 아니고 '도'로 들리는 것이며, 같은 '도'음이라고 해도 피아노와 기타는 각 진동성분의 조합비가 달라서 음색이 다르다. 이렇게 여러 고유진동들이 겹쳐지는 현상을 중첩이라고 부르는데, 이 현상은 양자컴퓨터가 고전컴퓨터, 즉 지금 이 글을 쓰기 위해 사용하고 있는 컴퓨터보다 혁신적으로 빠른 주 이유이다. (ㄱ)이나 (ㄴ)같이 생긴 파동의 소리는 매우 맑지만 건조하게 들린다.

줄이 아무렇게나 진동하지 않고 고유진동이 중첩된 상태에만 있을 수 있는 것처럼, 양자계도 아무런 상태에나 있을 수 있는 것이 아니고 소위 고유상태들이 중첩된 상태에만 존재한다. 우리는 수소원자가 바닥상태에 있을 때는 그 에너지가 -13.6eV (전자볼트 : 한 개의 전자가 1V의 전압에서 하는 일)이고 들뜬 상태들의 에너지는 이 값을 자연수의 제곱으로 나누어준 값들이라는 사실을 고등학교 때 배웠다. 이 에너지 값

들은 실험과 잘 일치하며 실험에서 이들의 사이값을 얻는 일은 없다. 이와 같이 특정한 에너지를 갖는 바닥상태나 들뜬 상태들이 수소원자의 고유상태들이다. 현의 일반적인 진동이 고유진동들의 중첩인 것처럼 수소원자는 일반적으로 바닥상태나 들뜬 상태 중의 하나에만 있는 것이 아니고 이들 상태들의 중첩된 상태에 있다.

물질파도 파동의 일종이므로 중첩이 된다고 해도 이상할 것은 없지만 문제는 이 중첩된 상태를 측정할 때 일어난다. 코펜하겐해석에 따르면, 중첩된 상태를 측정하면 고유상태 중의 하나가 측정되며 그 상태가 측정될 확률은 각 고유상태가 섞인 비율에 따라 결정된다는 것이다. 중첩된 상태에 있는 수소원자의 에너지를 측정해도 역시 -13.6eV나 이를 자연수의 제곱으로 나눈 값만 나오며 어떤 값이 측정될 것인지는 중첩된 비율에 따라 결정된다는 뜻이다.

이 중첩과 측정의 가설에서 나오는 한 가지 결론은, 중첩상태는 측정 후 고유상태 중의 하나로 변화한다는 것이다. 즉 중첩이 없어진다는 뜻인데 물리학자들은 이를 축소, 또는 붕괴한다고 표현한다. 중첩된 상태는 측정 시 어떤 결과가 나올 지를 중첩된 비율에 따라 확률적으로만 알 수 있다. 그러나 측정하고 나면 그 입자의 상태에 대해 100% 알고 있다. 즉 측정된 고유상태와 나머지 상태들의 중첩된 비율이 1대 0이어야 하므로 측정된 고유상태 이외의 상태는 붕괴하여 없어졌다는 뜻이다. 기타 줄의 경우 측정을 한다는 것은 기타 줄이 내는 소리를 듣는 일이다. 우리가 사는 거대한 세상에서는 이 경우 낮은 도와 높은 도가 섞여서 들리게 되며 앞서 설명한 바와 같이 이 것이 기타 소리와 피아노 소리가 구분되는 이유이다. 그런데 양자세계에서는 우리가 기타소리를 듣건 피아노 소리를 듣건 (ㄱ)이나 (ㄴ) 같은 고유진동 중의 한 소리만 들리며, 높은 '도'가 들릴 것인지 낮은 '도'가 들릴 것인지는 두 파동이 중첩된 비율에 따라 확률적으로 결정된다. 즉 피아노를 치든 기타를 치든 그 악기들이 양자역학의 규칙에 따라야 할 정도로 크기가 작은 경우에는 우리에게 다 똑같이 들리며 다만 악기에 따라 낮은 도와 높은 도 그리도 더 높은 도들이 들리게 될 확률이 다를 뿐이다.

두개의 음이 겹쳐져 있을 때 들리는 음파가 각 음의 파동함수인 사인함수들의 합으로

$$a\sin(\omega_1 t)+b\sin g(\omega_2 t)$$

와 같이 표현되는 것처럼, 양자세계에서 중첩된 물질파도 일반적으로

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

와 같이 표현된다. 여기서 $|0\rangle$은 0을 표현하는 물리적 상태, 즉 파동함수를 의미하며 $|1\rangle$은 1을 표현하는 물리상태의 파동함수를 의미한다. 고전전산의 경우에서는 각각 0볼트와 5볼트인 상태를 의미한다고 할 수 있다. 계수들을 $|a|^2+|b|^2=1$을 만족하도록 규격화시켜 놓으면 이런 상태에 있는 양자계를 측정했을 때 0인 상태가 측정될 확률과 1인 상태가 측정될 확률이 각각 $|a|^2$과 $|b|^2$이 된다. 측정에서 0이 나왔다면 이 양자계의 상태는 $a|0\rangle+b|1\rangle$ 에서 $|0\rangle$으로 변화(붕괴)한 것이고 1이 나왔다면 $|1\rangle$로 붕괴한 것이다.

한 가지 주의할 점은 이 식에서 나오는 덧셈기호는 0과 1의 덧셈이 아니라는 점이다. 만일 두 계수가 같고 0인 상태와 1인 상태의 상대적인 크기만이 중요해서 그 상태를

$$|0\rangle+|1\rangle$$

와 같이 간단히 썼다고 해도 이 수식이 의미하는 바는 0인 상태와 1인 상태가 같은 비율로 중첩되어 있다는 뜻이지 수치 0과 1을 더한다는 의미가 아니다.

고전 컴퓨터에서의 연산은 한쪽에 걸린 입력신호에 따라 다른 쪽으로 출력신호를 내는 게이트들의 공간적 배치에 의해 이루어진다. 반면 양자전산에서는 상태를 나타내는 함수가 시간에 따라 다음과 같이

$$\psi(t)=e^{-iHt/\hbar}\psi(0)$$

로 변화한다는 사실을 이용하여 $\psi(0)$를 입력, $\psi(t)$를 출력, 그리고 연산자 $U=e^{-iHt/\hbar}$를 게이트로 사용한다. 윗 식은 슐레딩거 방정식이라고 부르는 식이다. 보통 많이 인용되는 슐레딩거 방정식은 이 식에서 시간에 의존하는 항을 빼서 간단히 한 것이다. 여기서 H는 하밀토니안이라고 불리는 연산자인데, 우리가 외부에서 큐빗으로 사용되는 양자계에 전자기파 등을 걸어서 여러 가지로 바꾸어 줄 수 있다. 진화연산자라고 불리는 U는 유니타리 연산자이다.

Ⅲ. Shor 의 소인수분해 알고리듬

이 풀이법에서는 우선, 주기를 찾기 위해 쓰일 a 값들과 $x^a \bmod n$ 값들을 같이 충분히 많은 비트로 구성된 입력레지스터에 중첩하여 저장한다. 레지스터에서 a 값들이 기록된 부분을 제 1 레지스터, $x^a \bmod n$ 값이 기록된 부분을 제 2 레지스터라 부르기로 하자. a값은 0에서 최대 q까지의 값을 사용하는데 q값은 $2n^2$와 $3n^2$사이의 값 정도를 택하는 것이 좋다. 난수 x는 소인수분해를 할 n과는 서로 소라고 한다. 우연히 택한 난수 x가 n과 서로 소가 아니라면 물론 더 좋다. 레지스터는 모든 a 값에 대응하는 상태들을 모두 중첩시킨다. 이를 위한 첫 과정으로 제 1 레지스터에는 모든 a 값들을 중첩하여 적어 넣고, 제 2 레지스터는 0으로 초기화하여 놓는다. 이 단계의 전체 레지스터의 상태를 나타내는 식은 다음과 같다.

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |0\rangle$$

이 식에서 첫 번째 $|\ \rangle$는 제 1 레지스터의 상태를 나타내고 두 번째 $|\ \rangle$는 제 2 레지스터의 상태를 나타낸다. 이렇게 중첩된 상태에 제 1 레지스터의 값에 따라 제 2 레지스터에 mod값을 계산해서 넣는 유니타리 연산을 한다. 양자세계의 연산은 중첩된 모든 상태에 독립적으로 작용하기 때문에 전체 레지스터의 상태는 다음 식과 같이 변화한다.

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |x^a \bmod n\rangle$$

예를 들어 $n=6$을 소인수분해하기 위해 $x=2$를 선택했다고 하면 a를 0에서 7까지 변화시킴에 따라 $x^a \bmod n$ 은 1, 2, 4, 2, 4, 2, 4, 2가 되며 주기 r은 2이다. 이 경우 레지스터는 다음과 같이 초기화된 후

$$\frac{1}{\sqrt{8}}(|000\rangle|000\rangle+|001\rangle|000\rangle+|010\rangle|000\rangle+|011\rangle|000\rangle+|100\rangle|000\rangle+|101\rangle|000\rangle+|110\rangle|000\rangle+|111\rangle|000\rangle)$$

mod값을 계산하는 연산에 의해 다음과 같이 준비된다.

$$\frac{1}{\sqrt{8}}(|000\rangle|001\rangle+|001\rangle|010\rangle+|010\rangle|100\rangle+|011\rangle|010\rangle+|100\rangle|100\rangle+|101\rangle|010\rangle+|110\rangle|100\rangle+|111\rangle|010\rangle).$$

여기서 레지스터는 각각 세 비트씩 총 여섯 비트로 구성되어 있다. 이 식의 각 항의 $|XXX\rangle|YYY\rangle$에서 앞의 세 비트가 제 1 레지스터를 구성하며 a의 값이 기록되어 있고, 뒤의 세 비트가 제 2 레지스터를 구성하여 $2^a \bmod 6$ 값이 기록되어 있다. 이 식의 계수는 제곱해서 모두 더하면 1이 되도록 규격화되어 있으며 제 1 레지스터의 값은 0에서 7까지가 기록되어 있고 옆에 붙은 제 2 레지스터에는 각 경우의 나머지 값들이 적혀있다.

이 식을 제 2 레지스터의 값이 같은 항에 따라 인수분해 하여 다시 쓰면

$$\frac{1}{\sqrt{8}}[|000\rangle|001\rangle+(|010\rangle+|100\rangle+|110\rangle)|100\rangle+(|001\rangle+|011\rangle+|101\rangle+|111\rangle)|010\rangle]$$

와 같이 된다. 이제 제 2 레지스터 부분에 대해서만 측정을 하면 측정에 대한 양자물리의 기본가설에 따라 $|001\rangle$, $|010\rangle$, $|100\rangle$, 이 세 가지 상태 중의 하나가 측정된다. 제 1 레지스터는 측정되지 않으므로 이 과정에서 변화가 없으며 공차가 r인 a값들에 해당하는 상태들만의 중첩으로 남는다. 예를 들어 제 2 레지스터의 측정결과가 만일 $|100\rangle$, 즉 4였다면 이 값과 다른 제 2 레지스터의 상태들은 사라지고 전체 레지스터의 상태는 다음과 같이 붕괴된다.

$$\frac{1}{\sqrt{3}}(|010\rangle+|100\rangle+|110\rangle)|100\rangle$$

측정이 끝난 후 제 2 레지스터의 상태는 한 가지 뿐이고 제 1 레지스터에는 2, 4, 6에 해당하는 상태들만이 중첩되어 있으므로 계수도 변화하였다. 제 1 레지스터의 숫자들은 공차가 2이며, mod값으로 4가 아니고 2가 측정되었어도 남은 상태들의 공차는 같다. 만일 1이 측정되면 $a=0$인 상태만이 남게 되지만 a값을 충분히 늘임으로서 이런 일을 방지할 수 있다. 이렇게 우리가 찾는 주기를 가진 등차수열을 구했다면 목적의 반은 성취한 셈인데, 이 과정을 되돌아보면 양자세계의 중첩과 측정의 특별한 속성 덕임을 알 수 있다.

이 상태에서 제 1 레지스터의 상태를 읽을 수 있다면 공차가 2임을 당장 알아차릴 수 있으므로 즉시 주기를 구할 수 있겠지만, 안타깝게도 양자상태는 읽으려하면 전술한 바와 같이 중첩된 상태 중 하나가 읽혀질 뿐이다. 즉 제 1 레지스터를 측정하면 2나 4나 6 중의 하나가 측정될 뿐이므로 주기에 관한 아무런 정보도 얻을 수 없다. 그러므로 등차수열을 푸리에변환하면 공차에서의 함수값이 크게 나온다는 사실을 이용한다. 양자푸리에 변환은 다음과 같이 정의되는 연산이다.

$$|a\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i a c/q} |c\rangle$$

고전적인 이산푸리에변환 알고리듬이 $\{b_1, b_2, b_3, \ldots\}$의 수열을 $\{c_1, c_2, c_3, \ldots\}$와 같이 바꾸어 준다고 하면 이에 해당하는 양자푸리에 변환은

$$b_1|000\rangle + b_2|001\rangle + b_3|010\rangle + \cdots$$

와 같이 중첩된 상태를

$$c_1|000\rangle + c_2|001\rangle + c_3|010\rangle + \cdots$$

와 같이 변환시킨다. 이와 같은 연산은 유니타리임을 쉽게 증명할 수 있으며 양자전산에서는 어떤 유니타리 연산도 할 수 있음이 증명되어 있다. 어떻게 이 연산을 구현하는가의 문제는 이 글의 범위를 넘어서므로 생략하기로 한다. 이렇게 푸리에변환된 데이터의 상태는 주기에 해당하는 상태의 계수가 두드러지게 크기 때문에, 측정하면 그 상태가 측정될 확률이 다른 상태들보다 높게 되고 따라서 측정된 결과 값에서 주기를 알 수 있게 된다. 우리의 예에서는 주기 2에 해당하는 $|010\rangle$상태의 계수 c_3가 다른 계수들보다 훨씬 클 것이므로 측정 시 2라는 값을 얻을 확률이 가장 크다.

높은 확률로 측정된다는 말에서 짐작할 수 있듯이 양자 소인수분해 알고리듬은 반드시 옳은 결과를 얻는 것이 아니고 확률적으로 얻는다. 따라서 틀린 결과를 얻을 수도 있다. 그러나 어떤 수가 약수가 되는지 아닌지는 금방 확인해 볼 수 있으므로 서너 번 이와 같은 시행착오 과정을 거쳐 옳은 답을 얻는다 해도 크게 문제가 될 일은 없을 것이다. a값을 큰 수까지 시도할수록 물론 정확한 값을 알게 될 확률이 높아진다. 이산푸리에변환식을 생각해보면 금방 알게 되는 일이지만, 여기까지의 과정에서 얻게 되는 수치는 정확히 말하자면 주기 r이 아니라 l/r이다. l 와 r 각각을 얻으려면 연속분수전개방법을 쓰면 된다. 쇼의 소인수분해 알고리듬에 대한 더 자세한 설명은 참고문헌 8의 서적들에서 볼 수 있다.

위의 계산과정을 음미해보면 이 양자 소인수분해 알고리듬이 고전적인 소인수분해 알고리듬보다 비약적으로 빠를 수 있는 이유는 측정이라는 행위에 의해 등차수열이 한번에 걸러진다는 점과 푸리에 변환이 한번의 연산으로 얻어지기 때문임을 알 수 있다. 즉 양자세계의 가장 중요한 특징인 중첩과 측정에 의한 붕괴, 이 두 가지 성질 때문이다. 중첩된 양자상태의 이점은 모든 연산이 중첩된 상태에 독립적으로 작용한다는 자연계의 선형성에서 비롯된다. 이렇게 중첩에 의해 연산을 평행하게 동시에 수행하는 과정을 고전전산에서의 병렬처리처럼 양자병렬처리라고 부르며 고전 알고리듬보다 우수한 성능을 보이는 모든 양자 알고리듬들이 공통적으로 사용하는 성질이다. 같은 병렬처리라고 해도 양자병렬처리를 고전컴퓨터의 병렬처리로 대신할 수는 없다. N 비트로 나타내지는 2^N개의 숫자에 대해 동시에 병렬처리 하는데 양자컴퓨터는 한대면 되지만 고전컴퓨터는 2^N대가 필요하므로 비트수가 증가하면 필요한 고전컴퓨터의 수가 비현실적으로 증가하기 때문이다.

양자세계의 또 하나의 특징인 측정시의 붕괴는 항상 유리하기만 한 것은 아니다. 예를 들어 비트 오류 수정의 경우, 이 붕괴현상 때문에 고전적인 경우보다 훨씬 노력이 많이 든다. 고전전산에서는 7비트의 통신오류를 해결하기 위해 1비트의 패리티 비트를 써서 해결하지만 양자전산에서는 1비트의 통신오류를 해결하기 위해 4비트의 추가비트를 써야 한다. 이는 양자세계가 더 잡음에 민감하다는 것이 주 이유는 아니다. 고전전산에서 패리티 비트를 사용할 때는 우선 7비트에서의 1의 수를 읽는다. 그러나 양자전산에서는 비트를 측정하면 상태가 변화(붕괴)하므로 데이터 비트가 어떤 상태에 있는지 전혀 모르는 채로 오류를 수정해야 하기 때문에 어렵다. 데이터의 상태를 전혀 모르면 언뜻 오류수정 자체가 불가능할 것같이 느껴지므로 4비트의 추가비트로 수정된다는 사실만도 놀랍다.

V. 결 론

양자알고리듬은 쓸만한 것이 많지 않다. 고전적이든

양자적이든 새로운 알고리듬을 생각해 낸다는 것 자체가 쉽지가 않을 뿐 아니라 양자 알고리듬은 고전 알고리듬보다 효율적이어야 한다는 조건이 추가로 붙기 때문이다. 양자알고리듬을 다루려면 양자역학과 알고리듬 모두를 잘 알고 있어야 한다. 그러므로 정보과학을 전공하는 사람이 양자역학을 공부하거나 물리학을 전공한 사람이 정보과학을 공부해야 하는데 당연히 전자가 쉽다. 양자역학 지식은 초보적인 가설 몇 가지만 명확히 이해하고 있으면 충분하므로 정보과학기술자들은 여태까지 다루어왔던 규칙만 몇 가지 바꾸어 기존의 기술들이 어떻게 변화하는지 조사하면 된다. 반면 물리학자들은 양자역학은 필요이상 알고 있지만 정보과학에서 무엇이 문제가 되는지, 어떻게 처리하고 있는지 전반적인 지식을 단시일에 얻을 수 없다. 체스를 잘 두는 사람이 장기도 단시일에 잘 두게 되는 것이지 장기 규칙에 대해 연구하는 사람이 장기를 잘 두는 것이 아닌 것과 마찬가지이다. 양자정보과학 분야에서 가장 이름이 난 사람들은 대부분 정보과학을 전공한 사람들이었다. 글을 마치기 전에, 우리나라에서도 양자정보과학이 세계적인 수준에 오르려면 정보과학기술자들이 이 분야를 연구해야 함을 강조하고 싶다.

참 고 문 헌

[1] C. H. Bennett, IBM J. Res. Dev. 6, 525 (1973).

[2] P. Benioff, J. stat. Phys. 22, 563 (1980).

[3] R. P. Feynman, Int. J. Theor. Phys. 21, 467 (1982).

[4] D. Deutsch, Proc. R. Soc. Lond. A400, 97 (1985).

[5] P. Shor, Proceedings of 35th Annual Symposium on Foundations of Computer Science, 124 (1994).

[6] L. K. Grover, Phys. Rev. Lett. 79, 325 (1997).

[7] D. E. Knuth, The Art of computer Programming, Vol. 2: Seminumerical Algorithms, 2 ed. (Addison-Wesley, Reading, MA, 1981).

[8] M. Nielson and I. Chuang, Quantum Computation and Quantum Information (Cambridge Univ. Press, 2000).

A. John, R. Peter, "Electric Communication Development," Communications of the ACM, 40, pp. 71-79, May 1997.

〈著 者 紹 介〉

이 순 칠 (Sun-Chil Lee)

1976~1980년 : 서울대학교 물리학 학사

1980~1981년 : 서울대학교 물리학

1981~1986년 : Northwestern Univ. 물리학 박사

1986~1987년 : 한국과학기술원 전기전자과 위탁연구원

1987년~현재 : 한국과학기술원 물리학과 교수

1997~1998년 : Bell lab consultant