양자 원리와 컴퓨터: 양자컴퓨터

DOI: 10.3938/PhiT.21.052

김 재 완

Quantum Physics and Information Processing:
Quantum Computers

Jaewan KIM

The 2012 Nobel Prize in physics was awarded to two physicists who manipulated and measured of individual quantum systems and paved the way to the era of quantum information processing and quantum computing. Quantum physics, which provided hardware systems such as lasers and semiconductor devices to the field of information technology in the 20th century, will provide the field of information technology in the 21st century with not only hardware but also software and operating systems based on quantum principles. This article summarizes the status of quantum computers at the beginning of 21st century for the general public.

양자물리학의 시작

막스 플랑크(Max Planck)는 뜨거운 물체에서 나오는 빛 에너지의 색분포 즉 스펙트럼을 설명하기 위해 양자물리학을 발명하였다(1899년). 쇠가 뜨거워지면 붉게 빛나기 시작하다가 온도가 더 높아지면 주황, 노랑으로 빛의 파장이 짧아지면서 빛의 주파수가 높아진다. 빛이 물질과 에너지를 서로 주고받을 때 주고받는 빛 에너지의 양(量=quantity)은, 흔히 볼 수 있는 흐르는 물처럼 연속적인 양이 아니라, 수도꼭지에서 겨우 새어 나와 한 방울씩 떨어지는 물방울처럼 덩어리져 있다. 즉 빛 에너지는, 빛 주파수 ν ¹⁾에 비례하는 최소 단위의 에너지 덩어리 또는 에너지 양자(量子) $h\nu$ 의 정수배로만 주고받을 수

저자약력

김재완 교수는 미국 텍사스 휴스턴대학교 물리학과에서 이학박사 학위를 받은 후, 삼성종합기술원 계산과학팀 전문연구원/팀장, 카이스트 물리학과 연구원/교수를 거쳐 2002년부터 고등과학원 계산과학부 교수로 재직 중이다. (jaewan@kias.re.kr)

있다는 것이다. 여기서 비례상수 h 는 플랑크 상수라고 부른다.

아인슈타인도 빛의 에너지가 덩어리져 있다는 광양자(光量子) 가설을 이용하여, 빛을 받은 금속에서 전자가 튀어 나오는 광전효과(光電效果)를 설명하였다(1905년). 광전효과는 다양한 감지장치, 디지털카메라 등에서 빛을 전기에너지로 바꿔주는 원리이다.

플랑크와 아인슈타인의 양자물리학은, 1920년대 하이젠베르크의 불확정성 원리와 슈레딩거의 파동방정식 등을 거치면서 새로운 모습을 띠게 된다. 결정론적인 뉴턴역학으로부터 확률론적인 양자역학으로 전환이 일어나면서 빛과 물질에 대해 더욱더 본질적인 이해가 가능하게 되었다. 물질현상의 기본인 화학 주기율표의 원리도 양자물리학에 의해서 설명됨으로써 연금술을 의미하는 alchemy가 화학이라는 chemistry로 본격적인 탈바꿈을 하게 되었다. 1899년 미국의 특허청장이던 찰스 두엘(Charles Duell)이 “이제 발명될 만한 것은 모두 발명되었다(Everything that can be invented has been invented.)”고 했던 말이 무색하게도 양자물리학을 바탕으로 본격적인 발명이 이루어졌다. 현재 정보통신기술의 바탕이 되는 레이저나 반도체 등은 모두 1899년 양자물리학이 탄생된 이후 발명되었다.

정보처리 기계의 시작

그런 한편 1900년에 대수학자 힐베르트(Hilbert)는 20세기를 맞으면서 20세기에 해결되어야 할 수학문제 23개를 제시하였는데, 그중 하나인 ‘수학 명제의 기계적인 증명이 가능한가’ 하는 문제는 괴델(Gödel)의 불완전성 정리와 튜링(Turing)의 튜링기계(Turing machine)로 이어졌다. 튜링기계는, 0과 1 비트(bit)로 나타낸 정보를 저장할 수 있는 무한히 큰 저장장치(infinitely long storage)와 이 저장장치 위를 오가는 유한연산장치(finite state machine)로 이루어져 있다. 유한 연산장치는 무한히 긴 정보저장장치에서 데이터를 읽어 들여, 연산장치 자신이 가진 데이터와 함께 연산을 한 후, 자신의 데이터를 고쳐 쓰고, 저장장치에도 새로운 값을 기록한 후, 저장장치 위의 새로운 위치로

1) 數 즉 number를 뜻하는 n에 해당하는 그리스문자 “누”.

Fig. 1. Turing machine; model of modern digital computers.

옮겨 간다. 이 튜링기계는 현대 디지털 컴퓨터의 원형이 되었다. 한때 워크스테이션 컴퓨터 생산업체로 유명하던 DEC社(Digital Equipment Corporation)를 창업한 케네스 올슨(Kenneth Olsen) 사장은 1977년 “개인이 집에 컴퓨터를 가지고 있을 필요는 없다(There is no reason for any individual to have a computer in their home.)”고 했지만, 반도체 기술의 발전에 힘입어 사람들은 이제 집뿐만 아니라 책상 위에 또 손바닥에 컴퓨터를 가지고 살아가고 있다.

나노기술의 시작

1959년 파인만(Feynman)은 캘리포니아 공대에서 열린 미국물리학회에서 “There is plenty of room at the bottom.”이라는 강연으로 나노기술(nanotechnology) 시대의 비전을 제시하였다. 원자나 분자 같은 아주 작은 영역에 엄청나게 많은 정보를 기록하고 처리할 수 있다는 말이었다. 인텔(Intel)의 창업자 무어(Moore)가 제시한 ‘반도체의 집적도가 3년에 4배로 증가한다’는 무어의 법칙은 나노기술의 로드맵이 되었지만, 디지털 기술을 한없이 작은 그릇(hardware)에 실는 데에는 근본적인 한계가 있다. 디지털 정보는 0과 1이 분명히 구별되어야 하지만, 나노 이하의 영역에서는 하이젠베르크의 양자불확정성원리에 의해 0과 1의 구분이 모호해지는 양자물리학의 세계로 접어들기 때문이다. 0과 1의 구분이 모호해진다는 것은 디지털 컴퓨터에서 치명적인 약점이지만, 어쩌면 하나의 비트(bit)로 0과 1을 동시에 나타낼 수 있는 셈이 된다.

양자컴퓨터 아이디어의 시작

1983년 파인만은 새로운 컴퓨터의 개념을 제안하였다. 양자화학이나 강한 상호작용을 연구하는 물리 문제 중에, 전자(電子 electron) 한두 개 정도가 아니라 여러 개의 전자를 다루는 양자다체문제(量子多體問題, quantum many-body problem)는 어렵기로 유명하다. 아주 간단한 경우만 생각하여 격자점을 하나씩 차지하고 있는 전자의 스핀(spin) 상태가 up과 down 두 가지가 가능하다고 하자. 전자가 하나이면 up(1이라고 표시하자)

과 down(0이라고 표시하자) 두 가지 상태만 가능하지만, 두 개이면 00, 01, 10, 11 등 네 가지 상태, 세 개이면 000, 001, 010, 011, 100, 101, 110, 111 등 8가지 상태, 이런 식으로 기하급수적으로(지수함수적으로 exponentially) 경우의 수가 늘어나, 30개의 전자가 있으면 2의 30승, 약 10억의 30승, 즉 경(京, 10억의 16승)의 100조(兆) 배의 전자 상태가 가능하다.

디지털 컴퓨터 방식은, 계산능력을 높이기 위해 개별 프로세서의 계산속도와 계산용량을 높이는 방법과 함께 여러 개의 프로세서를 연결하여 쓰는 병렬 컴퓨터 방식을 쓴다. 그렇지만 N 개의 프로세서를 연결한 병렬디지털컴퓨터는 최대 N 배 빠른 계산을 할 수 있을 뿐이다. 즉 기껏해야 선형적으로 계산능력이 늘어나는 병렬컴퓨터 방식이다. 이것조차도 프로세서들 사이에 데이터를 교환하는 커뮤니케이션에 따른 제약 때문에 알고리즘에 따라서는 겨우 몇 배 이상 빨라지지 않는 경우도 있다. 이런 병렬디지털컴퓨터로 지수함수적으로 계산량이 늘어나는 양자다체문제를 해결한다는 것은 불가능하다. 파인만이 1983년 로스알라모스 연구소에서 행한 강연 “Tiny Computers Obeying Quantum Mechanical Laws”는 바로 양자다체문제를 ‘양자역학의 법칙을 따르는 아주 작은 컴퓨터들’ 즉 양자컴퓨터로 해결하자는 제안이었다.

디지털컴퓨터는 정보의 단위인 비트의 수가 늘어나면 계산공간이 비트 수에 기껏해야 선형적으로 비례하여 늘어날 뿐이지만, 양자컴퓨터는 정보의 단위를 0과 1이 동시에 될 수 있는 양자비트(quantum bit) 또는 큐비트(qubit)라고 할 때에 큐비트 수가 늘어남에 따라 계산공간이 지수함수적으로 늘어난다. 이를 양자병렬성(quantum parallelism)이라고 한다.

디지털컴퓨터에서 양자컴퓨터로의 발전은, 수학이 실수(實數, real number) 체계에서 복소수(複素數, complex number) 체계로 확장하면서 엄청난 발전을 이룬 데에 비할 수 있다. 실제로 양자컴퓨터의 큐비트는 0이나 1이 아니라, 0과 1의 중첩(重疊, superposition)을 복소수 계수를 이용하여 나타낸다. 복소수 계수는 0이나 1이 측정될 확률의 제곱근, 즉 확률진폭을 나타낸다.

양자컴퓨터용 알고리즘

여기서 한 가지 주의할 점은, 양자컴퓨터의 큐비트가 N 개이면 중간 계산과정에서 계산공간은 2의 N 승으로 커지지만, 계산의 시작과 끝은 여전히 N 개의 비트로 나타내어진다는 점이다. 따라서 양자컴퓨터의 양자병렬성을 제대로 활용하기 위해서는 양자 알고리즘을 잘 설계해야 한다.

현재 많이 알려진 양자 알고리즘으로는 양자다체문제와 함께, 쇼어(Shor)가 1994년에 만든 큰 수의 양자소인수분해(素因數分解, factoring) 알고리즘, 그로버가 1996년에 만든 양자검색(檢索, search) 알고리즘 등이 있다. 소인수분해 문제는 컴퓨터의 능력을 테스트하는 문제로서 많이 활용이 되어서, 새로운 슈퍼

Fig. 2. Linear parallelism of digital computers and exponential parallelism (or quantum parallelism) of quantum computers.

컴퓨터가 나오면 얼마나 빨리 아주 큰 수를 소인수분해하는가 하는 것으로 그 컴퓨터의 능력을 자랑한다. N 자리의 숫자를 소인수분해하는 데에 걸리는 시간은, 디지털컴퓨터로는 N 의 지수 함수에 가까울 정도이지만(superpolynomial), 양자컴퓨터로는 N 의 3승 정도에 지나지 않는다. 현재 널리 쓰이고 있는 공개키 암호방식은 큰 수의 소인수분해가 매우 어렵다는 사실을 이용한 것이기 때문에, 양자컴퓨터가 실용화되면 이 방식을 이용한 암호는 쉽게 풀려버릴 위험에 놓인다. 필자는 양자물리학과 통신보안의 관계를 ‘병 주고 약 주는’ 관계라고 표현하는데, 양자컴퓨터가 현재 공개키암호방식을 채용하고 있는 통신보안에 큰 위협이 되는 한편, 양자물리학은 절대도청이 불가능한 양자암호키 전송방식을 제공하기 때문이다. 양자 소인수분해 알고리즘의 핵심적인 부분에 양자 푸리에변환(Fourier transform)이 있는데, 이처럼 양자컴퓨터는 여러 숫자들의 전체적인 특성을 한꺼번에 파악하는 데에 큰 이점이 있는 것으로 보인다.

디지털컴퓨터 방식으로 N 개의 데이터에서 하나를 찾는 데에 걸리는 시간은 거의 데이터 크기 즉 N 에 비례하는 정도인데, 양자컴퓨터의 양자검색 알고리즘으로 $\sqrt{N}$ 정도 걸린다. 예를 들어, 만 개의 데이터에서 조건에 맞는 딱 하나를 찾을 때에, 운이 좋으면 한 번에 찾을 수도 있지만 운이 나쁘면 끝에 가서야 찾을 수 있어서, 평균 5천 번 정도 데이터를 읽어야 하지만, 양자컴퓨터는 데이터를 한꺼번에 처리함으로써 100번 정도만 데이터를 읽으면 조건에 맞는 데이터를 찾을 수 있다.

양자컴퓨터의 오류

양자컴퓨터라는 아이디어가 이렇게 대단해 보이지만 1990년대 중반까지만 해도 대부분의 사람들이 신기하지만 실용화할 수 없는 아이디어라고 여겼다. 한때 0과 1을 이용하는 디지털 컴퓨터 방식과 경쟁하던 계산방식으로 실수 아날로그(analogue) 컴퓨터 방식이 있었는데, 아주 제한적인 용도 이외에는 쓰이지 않게 되었다. 정보

처리의 연산은 일반적으로 비선형(非線型, nonlinear)적인데, 아날로그 컴퓨터처럼 실수를 사용할 경우 비선형성에 의한 혼돈(chaos) 현상이 나타나면 아주 작은 오류(error)가 순식간에 전체 계산을 망쳐 놓게 된다. 이에 비해 디지털 컴퓨터에서는 비트 0이나 1을 나타내는 전압이나 전류에 조그만 차이가 생기면 쉽게 0이나 1로 되돌려 놓을 수도 있고 여러 가지 오류수정 알고리즘(error-correction algorithm)이 가능하다. 양자컴퓨터의 큐비트를 나타내는 데에는 0과 1의 계수로 복소수가 쓰이는데, 복소수는 다시 두 실수로 나타내어지기 때문에 아날로그 컴퓨터처럼 한동안 오류수정이 불가능하다고 여겨졌다. 그러나 1996년 쇼어 등이 양자컴퓨터의 오류를 수정할 수 있는 알고리즘을 만들어 냈으로써 이제 양자컴퓨터는 원리적으로 실현 가능한 아이디어가 되었다.

양자컴퓨터의 실현

이렇게 양자컴퓨터에 관한 이론적인 아이디어가 구체화되어 가는 한편, 양자컴퓨터를 실험적으로 구현할 수 있는 기술이 1980년대 이후 형성되고 있었다. 그 중 대표적인 것이 2012년 올해 노벨 물리학상을 수상한 와인랜드(Wineland)의 이온덫(ion trap)과 아로시(Haroche)의 공동QED(空洞, cavity, quantum electrodynamics)이다. 디지털컴퓨터가 주로 반도체 실리콘을 바탕으로 만들어졌지만, 양자컴퓨터가 어떤 방식으로 구현될지 아직은 다양한 제안을 속에서 모색 중이다.

디빈첸조(DiVincenzo)는 양자컴퓨터를 구현하기 위한 다섯 가지 요건을 제시하였다.

첫째, 분명히 구별 가능한 두 상태(0과 1)를 가진 양자계(量子界)로서 확장 가능해야(scalable) 한다. 즉 여러 개의 큐비트를 쉽게 만들 수 있어야 한다. 한때 NMR(핵자기공명) 양자컴퓨터가 유망해 보였지만 확장 가능성이 없다는 점에서 미래의 양자컴퓨터 리스트에서 제외되고 있다.

둘째, 기준이 되는, 예를 들면 0, 양자상태를 만들 수 있어야 한다. 흔히 컴퓨터 프로그래머들이 쓰는 GIGO(garbage in, garbage out)라는 표현이 있다. 시작 데이터가 제대로 준비되지 않으면 계산결과는 엉터리다.

셋째, 필요한 양자연산 게이트(gate)들을 구현할 수 있어야 한다. 하나의 큐비트를 여러 상태로 회전하는 단일큐비트 게이트(single qubit gate)는 비교적 쉽게 구현할 수 있지만, 두 개의 큐비트에 작용하여 얽힘(entanglement)을 만드는 두 큐비트 게이트(two-qubit gate)는 일반적으로 구현하기가 쉽지 않다. 1995년 졸리(Zoller)와 시락(Cirac)은 이온덫에서 두 큐비트를 구현하는 방법을 제안하였고, 바로 같은 해에 와인랜드는 이를 직접 구현하였다. 와인랜드는 현재의 원자시계보다 100배 정도 정확한 시계를 만들기 위해 축적해온 기술이 바로 두 큐비트 양자게이트에 필요한 기술이라는 것을 알아채고 단 몇

Fig. 3. DiVincenzo's five prerequisites for realizing quantum computers.

Fig. 4. Cluster state: Each qubit on virtual lattice site is prepared in $|+\rangle$ state, which is a linear superposition of 0 and 1 with equal amplitudes, then Controlled-Z operations are applied to two neighboring qubits. For example, two qubits in $|+\rangle$ states are equal-amplitude superposition of 00, 01, 10, and 11 states. Controlled-Z operation on these two qubits preserves the sign of 00, 01, and 10 states, but flips the sign of 11 state from $+$ to $-$ (by changing the phase), and maximally entangles the two qubits. Cluster state is a huge entangled quantum state in which every qubit is entangled to the other qubits. In cluster state quantum computing, once the cluster state is prepared, expensive two-qubit operations are not needed any more and quantum computation can be completed through only single-qubit operations.

달 만에 이 일을 해냈던 것이다. 현재 이온덫 방법은 여러 면에서 양자컴퓨터 구현에 가장 유리할 것으로 기대되고 있다.

넷째, 양자컴퓨터가 연산을 하는 동안, 연산에 필요한 게이트 이외에는 외부와의 상호작용을 차단할 수 있어야 한다. 큐비트들을 조작하기 위해서는 외부와의 상호작용이 가능해야 하고, 다른 한편으로는 외부의 작용을 차단해야 하는 모순적으로 보이는 상황이다. 디지털컴퓨터에서 잡음(noise)과 이로 인한 오류를 차단해야 하는 것과 같은 조건이지만, 양자컴퓨터에서는 훨씬 더 실현하기 어려운 조건이다. 한 양자계의 양자상태가 외부와의 상호작용으로 결맞음(coherence)을 잃어버리는 것을 결잃음(decoherence)이라고 하고, 양자연산이 제대로 되기 위해서는 이 결잃음을 피하고 결맞음을 유지하기 위해 양자오류수정 알고리즘과 함께 다양한 방안이 모색되고 있다.

다섯째, 양자 계산이 끝나서 최종 상태에 이르렀을 때에 원하는 정보를 측정할 수 있어야 한다. 애써 계산을 다했는데

이터를 출력할 수 없다면 헛수고인 셈이다. 실제로 양자계 중에는 개별 큐비트에서 나오는 신호가 너무 약하다든지 하는 이유로 측정이 불가능한 경우가 많이 있다.

이런 다섯 가지 조건을 두루 만족하는 양자컴퓨터 방식으로 이온덫 방식과 양자광학적 방식, 초전도 방식 등 여러 다양한 방식이 논의되고 있지만, 아직 어떤 방식이 미래의 양자컴퓨터로 등장할지 확실히 알기 어려운 상황이다.

양자컴퓨터의 두 양식, 양자회로 방식과 클러스터상태 방식

필요한 큐비트들을 초기상태로 준비해서 단일큐비트 게이트와 두 큐비트 게이트들을 양자알고리즘에 따라서 작용해 가면서 최종 양자상태를 준비한 후, 양자 측정을 통해 양자 계산을 마무리하는 ‘양자회로(quantum circuit)’ 방식 외에, 클러스터 상태(cluster state)라고 하는 아주 거대한 양자 얽힘 상태를 처음에 준비한 후, 이후로는 두 큐비트 게이트는 쓰지 않고 단일큐비트 게이트만을 사용하여 개별 큐비트들을 하나씩 측정해 나가는 방식으로도 양자계산을 할 수 있음이 증명되었다. 이를 클러스터 상태 양자컴퓨터 또는 일방양자컴퓨터(one-way quantum computer)라고도 하는데, 앞선 측정 결과에 의해 다음 큐비트의 측정 방식이 정해지기 때문이다. 클러스터 상태 양자컴퓨터는 일단 초기 클러스터 상태만 만들어지면 구현하기 힘든 두 큐비트 양자게이트를 쓸 필요 없이 단일큐비트 게이트와 함께 측정만 하면 되기 때문에 쉬운 장점도 있지만, 양자회로 방식보다 훨씬 많은 큐비트들을 준비해야 하기 때문에 어려운 점도 있다.

양자물리학이 하드웨어뿐만 아니라 소프트웨어와 운영체제까지 담당하는 양자컴퓨터

올해의 노벨 물리학상 수상자는 단일 양자계를 조작하거나 측정하는 데에 선구자 역할을 한 와인랜드와 아로시로 결정되었다. 이로써 양자물리학은 20세기에 레이저나 반도체처럼 정보 기술을 담는 하드웨어를 제공하는 데에 머물렀지만, 21세기에는 정보 단위가 비트가 아닌 큐비트를 채용하여 소프트웨어와 운영체제까지 양자물리학이 담당하는 진정한 의미의 양자정보처리 시대가 열리게 되었다.

REFERENCES

- [1] Soonchil Lee, *Quantum computer: 21st century science revolution*, Sallimjisikchongseo 36 (2003).
- [2] George Johnson, *Quantum computer*, translated by Jaewan Kim [original title "Shortcut through time"] (Hanseung, 2007).
- [3] Los Alamos Science, No. 27, 2002. <http://www.fas.org/sgp/othersgov/doe/lanl/pubs/number27.htm>
- [4] Jaewan Kim, *Phys. High Technol.* **13**(1/2), 7 (2004).
- [5] Special Issue 'Quantum optics and quantum information science', *Phys. High Technol.* **19**(10) (2010).