양자컴퓨터 기술 동향 및 산업 응용
Technological Trends and Industrial Applications of the Quantum Computers

이혁성(KIST 기술정책연구소)

차 례

1. 서론
2. 양자컴퓨터 기술 개념 및 현황
3. 양자컴퓨터 산업응용 방향
4. 결론

■ keyword : | 양자컴퓨터 | 양자물리학 | 양자중첩 | 양자얽힘 등

1. 서론

양자컴퓨터는 현존하는 슈퍼컴퓨터를 모두 합친 것보다 월등히 뛰어난 연산능력을 발휘한다는 특징 때문에 전세계적으로 큰 관심을 받고 있다. 미국, 중국, 영국 등 주요 선진국 정부들은 물론 구글, IBM, 마이크로소프트 등 글로벌 대기업 또한 양자컴퓨팅 기술주도권을 갖기 위해 치열한 경쟁을 펼치고 있다.

국가 안보 차원에서 미국 연방 상원은 2018년 12월, 향후 5년간 총 12억 달러를 양자정보과학연구에 투입하는 "국가양자주도법(the National Quantum Initiative Act)을 통과시켰다. 이를 통해 각 대학과 연구소에서 개별적으로 추진하던 연구를 센터 단위로 결집시키며, 연방에너지부(Department of Energy)와 미국 국가표준기술연구소(NIST)가 이를 적극적으로 지원하게 된다.

후발주자인 중국은 미국의 약 8배 이상을 투자하고 있다. 2020년까지 10조원을 투입하여 안후이성 허페이시에 37헥타르에 이르는 대단지를 조성하여 양자정보과학 국가연구소를 설립한다는 계획을 추진 중이다. 실제로 중국은 양자위성 기반의 아시아-유럽 대륙 간 양자암호통신 검증에 성공함으로써 세계 양자기술을 선도 중이다.

민간 차원에서도 양자컴퓨터 기술 개발에 대한 투자가 대대적으로 이루어지고 있다. 구글, IBM, 마이크로소프트, 리게티 컴퓨팅 등 ICT 기업은 직접적으로 양자컴퓨팅 기술 개발에 뛰어들었다. 다른 분야의 기업들 역시 양자컴퓨터 도입을 적극적으로 추진하는 추세이다. 에어버스는 항로결정 등 복잡한 문제를 보다 효과적으로 풀기 위해 그동안 슈퍼컴퓨터에 대대적인 투자를 해오다 최근 양자컴퓨터 도입을 선언하였다. 또한 금융기업인 골드만삭스와 BBVA, 자동차 기업인 폭스바겐과 BMW 등 다양한 분야의 기업들이 양자컴퓨터에 대한 관심과 대응전략을 발표하고 있다.

이와 같이 전 세계적인 관심을 받고 있는 양자컴퓨터는 기존의 디지털컴퓨터와 무엇이 다른가? 본고는 양자컴퓨팅 기술의 개념과 개발 동향을 살펴보고, 향후 어떻게 산업에 적용될 것인지에 대해 고찰한다.

2. 양자컴퓨터 기술 개념 및 현황

2.1 양자컴퓨터 기술 개념

2.1.1 디지털컴퓨터 vs. 양자컴퓨터

현재 우리가 사용하는 디지털컴퓨터는 비트(bit), 즉 2진법(0/1)을 사용하여 트랜지스터에 전류가 흐를 때를 1, 그렇지 않을 때를 0으로 인식해 연산기능을 수행한다. 그리고 컴퓨터의 연산속도를 향상시키기 위해 트랜지스터를 더욱 많이 집적시킴으로써 CPU 자체의 성능을 높임과 동시에 여러 개의 CPU를 병렬로 연결해왔다. 그러나 처리해야 할 데이터는 기하급수적으로 증가하는 반면, 연산속도는 CPU 병렬연결 개수와 비례하여 증가함으로써 점차 디지털컴퓨터의 한계가 나타나기 시작했다. 이와 더불어 트랜지스터 크기가 점점 작아지면서 양자현상이 두드러져 제대로 작동하지 못하게 되어 연산속도 향상 역시 한계에 부딪히고 있다.

따라서 기존 디지털 방식의 슈퍼컴퓨터의 성능향상은 딥러닝 연산에 특화된 방향으로 이루어지고 있고, 다른 컴퓨팅 방식, 즉

양자컴퓨터 개발을 통해 보편적 연산능력의 대폭 향상을 꾀하고 있다. 디지털컴퓨터는 비트 수가 늘어나면 계산공간 역시 선형적으로 비례하여 증가한다. 양자컴퓨터는 큐빗(qubit)이라는 정보 단위를 사용하는데, 큐빗은 0 아니면 1이 아닌 0과 1을 동시에 가질 수 있는 비직관적인 성질(양자중첩)을 지니고 있다. 이러한 특성 때문에 큐빗이 늘어남에 따라 양자컴퓨터의 계산공간은 지수함수적으로 늘어난다.

예를 들어 8비트 디지털컴퓨터와 8큐빗 양자컴퓨터를 이용하여 1과 256 사이에 있는 어떤 함수의 근을 찾는다고 하자. 전자는 함수에 1부터 256까지 넣으면서 결과값이 0인지 아닌지를 확인한다. 따라서 최대 256번의 반복연산을 실시해야 한다. 반면, 양자컴퓨터의 경우, 각 큐빗은 0과 1을 동시에 가질 수 있다는 성질 덕분에 단 한 번의 연산으로 답을 찾아낼 수 있다. 8큐빗은 2^8(=256)개의 숫자를 나타낼 수 있기 때문이다. 현재 우리가 보편적으로 사용하는 32비트, 64비트 컴퓨터를 같은 큐빗 수를 지닌 양자컴퓨터와 비교하면 연산속도는 더욱 더 차이가 나게 된다. 이 때문에 전 세계적으로 양자컴퓨터 개발에 대한 경쟁이 치열해지고 있는 것이다.

그러나 양자컴퓨터가 안정적으로 성능을 발휘하기 위해서는 아직 해결해야 할 문제가 많이 남아있다. 따라서 대부분의 문제를 해결하기 위한 가장 효율적이고 용이한 도구는 여전히 고성능의 디지털컴퓨터이다. 다만, 중장기적으로 양자컴퓨터는 신약 후보물질 발굴, 도시교통 최적화 등 복잡한 문제 해결 영역에서부터 기존의 디지털컴퓨터를 서서히 대체해 나갈 것이다. 앞으로 양자컴퓨터가 어떤 방향으로 발전할 지 살펴보기에 앞서 양자컴퓨터의 근간을 이루는 양자물리학 원리에 대해 짚어보고자 한다.

2.1.2 양자컴퓨터와 양자물리학

양자물리학 또는 양자역학은 미세입자, 즉 전자가 원자 내에서 어떻게 움직이는지를 밝혀내는 학문이다. “양자(量子)”는 “불연속적으로 표현되는 물리량”을 의미한다. 빛을 내는 물체 근처에 ND 필터(neutral density filter)를 놓고 광량을 측정하면 ND 필터의 강도가 높아질수록 이를 통과하는 에너지는 계단형태로, 즉 불연속적으로 감소함을 확인할 수 있다.

이런 불연속적인 특징 때문에 아주 작은 미세입자의 세계(양자계)는 연속적인 물리계와 달리 반직관적인(counterintuitive) 현상이 일어난다. 그것이 바로 양자중첩(superposition), 얽힘(entanglement)이다. 이는 이론적 개념으로만 존재하는 것이 아니라 실재하는 현상이다.

양자중첩이란 큐빗이라는 하나의 입자 속에 0과 1이라는 속성이 동시에 존재하는 것을 말한다. 나노 단위 이하의 영역에서는 베르너 하이젠베르크의 양자 불확정성원리(Uncertainty Principle, 1925)에 의해 0과 1의 구분이 모호해진다. 이 때문에 양자중첩은 우리가 물리적으로 인지하는 실수(real number) 체계가 아닌 허수(imaginary number)가 포함된 복소수 체계(complex number)로 표현된다(에르빈 슈뢰딩거의 파동방정식). 이 때 복소계수는 0이나 1이 측정될 확률의 제곱근을 의미하며, 이는 전자는 확률적으로 존재한다는 것을 의미한다(막스 보른의 확률해석). 확률적 상태는 큐빗이 측정된 순간 0 또는 1로 결정된다. 이러한 양자중첩의 원리에 의해 여러 입력값을 동시에 처리할 수 있는데, 이를 “양자병렬성(Quantum Parallelism)”이라 일컫는다.

양자얽힘은 쌍을 이루는 두 양자는 아무리 멀리 떨어져 있어도 하나의 상태를 공유하는 현상이다. 즉, 한 쪽의 양자가 측정된 순간 우주 저 편에 있는 얽힌 양자(쌍입자)의 상태가 동시에 결정된다는 것이다. 이 때문에 정보전달은 빛보다 빠를 수 없다는 아인슈타인의 특수상대성이론의 국소성에 위배된다는 논란이 일어났다. 양자물리학자들은 양자얽힘을 초광속 정보전달보다는 두 쌍입자 사이의 원초적인 연결고리(비국소성)로 해석한다. 애초에 쌍입자라는 것은 하나의 원자에서 분리되었기 때문에 두 입자는 아무리 멀리 떨어진다 해도 동일한 물리계 안에서 연결되어 있으므로 정보를 전달하는 과정이 필요 없다는 의미이다. 이론적 논란은 여전하나 양자얽힘은 2017년 6월 중국의 양자통신위성 모쯔(墨子)를 이용한 실험에서 실증되었다. 또한 얽힘 현상을 이용하면 10개의 양자로 20개의 상태를 만들어낼 수 있기 때문에 양자컴퓨터의 연산능력을 기하급수적으로 향상시킬 수 있다는 점에서 양자얽힘은 양자컴퓨터 구현의 핵심원리가 된다.

2.2 양자컴퓨터 기술 개발 동향

2.2.1 현황

물리학자 리처드 파인만이 1982년 양자컴퓨터 개념을 제시한 이후 1995년에 이르러서야 미국 NIST에 의해 양자컴퓨터가 처음 만들어졌다. 양자컴퓨터를 구현하기 위해서는 다섯 가지 조건을 만족해야 하는 것으로 알려져 있는데[1], 이 조건을 만족하는 양자컴퓨터 구현 방식으로 NIST가 사용한 이온덫을 비롯하여 반도체, 초전도체, 광자, 다이아몬드 등 다양한 방법이 시도되고 있다.

표 1. 디빈첸쪼(DiVincenzo)의 양자컴퓨터 구현 조건[1]

조 건	설 명
구별 가능한 상태(0/1)를 가진 양자계로의 확장	다수의 큐빗을 쉽게 만들어낼 수 있는가?
기준이 되는 양자상태의 설정	시작 데이터를 안정적으로 확보할 수 있는가?
양자컴퓨팅 과정 동안 외부와의 상호작용 차단	결 어긋남을 줄이기 위한 양자오류 수정이 가능한가?
필요한 수만큼의 양자연산 게이트 구현	2개의 큐빗을 이용하여 얽힘을 구현할 수 있는가?
연산 후 최종상태에서의 원하는 정보 측정	충분한 세기와 신뢰성을 갖춘 데이터를 획득할 수 있는가?

상용 양자컴퓨터 개발 경쟁은 2011년 캐나다의 디웨이브(D-Wave)社가 128큐빗 양자컴퓨터를 선보이면서 치열해지기 시작했다. 디웨이브는 2013년 516큐빗, 2015년 1,000큐빗짜리 양자컴퓨터를 연달아 선보였으나 오류가 많이 발생하여 상용화 수준에 미치지 못한다는 비판도 받고 있다. 구글은 2016년 초전도체 방식을 이용한 9큐빗 프로세서를 선보였으며, 2018년 72큐빗 프로세서를 개발했다고 발표했다[2].

한편 국내에서는 KIST, IBS, 표준과학연구원 등 정부출연연구기관을 중심으로 양자컴퓨터 연구가 이루어지고 있다. KIST는 2018년까지 광자, 고체점결함 스핀 큐빗 생성과 제어에 대한 연구를 진행해왔으며, 2019년부터는 양자 노드, 양자 인터페이스, 양자얽힘 치환기술 등 하이브리드 큐빗을 연구한다. IBS는 양자오류가 일어날 가능성은 가장 적지만 아직까지 개념이 검증된 적이 없는 '유사입자' 연구를 수행하고 있다.

양자컴퓨터 기술 개발에는 크게 세 가지 마일스톤이 있다. 첫째, 양자우월성(Quantum Supremacy)이다. 양자컴퓨터의 성능이 기존의 디지털컴퓨터 성능보다 월등하다는 것을 보여줄 수 있어야 한다. 전문가들은 대략 50큐빗 시스템에서 양자우월성이 달성될 것으로 예측하고 있다. 이 때문에 구글, IBM 등 글로벌 대기업들은 50큐빗을 목표로 치열한 경쟁을 벌이고 있다.
둘째, 양자오류 정정이다. 큐빗이 늘어날수록 양자오류가 발생할 가능성 또한 높아진다. 따라서 오류를 수정할 수 있는 결함허용(fault-tolerant) 양자컴퓨팅을 추구하면서 논리큐빗 구현과 양자오류 정정을 실증할 수 있어야 한다. 이를 위해서는 고성능 큐빗 제어기술이 필요하다.

셋째, 소규모 양자컴퓨팅 네트워크를 구축해야 한다. 양자컴퓨팅은 양자정보통신과 밀접한 관련을 가질 수밖에 없다. 미래의 인터넷은 양자인터넷으로서 분산형 컴퓨팅 구현에 적합할 것으로 예상된다. 이에 대한 컨소시움으로는 Quantum Internet and Networked Computing (QuTech), Networked Quantum Information Technologies Hub가 있다. 특히, 후자는 20큐빗으로 이루어진 양자노드 20개를 연결한 통신망 구축을 추진하고 있다.

2.2.2 향후 기술개발 목표

양자컴퓨터 기술 개발 마일스톤을 모두 달성하기 위해서는 해결할 문제가 많다. 무엇보다 양자중첩과 얽힘이라는 특성을 안정적으로 활용할 수 있어야 한다. 즉, 0이면서 1인 양자상태가 연산과정에서 변하지 않아야 한다. 관측되는 순간 상태가 결정되면서 동시에 양자오류가 발생되는 등 외부환경에 취약한 양자를 원 상태대로 온전히 유지시키고 이를 확인할 수 있는 기술이 필수적이다. 즉, 양자컴퓨터 성능 향상에 있어 큐빗 개수를 늘리는 것뿐만 아니라 양자오류를 줄이는 것 또한 핵심적이다.

2018년 1월 미국 칼텍(Caltech)의 존 프레스킬(John Preskill) 교수는 현재 개발된 양자컴퓨터의 성과를 높이 평가하고 앞으로 지속적으로 활용성을 확보해나가기를 바라는 의도로 양자오류는 정정되지 않은 상태인 50~100큐빗의 중간규모 양자컴퓨터(Noisy Intermediate- Scale Quantum Computer)의 등장시기를 NISQ 시대라고 명명했다[3]. 그리고 NISQ에 의한 연산속도향상을 위해서는 최적화, 양자딥러닝, 양자어닐링, 잡음탄력양자회로 등 다양한 기술 개발이 필요하다고 말했다.
전문가들은 양자컴퓨터 개발에 있어 이론적인 장애물은 없다고 여긴다. 다만 개별 미세입자의 양자상태를 조작할 수 있는 기술이 필요할 뿐이다. 나노기술의 발전이 이러한 기술적 한계를 극복하는 핵심요소가 될 것이다.

양자컴퓨터는 그 뿌리가 되는 양자물리학을 획기적으로 진전시키는 기폭제가 될 것이다. 분자, 원자, 전자 단위에서의 물리적 메카니즘 분석이 가능해지면서 여전히 베일에 싸여있던 자연현상을 이해할 수 있게 될 것이다. IBM 퀀텀은 2019년 6월 11일 '매경-IBM Think Summit Korea'에서 IBM Q를 공개하면서 양자컴퓨터를 통해 커피에 녹아있는 카페인의 원자 구성요소를 파악할 수 있으며 이는 현존 컴퓨터로는 불가능하다고 말했다. 카페인 분자 하나가 가진 에너지를 계산하는 데에 160큐빗의 양자컴퓨터가 필요하다고 할 정도이다[4]. 실제로 NISQ 시대를 넘어 결함허용의 시대로 접어들면서 대규모 양자컴퓨터가 등장하게 되면 의료, 화학, 금융, 제조 등 전 산업에서 큰 변혁이 일어날 것으로 예상된다.

3. 양자컴퓨터 산업응용 방향

양자컴퓨터는 기존의 슈퍼컴퓨터가 담당하던 많은 부분을 대체할 수 있다. 예를 들어 기상예측, 암호해독, 자율주행, 신약후보물질 발굴, 도시교통 최적화, 우주탐사 등 아주 복잡한 계산이

필요한 부분에서 말이다.

2017년 12월 초 실리콘밸리에서 개최된 Q2B 컨퍼런스에서 폭스바겐(자동차), 골드만삭스(금융), 에어버스(항공)가 자신들의 사업에 양자컴퓨터를 어떻게 활용하고자 하는지 소개하였다[5,6].

폭스바겐은 디웨이브 2000Q를 비롯한 2종의 양자컴퓨터를 활용하여 연산능력을 직접 검증하면서 도시교통·이동경로 최적화 서비스를 준비하고 있다. 기존 슈퍼컴퓨터로도 수행 가능한 작업이지만 양자컴퓨팅을 통해 보다 향상된 최적화를 실현시키는 것이 이들의 목표이다. 또한 전기차 시대를 대비하여 화학 시뮬레이션을 통한 전기차용 고성능 배터리 개발에도 양자컴퓨터를 적용 중이다.

골드만삭스는 금융 리스크 계산과 같이 아주 많은 경우의 수를 계산해내기 위해 양자컴퓨팅을 통한 몬테카를로 시뮬레이션의 고속화를 추진 중이다. 그리고 중장기적으로 기존 공개키 암호 방식이 양자컴퓨터에 의해 깨질 수 있음을 우려하여 정보보호 차원에서의 양자컴퓨터 개발에도 관심을 갖고 있다.

에어버스는 항공기 설계나 고장 원인 분석에 양자컴퓨터 도입을 검증하고 있다. 항공기 설계를 위해 엄청난 양의 시뮬레이션을 슈퍼컴퓨터에서 실행하고 있는데, IT 예산의 3%가 이와 관련한 하드웨어에 투자되고 있어 양자컴퓨터를 통한 예산절감 효과를 기대하고 있다.

이 밖에도 신생 벤처기업 리게티 컴퓨팅은 기존 디지털컴퓨터와 양자컴퓨터를 연결한 후 양자 클라우드 서비스를 공개했다. 이는 현재의 클라우드 서비스보다 최소 20배 더 빠른 양자 알고리즘을 실행할 수 있다.

또한 양자컴퓨터는 기계학습(machine learning)의 성능을 대폭 향상시켜 인공지능이 만들어내는 지식 총량이 인류의 지식 총량을 초과하는 특이점(singularity)을 앞당길 것으로 전망된다. 2018년 11월 이탈리아 파비아 대학 연구팀은 양자컴퓨터에 퍼셉트론을 구현하여 복잡한 이미지와 패턴을 분류해내는 데에 성공했다. 또한 IBM과 MIT는 2019년 3월, 양자컴퓨터를 통해 머신러닝을 가속화할 수 있는 기능매칭 기능을 개발해 발표했다.

4. 결론

양자컴퓨터가 현실에서 실제 의미 있는 문제를 해결하기 위해서는 시간이 더 필요하다. 큐빗의 개수를 늘림과 동시에 큐빗 제어, 양자오류 정정 등 안정성을 확보해야 하기 때문이다. 전 세계 선진국들은 공공·민간부문을 가리지 않고 이러한 기술 난제를 해결하기 위한 경쟁에 뛰어들고 있다. 기업들의 응용사례와 향후 전략에서도 볼 수 있듯이 양자컴퓨터는 산업분야를 가리지 않고 혁신적인 기술과 시스템을 만들어내는 데에 적용될 것이다. 급속도로 발전 중인 양자컴퓨터는 막대한 재원과 인력이 투입되어야 하는 만큼 우리나라도 중장기적 관점에서 국가적 역량을 결집하기 위한 정책이 추진되어야 한다.

참고문헌

[1] DiVincenzo, D.P. (2000), "The Physical Implementation of Quantum Computation," Fortschritte der Physik: Progress of Physics, 48(9-11), 771-783.

[2] http://biz.chosun.com/site/data/html_dir/2018/03/21/2018032103790.html

[3] Preskill, J. “Quantum Computing in the NISQ Era and Beyond,” Quantum, 2, 79.

[4] https://www.mk.co.kr/news/economy/view/2019/06/406757/

[5] 정보통신기술진흥센터 (2017), “폴크스바겐, 골드만삭스, 에어버스의 양자컴퓨터 활용 계획,” 주간기술동향, 1828호.

[6] 정보통신기술진흥센터 (2019), “양자컴퓨팅 선도기업들, 양자컴퓨터 소프트웨어 개발자 확보 경쟁 시작,” 주간기술동향, 1882호.

저자소개

● 이 혁 성(Hyeokseong Lee)

·2008년 2월 : KAIST 산업공학과 (공학사)
·2010년 2월 : KAIST 산업및시스템공학과 (공학석사)
·2012년 2월 : KAIST 기술경영전문대학원 (공학석사)
·2017년 2월 : KAIST 기술경영전문대학원 (공학박사)
·2017년~현재 : 한국과학기술연구원(KIST) 기술정책연구소 선임연구원
〈관심분야〉 기술경영, 기술정책, 산업융합, 신산업분석