제104회 KISTEP 수요포럼

주 제 : 양자(量子)기술이 그리는 미래
- 양자컴퓨팅의 현황과 이슈

담당자 : 신동평 부연구위원(T. 02-589-2328)

포럼 종합 요약

2019. 5. 8

KISTEP 한국과학기술기획평가원
Korea Institute of S&T Evaluation and Planning

1. 발표 주요 내용

□ 개요

o 양자정보 기술이 미래기술로 각광받고 있으며, 특히 양자컴퓨팅 기술이 그 핵심으로 지난 20여 년간 급격히 성장. 양자컴퓨터는 양자역학적 원리를 이용하여 계산을 수행하는 완전히 새로운 개념의 컴퓨터 기술.

o 20세기 초반 태동한 양자역학이 자연 현상을 설명하기 위한 과학이었다면, 21세기의 양자기술은 양자상태를 직접 제어하고 활용하여 기존에 없는 유용한 성능을 얻는 적극적 기술임.

□ 양자컴퓨팅 기술개요: 양자컴퓨터란 무엇인가?

o 고전적 디지털 기술에서 0과 1의 두가지 상태로 정보를 처리하는 비트(bit)와 달리 양자컴퓨터는 0과 1 두가지 상태의 양자역학적 '중첩'을 이용하는 큐비트(qubit)을 이용하여 정보를 기록하고 처리함.

o 멀리 떨어진 두 개의 큐비트 사이에 강한 연결이 존재하는 양자 '얽힘'(quantum entanglement)을 이용함.

□ 양자컴퓨터에 대한 사실과 오해

o 양자컴퓨터는 기존 컴퓨터 기술과 완전히 다른 새로운 개념으로 독자적 분야를 창출하고 기술적 패러다임을 근본부터 바꾸는 파괴적 혁신기술.

o 양자컴퓨터는 속도가 빠르거나 용량이 큰 전지전능한 계산 기계가 아니고, 양자역학적으로 동작하면서 현재의 컴퓨터와 상호 보완적으로 특화된 알고리듬을 문제를 푸는 보조적인 슈퍼 머신으로 이해해야 함.

o 큐비트의 개수가 많다고 해서 양자컴퓨터의 성능이 높은 것은 아니며, 정확성 및 연결성 등 다양한 요소를 고려한 성능지수를 평가해야 함. error rate가 적고 큐비트 개수가 많으면 많은 기능을 할 수 있음.

o 실용적이고 강력한 성능의 양자컴퓨터의 본격적 등장은 약 10년 이상이 걸릴 것으로 예상함.

□ 해외 연구개발 현황 (정부)

o 미국은 이미 2000년대 초중반부터 CIA 산하 연구기관인 IARPA주도로 대규모 정부개발사업을 진행하여 압도적인 기술 우위를 확보하였음.

o 미국은 2018년말 국가적 전략으로 13억달러 규모의 양자이니셔티브(Nationial Quantum Initiative)를 시작하였는데, 이는 나노기술이 태동하던 나노이니셔티브가 나노기술 붐을 가져온 일을 유추하면 됨.

o 유럽은 다년간의 논의를 거쳐 2018년 하반기 EU Quantum Flagship 프로그램을 시작하였으며, 이는 10년간 10억유로를 투자하는 규모임.

o 영국은 UK National Quantum Technology Programme을 2013년부터 수행하여 5년간 2억7천만 파운드를 투자하였고, 2단계 5년 프로그램을 비슷한 규모로 시작하는 단계임.

o 중국, 일본, 캐나다, 호주 등에서 정부 주도로 대규모 양자컴퓨터 개발 사업이 진행 중임.

□ 해외 연구개발 현황 (민간)

o IBM은 2016년 5월 처음으로 양자컴퓨터 클라우드 서비스를 공개, 무료 제공하기 시작한 후, 2017년말부터 삼성 등을 대상으로 소규모 유료 서비스 시작. IBMQ 클라우드에는 수십만명이 접속하여 연구목적으로 활용 중.

o Google은 2014년 9월에 당시 가장 앞선 기술력을 가지고 있던 산타바바라 대학 연구팀을 통째로 인수하면서 본격적인 하드웨어 개발에 뛰어들었고, 현재 기술적으로는 가장 앞서있다고 평가받고 있음.

o 캐나다의 D-wave사는 양자어닐러라는 독특한 방식의 제한적 용도의 양자컴퓨터를 상용화하여 판매하고 있음.

o 실리콘밸리를 중심으로 Rigetti, IonQ, PsiQ 등의 양자컴퓨팅 스타트업들이 대규모 투자를 유치하면서 다수 등장하고 있음.

o 알리바바, 텐센트 등 중국 IT기업들도 양자컴퓨터 개발에 뛰어들었으며, 에어버스 등 대규모 계산량이 많은 기업들에서도 적극적 관심

□ 현재의 기술수준: NISQ

o 현재는 오류가 보정되지 않고 유한한 성능을 가지는 소규모 양자컴퓨터가 활용되는 시기로, NISQ(Noisy Intermediate-Scale Quantum) 시대로 지칭.

o 양자컴퓨터의 성능을 향상시키는 연구와 병행하여, 현재 성능 수준의 양자컴퓨터에서 유용한 활용 분야를 찾는 연구가 활발히 진행되는 중

o 변수가 많은 문제의 최적화, 신물질 개발 등의 양자화학 문제, 양자기계학습 등에 응용 등이 유망한 분야로 고려되고 있음.

□ 현재의 이슈 및 대응

o 현재 양자컴퓨터 기술, 나아가 양자 기술 전반은 관련 인력의 부족이 기술발전의 가장 큰 병목이라고 판단되고 있음.

o 유럽 프로그램의 경우 “eco-system” 형성을, 미국 NQI의 경우 “quantum-smart workforce” 양성을 주요 목표로 삼고 있음.

o 단기간에 큰 시장이 형성되지 않는 반면, 기술의 난이도가 매우 높고 진입장벽이 존재하는 극한정밀기술의 융합분야이므로, 기술개발의 모멘텀을 장기간 유지하는 것이 각국 정부의 관심사임.

o 기업체의 경우는 현재의 기술수준을 발전시키는 혁신적 아이디어와 함께 단기적으로 실용적 활용방안을 제공하는 가치창출에 집중하고 있음.

□ 전략적 접근: 우리의 전략은?

o 현재 국내 연구역량은 선진국에 비해 7년~10년 정도 뒤처져 있다고 평가.

o 따라서 향후 3~5년은 fast-follower전략이 불가피하며, 정부의 전략적 프로그램을 통해 단시간 내에 격차를 5년 내로 좁히고, catching range 안으로 들어가는 것이 중요함.

o 양자컴퓨터 및 양자정보기술은 순수과학부터 실용적 공학까지 매우 넓은 분야의 종합적 연구가 필수적인 분야이지만, 기술적으로는 기초연구 단계이고, 장기연구 주제임을 인지해야 함.

2. 패널토론 주요 내용

< 서울대 - 김도헌 교수 >

□ 양자컴퓨팅 개념에 대한 대중의 오해 불식 필요

o 양자컴퓨팅는 양자역학적으로 정보를 처리하는 기술로, '양자'라는 것이 미시세계에 있는 것에 정보를 쓰는 것이 아님

□ 양자컴퓨팅에 대한 관심도의 증가

o 국내 학생들 사이에도 양자 컴퓨팅에 대한 관심과 중요성을 인식하는 변화가 있고 고무적

□ 다양한 양자컴퓨팅 플랫폼에 대한 접근

o 양자컴퓨팅을 위한 플랫폼은 다양하며, 큐비트를 증가시키기 위한 연구는 물론 오류 감소를 위한 심도 있는 연구가 필요함.

o 플랫폼이 다양하더라도 기술적 필요사항 및 language 등은 공통적으로 적용되기 때문에 하나의 플랫폼에서 트레이닝이 잘 된 인력들은 다른 플랫폼 간에 왕래도 허용이 가능

< 서울대 - 김태현 교수 >

□ 양자컴퓨팅에 대한 오해

o 양자컴퓨터가 기존 컴퓨터를 완전히 대체할 것이라는 등 잘못된 인식이 존재하며, 건전한 연구 생태계 조성에 악영향으로 작용.

o 실용적인 양자컴퓨터의 시기에 대한 현실 이상의 과장된 기대가 많은데, 현실에 기반의 제대로 된 예측이 일반인에게 공유되어야 함.

o 시장은 5년 이상 기다려주지 않지만, 연속적인 연구가 진행되려면 잘못된 오해들이 해소되어야 함.

□ 학제 간 다양성의 확보

o 양자정보 분야에 대한 과장되지 않은 이해가 공유된 범위 내에서는 이를 발전시키기 위한 다양한 분야의 협력이 필요함

o 양자 역학에 대한 사전 교육이 없는 인력들도 약 1~2년 정도의 집중 교육을 통해 기본 지식을 습득할 수 있는 교육 프로그램이 필요

< KIST - 문성욱 책임연구원 >

□ 양자암호통신에서의 문제

o 양자 암호가 안전한 이유는, 양자가 가지는 고유 특성 때문임. 양자는 복제가 불가함.

o 양자암호통신의 Key 생성, 분배, 관리 중, key 생성과 분배의 수준은 월등하나, 관리는 사람이 직접 관여하는 문제

o 통신에 있어 멀리 못가는 단점이 있으며, 퀀텀 리피터(Quantum repeater)가 필요. 리피터는 증폭기의 역할을 하며 양자암호의 특징과 모순되나 그 문제를 근본적으로 해결한 것이 중국 양자 인공위성. 국내의 양자암호통신은 저궤도 위성 기반의 시스템이 적절

□ 양자 컴퓨팅 기술을 통한 RSA의 무력화?

o 양자컴퓨터가 나오면 기존의 RSA가 붕괴가 될 수 있음. 양자 암호는 RSA 양자 암호를 깨는 동시에 막는데 쓰임. 양자의 연구가 되고 있으나, 양극단의 일에 놓일 것으로 생각함.

□ 양자 컴퓨터의 구현

o 양자컴퓨터의 구현에는 많은 큐비트가 필요. 특성이 같은 큐비트를 동일하게 만드는 것의 어려움 존재. 극한기술이고 한계 극복기술이므로 지속적인 연구를 위한 투자가 필요.

o 공용 양자 컴퓨터가 국내에서 만들어질 가능성은 매우 낮으나, 현재 기술수준에 비해 낙관적으로 바라보고 있음. 양자 과학기술 문화는 만드는데 성공했으나, 양자 컴퓨터 기술 수준은 매우 낮음

< IBM - 신창호 본부장 >

□ 양자컴퓨팅이 바꿔놓을 미래 비즈니스의 변화

o 양자컴퓨팅은 산업 전체에 혁명을 일으킬 잠재력이 존재하며, 이후 기업 비즈니스에 있어서 fast follow 전략은 크게 변화될 것.

□ 양자컴퓨팅 기술에 대한 전략

o 수용 전략에 있어 양자컴퓨터를 직접 개발할 것인가, 컴퓨팅을 할 것인가, 관련 교육을 할 것인가를 결정해야 함.

□ 기술의 수용성 및 생태계 조성 문제

o 해외에서는 기술의 상용화보다는 파생되는 IP 전략 수립, 양자컴퓨팅 생태계에 대한 논의가 진행 중인데, 국내 기업은 수용성이 낮음.

o 국내 기업은 문제를 발견하고 정의하는 resource의 부족함. 양자컴퓨팅 서비스를 클라우드로 제공하고 있더라도 어떤 문제를 어떻게 해결할지에 대한 정의가 없음.

□ 양자컴퓨팅 기술 활용 및 사회적 저변의 확대

o 미국 스타트업 중에는 양자 시뮬레이션을 통해 재료, 화학 분야의 새로운 사업을 준비 중인 사례 존재

o 양자컴퓨팅 하드웨어 외에 양자 컴퓨팅 허브 구축을 통해 기업 및 연구기관들이 참여하는 활발한 연구 생태계 조성 필요