

양자 컴퓨팅: 무엇에 유용한가

(2023.06.05., 양자정보연구지원센터)

□ 양자 컴퓨팅 활용 연구의 유용성 탐색

- 대부분의 연구자는 양자 컴퓨터를 본 적이 없고 유용한 일을 할 수 없다고 생각, 수십 년간 연구는 컴퓨팅에서 혁명을 촉발할 기계를 생산하지 못함, 그러나 개발이 예상보다 잘 진행되고 있다고 함
 - 2월 대규모 모듈식 양자 컴퓨터에 대한 원리 증명 발표(Sussex 대학)
 - 양자 컴퓨터가 양자 물리학 및 화학 시뮬레이션, 온라인 금융 거래 같은 민감한 통신 보호에 사용되는 공개키 암호 시스템을 깨는데 기존 컴퓨터보다 큰 이점 제공하리라는 수학적 증거 얻음
 - 모든 사용 사례는 고전 컴퓨터로 할 수 없는 유용한 어떤 것도 아직 달성하지 못함(Scott Aaronson)
 - 하드웨어 구축의 어려움으로 복잡해짐, 양자 컴퓨터는 초전도 링, 광학 트랩의 큐비트로 데이터 저장, 큐비트가 중첩 상태로 유도될 때, 양자 컴퓨터에서 알고리즘을 실행
 - 유용한 계산은 엄청난 수의 큐비트가 있는 양자 기계에서만 가능하며 아직 존재하지 않음, 큐비트와 상호작용은 열 진동, 우주 광선, 전자기 간섭 및 기타 잡음으로 발생하는 오류에 견고해야 함
- **정당한 회의론**
 - 큐비트 측면에서 세계 가장 큰 양자 컴퓨터는 433개 IBM Osprey, 200만 큐비트라도 일부 양자 화학 계산에는 100년이 걸리고 (2022), 8시간 내 최첨단 암호화 해독에 2천만 큐비트 필요(2021)
 - 2천만 큐비트는 도달 불가능하게 보이지만 이전 추정치인 10억 큐비트보다 훨씬 적으며, 양자 화학 계산이 직면한 문제 중 일부는 하드웨어 혁신으로 극복 가능함(낙관적)
 - 예를 들어, 약 50개 궤도 전자의 바닥 상태 에너지 계산하는 양

자 알고리즘이 근본적으로 더 효율적일 수 있음을 증명, 알고리즘 작업이 다양한 양자 논리 게이트 주변에 분산되는 방식을 변경하면 이론적 실행 시간이 몇일로 단축됨(5배 향상)

○ 양자 도약, 양자 이점 활용 시작

- 반도체 제조를 위한 리소그래피 기술 개선, 약물 설계 혁신이 가능한 작은 광활성 분자의 바닥 및 여기 상태의 에너지 찾기, 단일 산소 분자의 단일항 및 삼중항 상태 시뮬레이션으로 배터리 연구자의 관심을 끌고 있음
- IBM 성과 중 일부는 양자 컴퓨터의 오류 감소 조치 결과, 양자 정보 손실 없이 고전 컴퓨터에서 분리 및 시뮬레이션할 수 있는 양자 회로의 일부 식별

○ 긴 게임

- 향후 5년 내 유용한 무언가를 제공할 수 있다면, **화학 계산**일 것임, 상대적으로 적은 수 큐비트의 양자 컴퓨터 사용 가능
- 위험 관리, 재료 과학 및 물류 최적화 같은 **금융 응용 프로그램**도 단기적으로 양자 컴퓨팅 이점 얻을 가능성이 높음
- 양자 머신 러닝은 고전적 알고리즘을 능가할 수 없지만 탐구할 여지는 있음

○ 양자 머신 러닝을 향하여

- 머신 러닝 알고리즘은 데이터에 숨겨진 구조와 패턴을 찾는 다음 알고리즘이 다른 데이터 세트에서 동일한 패턴을 인식하도록 수학적 모델을 생성, 이미지 인식과 같은 작업 수행
- 그러나 머신러닝의 양자 버전을 사용하면 더 적은 매개변수와 훨씬 적은 훈련 데이터가 필요할 수 있음

(원문)

1. https://www.nature.com/articles/d41586-023-01692-9?utm_source=Nature+Briefing&utm_campaign=d128e37f03-briefing-dy-20230525&utm_medium=email&utm_term=0_c9dfd39373-d128e37f03-47888812