

# 양자 이점이란 무엇인가

(2023.12.12., 양자정보연구지원센터)

## □ 양자 이점과 그 중요성

- 양자 이점은 양자 컴퓨팅에서 중요한 이정표로, 고전 컴퓨터의 능력을 넘어설 수 있는 문제들에 대한 해결책을 제공함
  - 양자 컴퓨터는 양자 역학의 독특한 행동을 활용하여 비현실적인 고전적인 문제들을 다룸
- 양자 컴퓨팅 힘의 원천
  - 양자 컴퓨팅은 0과 1의 중복 상태에 존재할 수 있는 양자 비트인 ‘큐비트’에 의존함
  - 양자 컴퓨팅 파워는 중복 상태, 간섭 및 얽힘의 상호작용에서 나옴
  - 간섭은 올바른 솔루션을 증폭(보강 간섭)하고 잘못된 답을 억제(상쇄 간섭)하며, 얽힘은 고전 컴퓨터의 범위를 넘어선 계산 속도 향상을 가능하게 함
- 양자 컴퓨팅의 응용 분야
  - 양자 컴퓨팅은 암호학, 시뮬레이션 및 감지에서의 잠재적인 응용 분야가 있음
  - 암호학에서 양자 컴퓨터는 현재 암호화 알고리즘을 해독할 수 있어 포스트-양자 암호학(post-quantum cryptography)의 필요성이 생김
  - 양자 시뮬레이션은 화학 및 재료 과학에서 예측을 가속화함
  - 양자 감지는 다양한 분야에서 물리적 특성을 감지하고 측정하는데 있어 비양자 기기보다 더 높은 감도와 정밀도를 제공함
- 양자 인터넷과 양자-고전 컴퓨팅 연결
  - 양자 인터넷과 같은 프로젝트는 양자 컴퓨터를 안전한 통신으로 연결하려는 목표를 가지고 있음

- 양자 키 분배(QKD)와 같은 양자 암호 프로토콜을 사용하여 통신 채널을 양자 컴퓨터를 활용한 계산적 공격으로부터 보호함
- 양자 컴퓨팅의 도전 과제, 결맞음 유지 및 오류 수정
  - 양자 컴퓨터는 환경과의 의도하지 않은 상호작용에 매우 민감함
  - 큰 규모의 양자 시스템을 구축하려면 결잃음(decoherence)을 극복하는 것이 필요하며, 효과적인 오류 억제 및 수정 방법을 개발해야 함
- 양자 컴퓨팅의 산업 및 연구 풍경
  - 스타트업과 Google, IBM과 같은 기존의 기술 산업 참가자들은 양자 하드웨어 및 소프트웨어 개발에 투자하고 있음
  - 학계와 산업 간의 협력은 세계 각국 정부로부터의 큰 투자와 함께 분야의 진전을 가속화시킴
- 양자 컴퓨팅 개발, 성과와 위험
  - 양자 컴퓨팅은 특정 분야에서 양자 이점을 보여주는 초기 신호를 보여주었지만, ‘양자의 겨울’이라는 위험도 존재함
  - 기술 사업은 즉각적인 응용 분야에서 양자 이점을 실현하기 위해 노력하고 있지만, 가까운 미래에 실용적인 결과가 나타나지 않으면 투자 감소의 위험이 있음
- 양자 컴퓨팅의 잠재력 및 계속되는 진전
  - 양자 컴퓨팅은 생성적 AI의 등장과 마찬가지로 혼란을 일으킬 수 있음
  - 현재 양자 컴퓨팅 기술 개발은 중요한 분기점에 있음
  - 양자 기술의 기본 원리를 조사하는 학문적 연구는 매일 마주치는 새롭고 밝은 학생들의 열정에 의해 지속적으로 진전됨

(원문)

1. <https://theconversation.com/what-is-quantum-advantage-a-quantum-computing-scientist-explains-an-approaching-milestone-marking-the-arrival-of-extremely-powerful-computers-213306>