

오류 없는 양자 컴퓨팅의 가능성

(2024.07.08., 양자정보연구지원센터)

- 양자 회로 검증을 위한 심볼릭(Symbolic) 모델 체크 방식, 오류 없는 양자 컴퓨팅의 가능성
 - 양자 회로, 양자 알고리즘 설계 및 구현에 사용됨
 - 양자 컴퓨팅은 양자 물리학 법칙을 이용해 고전 컴퓨팅으로 매우 어려운 복잡한 계산 문제를 해결하는 급성장하는 기술임
 - 전 세계 연구자들은 많은 양자 알고리즘을 개발하여 고전 알고리즘에 비해 상당한 개선을 보여줌
 - 양자 회로는 이러한 알고리즘 개발에 중요한 모델로, 실제 양자 하드웨어에 배포하기 전에 양자 알고리즘을 설계 및 구현하는데 사용됨
 - 양자 회로는 양자 게이트, 측정, 큐비트 초기화 등 일련의 작업으로 구성됨
 - 상징적 모델 검사 접근 방식 제안(일본 JAIST)
 - Maude 프로그래밍 언어를 사용하여 양자 회로의 모델 검사를 위한 상징적 접근 방식 개발
 - Maude는 복잡한 시스템의 형식 사양 및 검증을 지원하는 고수준 사양/프로그래밍 언어로, 선형 시간 논리(LTL) 모델 검사기를 갖추고 있음
 - 연구자들은 Maude에서 양자 회로를 양자 게이트와 측정 응용의 일련으로 공식적으로 지정함
 - 이 접근 방식을 사용해 여러 초기 양자 통신 프로토콜을 검증함
 - 초밀집 코딩(Superdense coding), 양자 텔레포테이션(Quantum Teleportation), 양자 비밀 공유(Quantum Secret Sharing) 등 검증
 - Quantum gate teleportation의 원래 버전이 원하는 속성을 만족하지 않는 것을 발견하고 수정된 버전을 제안해 정확성을 확인함

- 이러한 발견은 양자 회로 검증을 위한 혁신적인 접근 방식의 중요성을 의미함
- 이 방법의 몇 가지 한계를 지적하며 추가 연구가 필요하다고 언급함
 - 미래 더 많은 양자 게이트와 복잡한 수 연산을 처리하기 위해 상징적 추론을 확장하고, 양자 프로그램 및 양자 암호 프로토콜의 모델 검사에 적용하고자 함(Dr. Do)
 - 양자 회로의 검증 및 사양을 위한 일반적인 프레임워크를 향한 첫걸음을 의미하며, 오류 없는 양자 컴퓨팅을 위한 길을 열어줌
- Maude에서 양자 회로를 검사하는 상징적 모델(*PeerJ Computer Science*)
 - 디랙 표기법과 기본 행렬 연산을 사용한 양자 역학의 법칙을 통해 양자 회로를 모델 검증하는 심볼릭 접근법을 제시함
 - 심볼릭 접근법은 재작성 논리에 기반한 고급 명세/프로그래밍 언어인 Maude를 사용하여 구현됨
 - 사례 연구로는 초밀집 부호화, 양자 텔레포테이션, 양자 비밀 공유, 얽힘 스와핑, 양자 게이트 텔레포테이션, 두 거울상 텔레포테이션, 양자 네트워크 코딩 등 여러 양자 통신 프로토콜을 형식적으로 명세하고 검증함
 - 이 접근법은 Maude에서 양자 회로를 형식적으로 명세하고 검증할 수 있는 일반적인 프레임워크의 첫 단계가 될 수 있음을 시사
 - 제안된 양자 회로 형식 명세 방법을 통해 Maude에서 양자 회로를 일련의 양자 게이트/측정 응용으로 설명할 수 있음
 - 초기 상태와 선형 시간 논리(LTL, linear temporal logic)로 표현된 원하는 속성과 함께 양자 회로가 제안된 방식으로 명세되면, 제안된 모델 검증 기술은 내장된 Maude LTL 모델 체커를 사용하여 초기 상태에서 시작, 양자 회로가 속성을 충족하는지 자동으로 형식 검증을 수행

(원문)

1. <https://thequantuminsider.com/2024/07/01/symbolic-model-checking-approach-to-verify-quantum-circuits-could-lead-to-error-free-quantum-computing/>