양자 정보 처리: 비트에서 큐비트로

(2023.08.09., 양자정보연구지원센터)

□ 양자 역학, 양자 게이트 및 양자 알고리즘이 새로운 컴퓨팅 시대를 여는 방법, 양자 정보 처리(QIP)

○ QIP(Quantum Information Processing)

- 양자 역학의 원리와 응용 사용하여 정보를 조작하고 처리함, 큐비트는 여러 확률적 상태에 존재할 수 있으므로 병렬 계산 가능
- 큐비트 상태가 상호 연결되는 얽힘 및 중첩 현상 활용, 양자 컴퓨터는 특정 계산을 고전 컴퓨터보다 기하급수적으로 빠르게 수행할 수 있음, 암호 해독, 최적화 및 시뮬레이션에서 획기적 발전
- Shor 소인수 분해 알고리즘 및 Grover 검색 알고리즘에서 QIP 능력 확인, 그럼에도 실용적이고 오류 수정된 양자 컴퓨터 구축은 섬세한 양자 상태 정밀 제어와 노이즈 및 결잃음(decoherence) 감소 같은 주요 과제가 남아 있음

○ 양자 정보 처리 vs. 고전 정보 처리

- classical information processing: 고전 정보 처리에서 정보는 고전 비트를 사용하여 처리 및 저장됨(비트 또는 이진수, 0 또는 1), 논리 게이트 사용하여 미리 정의된 규칙에 따라 비트 조작 계산 수행, 알고리즘과 프로그램은 고전 비트 입력을 순차적으로 처리
- quantum information processing: 데이터 조작 위해 양자 역학 원리 이용, 큐비트는 여러 확률적 상태로 존재(중첩), 병렬 계산 수행 가능하며 고전 컴퓨터보다 더 효율적인 방식으로 특정 문제 해결이 가능함

○ QIP에서 큐비트와 그 역할

- 양자 정보 처리에서 큐비트는 양자 정보 저장 및 조작, 원자, 이온, 광자 및 초전도 회로 포함한 다양한 물리적 시스템 사용하여 구현(두 개 이상 고유한 양자 상태가 있는 물리적 시스템 사용)

- 회전 및 얽힘 같은 양자 게이트 연산 통해 큐비트 상태 조작, 양자 알고리즘과 양자 계산은 고전적 논리 게이트의 양자 아날로그 작업에 의존함
- 얽힘은 큐비트의 중요 특성임, 물리적으로 분리된 경우에도 여러 큐비트는 얽힘을 통해 양자 상태를 연결할 수 있음, 양자 컴퓨터는 병렬 계산이 가능함, 노이즈와 결잃음은 큐비트의 섬세한 양자 상태 방해, 컴퓨팅 오류를 일으킬 수 있음
- 기본적으로 큐비트는 양자 정보를 저장, 조작 및 얽히기 위한 기반 제공함

○ **QIP 알고리즘 및 애플리케이션**

- 양자 컴퓨팅 잠재력 실현하려면 QIP 알고리즘과 애플리케이션 필요, 알고리즘을 가능하게 하는 기술로 Shor 알고리즘은 QFT (Quantum Fourier Transformation) 및 QPE(Quantum Phase Estimation)을 활용함
- (**양자 시뮬레이션**) 고전 컴퓨터로 분석이 어려운 복잡한 양자 시스템을 양자 컴퓨터 사용하여 시뮬레이션 연구, 응용 분야에는 화학, 재료 과학 및 최적화 포함
- (**Shor 알고리즘**) 고전적 알고리즘과 비교할 때, 큰 숫자를 기하급수적으로 빠르게 인수분해 함, 공개 키 암호화에 대한 잠재적 영향과 암호화 분야의 관심 증대
- (**양자 검색 알고리즘**) Grover 알고리즘은 고전 검색 알고리즘에 비해 2차 속도 향상 제공함, 가능한 응용 프로그램으로 데이터베이스 검색, 데이터 마이닝 및 최적화가 있음
- (**양자 머신 러닝**) 양자 컴퓨터는 전통적 머신 러닝 알고리즘 개선, 새로운 양자 관련 알고리즘 개발에 사용, 양자 머신 러닝 학습 기술 적용 개선 예로 패턴 인식, 최적화 및 데이터 분석 있음
- (**양자 최적화**) 고전 컴퓨터는 포트폴리오 최적화, 공급망 관리 및 물류 관련하여 최상의 솔루션 찾는데 어려움이 있으므로 양자 알고리즘을 문제에 적용, 솔루션 속도를 기하급수적으로 향상

○ QIP에서 양자 오류 수정(QEC) 작동

- 양자 정보 처리의 필수 개념인 양자 오류 수정은 노이즈 및 결잃음으로 인한 오류로부터 양자 상태 보호, 양자 상태의 오류는 양자 상태를 실제로 관찰하지 않고도 양자 역학의 원리 활용하여 감지하고 수정할 수 있음
- (**양자 오류 수정 코드**) 1차적으로 양자 오류 수정 코드 설계가 필요함, 추가 "ancilla" 큐비트 사용하여 원래 양자 상태를 더 큰 Hilbert 공간으로 인코딩함, 인코딩 프로세스에서 정보는 여러 물리적 큐비트에서 분산되어, 중복성 초래함
- (**신드롬 측정**) 양자 상태 오류 정보 제공 외에도, 인코딩된 정보와 직접적으로 관련되지 않고 양자 상태에서 오류의 존재 및 유형에 대한 정보 제공함, 물리적 큐비트의 하위 집합에 일련의 측정 적용하여 증후군을 식별할 수 있음
- (**오류 감지**) 오류의 존재와 위치 확인하기 위해, 측정에서 얻은 증후군을 면밀히 조사, 신드롬 정보 사용하여, 오류 유형(위상 플립 or 비트 플립)과 양자 상태에서 위치 결정
- (**오류 수정**) 오류 감지 후 인코딩된 정보를 복원하기 위해 오류 수정 절차가 적용됨, 오류가 시스템의 큐비트에 미치는 영향을 되돌리기 위해, 양자 게이트 또는 연산을 큐비트에 적용함, 신드롬 정보의 결과로서, 특정 시퀀스의 양자 게이트가 일반적으로 적용되어 문제를 해결함
- (**내결함성 연산**) 오류가 있음에도 양자 오류 수정은 내결함성(Fault-tolernat) 양자 계산의 기초 제공, 오류 수정 절차를 지속적으로 적용하면 오류 완화 가능하므로 연산의 정확성 보장, 내결함성 양자 연산을 위한 좋은 후보인 표면 코드 개발됨
- 양자 오류 수정은 노이즈 및 결잃음으로부터 민감한 양자 상태를 보호하는 QIP 주요 도구임

○ QIP의 제한 사항(한계)

- 컴퓨팅을 혁신할 잠재력에도 불구하고 QIP는 많은 제한이 존재함, 주요 장애물 중 하나는 양자 시스템이 잡음과 환경 상호 작용에 매우 민감함(취약)
- 큐비트의 안정성과 일관성은 계속해서 중요한 문제를 제기함, 큐비트 수를 늘리면 더 복잡해지고 오류율이 높아지므로 현재 양자 시스템은 확장 가능하지 않음

○ QIP를 통한 산업 혁신

- 약물 발견 및 재료 설계에 적용: 분자 상호 작용 및 속성을 시뮬레이션하여 개발 프로세스를 가속화, 보다 효율적인 약물 스크리닝 및 새로운 재료 발견 가능
- 금융 서비스 및 최적화 문제: 포트폴리오 관리, 위험 평가 및 공급망 최적화 개선
- 머신 러닝과 인공 지능(AI): AI 모델의 교육 및 최적화 향상, 보다 정확한 예측과 결정을 내릴 수 있음, 이미지 인식, 자연어 처리 및 패턴 인식 같은 분야 발전에 기여
- 물류 및 운송: 경로 계획, 자원 할당 및 스케줄링 최적화, 보다 비용 효율적이고 효율적인 운송 시스템과 항공 여행 및 도시 계획 같은 산업에서 개선

(원문)

1. https://thequantuminsider.com/2023/07/26/quantum-information-processing-from-bits-to-qubits/