

미래 新기술의 정점, 양자컴퓨터(Quantum Computer) 2부

송완영 연구위원

TRUDER FIRST



미래 新기술의 정점, 양자컴퓨터(Quantum Computer) 2부

송완영 연구위원(wysong@hf.go.kr)

- ❖ 양자컴퓨터는 큐비트 간 중첩과 얽힘 등 양자역학의 특성을 이용하여 디지털 컴퓨터 대비 월등한 계산능력으로 기존 방법의 한계 극복과 동시에 새로운 응용 가능성을 제시하고 있음
- ❖ 범용 양자컴퓨터 구축을 위한 국가 및 글로벌 기업의 관심이 집중되고 있는 바, 2부에서는 양자컴퓨터 구현의 현주소와 응용 분야 및 전망과 시사점 등을 살펴보고자 함

본고의 내용은 집필자의 개인 의견으로 주택금융연구원의 공식적인 견해와 다를 수 있습니다.

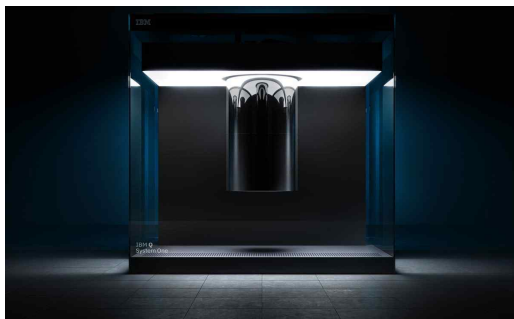
1. 양자컴퓨터 구현

▣ 양자컴퓨터 유형 및 개발현황

● 양자컴퓨터는 크게 아날로그 방식과 디지털 방식으로 분류³⁾

- 디지털 방식은 기존 컴퓨터처럼 일반적인 연산 수행, 즉 범용 목적으로 개발
 - 양자컴퓨팅 기법과 알고리즘을 이용하여 연산처리 속도를 기존 방식에 비해 제곱(quadratic) 또는 지수함수적(exponential)으로 향상
 - 단, 기존 디지털 컴퓨터를 완전히 대체하는 것이 아닌 양자컴퓨팅 방식이 더 효과적인 영역 중심으로 발전 예상
- 아날로그 방식은 캐나다 D-Wave systems 채택 방식이 대표적이며 대부분 최적화 문제 등에 국한된 제한적인 기능으로 범용성이 현재로서는 다소 낮음
 - 최적화 문제에 양자 어닐링(Quantum Annealing) 기법 등을 적용하여 지수함수적 속도 개선

〈디지털 양자컴퓨터 : 20큐비트 IBM Q〉



※ 자료 : IBM

〈아날로그 양자컴퓨터 : 2000큐비트 D-Wave〉



※ 자료 : D-Wave Systems, 가격 \$1,500만

〈주요 양자컴퓨터 유형별 개요〉

구분		아날로그 방식(양자 어닐링)	디지털 방식
특징	응용 범위	▪ 최적화(Optimization) 등에 특화	▪ 범용 목적 추구
	기술적 특징	▪ 원리: 양자 어닐링 ▪ 작동 온도: 10mK (1K ~ -273℃) ▪ 오류정정 방식: 미정	▪ 원리: 양자게이트 구현 ▪ 작동 온도: 10mK ▪ 오류정정 방식: 확정
	큐비트 구현	▪ 초전도 방식 ▪ 현재 약 2,000 큐비트 구현	▪ 초전도, 이온트랩, 광자, 양자점 등 ▪ 20 ~ 72 큐비트 구현
상황	상용화 시기	▪ 2011.5, D-Wave 초기버전 출시	▪ 2020 ~ 21년 예정
	주체	▪ D-Wave Systems, Google 등 ▪ NASA 등 다수 운용 중	▪ IBM, Google, Alibaba 등
	최근 상황	▪ D-Wave 2000Q 출시('17.1.) ▪ Google Quantum Annealer Ver.2 개발 중	▪ IBM Q를 클라우드 형태로 제공, 100만 건 이상 처리 ▪ Google, 2018.3, 72 큐비트 양자 프로세서 공개

※ 자료 : 참고문헌[3] 조성선, “양자컴퓨터 개발 동향과 시사점”, 정보통신기술진흥센터, 2018, 표4

■ 디지털 방식 범용 양자컴퓨터 구현에 필요한 조건

- 기존 디지털 컴퓨터는 실리콘 소재 반도체를 중심으로 발전된 반면 양자컴퓨터는 현재 다양한 가능성을 열어두고 연구가 진행 중
- 양자역학적 특성을 최대한 이용해야 한다는 점에서 제시된 범용 양자컴퓨터 구현을 위한 다섯 가지 요건(DiVincenzo Criteria)은 다음과 같음^{[1][5]}
 - ㉠ 물리적으로 구별 가능한 두 고유상태(0, 1 등), 즉 큐비트 구현이 가능해야 하며 여러 개의 큐비트로 이루어진 시스템을 만들 수 있어야 함
 - 현재 개발 중인 물리적 큐비트는 광자(Photon) 큐비트, 이온 트랩(Ion Trap), 레이저를 이용한 중성원자 포획, 양자점(Quantum Dot), 초전도체 이용 등이 있음
 - ㉡ 기준이 되는, Grover 알고리즘(1부에서 기술) 구현을 위한 초기 큐비트 상태 같은 양자상태를 만들 수 있어야 함
 - ㉢ 큐비트 간 얽힘(Entanglement) 상태를 만들어 필요한 양자연산 게이트(gate) 연산을 수행할 수 있어야 함
 - ㉣ 연산을 하는 동안 연산에 필요한 게이트 이외에는 외부와의 상호작용을 완전히 또는 효율적으로 차단할 수 있어야 함

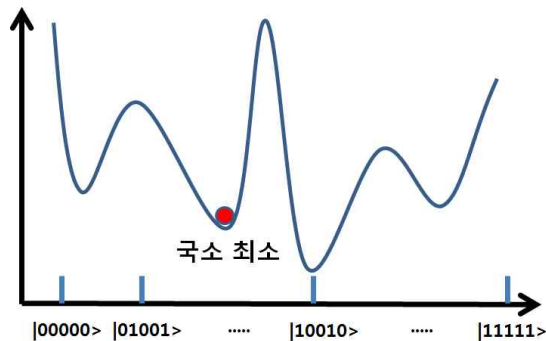
- 양자상태가 외부와의 상호작용으로 고유상태 특성(결맞음; coherence)을 잃어버리는 것을 결잃음(decoherence)이라고 하고, 이 결잃음을 최소화하고 결맞음을 유지하기 위한 오류정정 알고리즘이 마련되어야 함

㉔ 연산 종료 후 원하는 정보를 높은 확률로 측정할 수 있어야 함

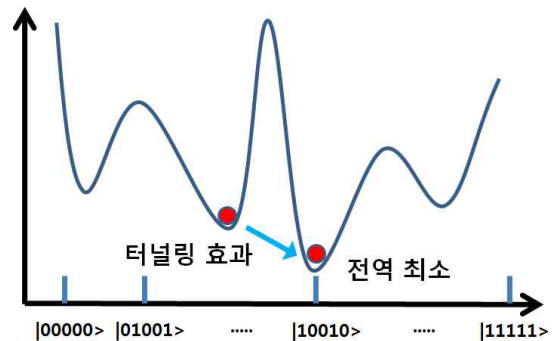
■ 아날로그 방식 양자컴퓨터 : D-Wave System 예시

- D-Wave System은 단열양자컴퓨팅(Adiabatic Quantum Computing)을 양자어닐링 방식으로 구현하여 복잡계의 최소값을 찾는 문제에 응용하고 있음
 - 어닐링 기법의 핵심은 여러 산봉우리가 있는 지역에 비가 내린 후 시간이 지나면서 중력에 의해 낮은 곳 중심으로 물이 고이는 현상을 이용하여 가장 낮은 위치를 찾는 과정에 비유할 수 있음
- 거시세계 또는 고전역학에서는 찾은 위치가 국소 최소점(local minimum)일 가능성도 있으나 양자역학에서는 양자터널링 효과(1부에서 기술)에 의해 전역 최소점(global minimum)을 높은 확률로 찾을 수 있음(그림 참조)

〈Local Minimum : False minimum〉



〈Global Minimum : True minimum〉



- D-Wave System은 ㉑ 초전도체 큐비트 2,000여 개 준비하고, ㉒ 큐비트 간 상호작용을 최소값을 찾고자 하는 문제에 맞게 설정한 뒤, ㉓ 자기장을 가한 후 서서히 풀어주는 작업을 반복하여 시스템 에너지가 최소가 되는 큐비트 조합을 찾음
- 따라서 어닐링 방식의 양자컴퓨터는 양자알고리즘 및 양자게이트를 이용하여 연산을 수행하는 것이 아니라 자연법칙에 맡겨(*Nature knows the answer*) 문제를 해결하고자 하는 접근 방식임
- 현재는 최적화 문제 등에만 국한되어 사용되며, 범용 양자컴퓨터를 활용하여 수행할 수 있는 작업이 제한되어 진정한 의미의 양자컴퓨터가 아니라는 논란 지속

2. 양자컴퓨터 응용 분야

■ 상용화 시 활용 기대 분야

- 양자컴퓨터는 기존 컴퓨터 응용분야를 모두 대체하는 것이 아니라 양자역학적 특성을 이용한 연산이 보다 우월하고 효율적인 분야에 우선 적용될 전망

〈양자컴퓨터 활용 분야 예시〉

분야	응용 예	사례
IT	▪ 기계학습 연산속도 개선 ▪ 고속 이미지 인식	▪ Google, D-Wave Systems 등의 이미지 인식 정확도 향상
화학	▪ 분자설계 ▪ 화학반응 양자 시뮬레이션	▪ IonQ 화학 시뮬레이션 SW ▪ MicroSoft, Havard 대학 등 기초 연구
제약	▪ 단백질 3차원 구조 분석, 알츠하이머병 등 특효약 개발	▪ Stanford Folding@home 프로젝트 ▪ Havard, D-Wave Systems 단백질 분석 실험
의료	▪ 암 치료용 약물, 최적 복용량 산출 ▪ 개인 맞춤형 의료	▪ Stanford, Texas 대학 기초 연구
교통	▪ 도시 교통 서비스 최적화	▪ Volkswagen, Google 공동 개발 ▪ Volkswagen, 주문형 이동 서비스를 위한 알고리즘 개발
항공·우주	▪ 유체역학적으로 최적화된 기체 설계 ▪ 비행 제어 시스템 버그 탐색 최적화	▪ NASA, 비행체 날개 설계 최적화 ▪ Lockheed Martin, Airbus 등의 제어 시스템 버그 탐색 SW개발 (6개월 → 6주)
금융	▪ 포트폴리오 최적화 ▪ 금융상품 프라이싱 ▪ 리스크 관리	▪ '16년, D-Wave Systems, "Quantum for Quants" 설립 ▪ 바클레이즈, 골드만삭스 등 기초 연구 투자

※ 자료 : 참고문헌[3] 조성선, "양자컴퓨터 개발 동향과 시사점", 정보통신기술진흥센터, 2018, 표3

■ 양자 기계학습(Quantum Machine Learning)

- 빅데이터 시대를 맞이하여 양자컴퓨팅 기술을 기계학습에 적용하려는 시도 급증
 - 최근 폭발적으로 증가하고 있는 비정형 데이터에 대한 분석과 활용을 위해 딥러닝(Deep Learning)을 포함한 기계학습 방법론의 중요성이 높아지고 있으며, 처리속도 개선을 위한 병렬·분산 처리 및 양자컴퓨터 활용 등 다양한 방법 모색
 - 기계학습은 주어진 입력데이터를 분석하고 그 결과를 토대로 내부 변수를 문제해결에 적합하게 변화시켜 컴퓨터가 직접 학습하는 효과를 얻도록 유도하는 알고리즘
 - 학습에 필요한 데이터가 많을수록 기계학습 효과가 증가하나 계산시간 역시 급증하므로 보다 강력한 컴퓨팅 파워 요구

- 양자컴퓨팅은 기존 기계학습 알고리즘 계산속도 개선에 기여하거나 양자어닐링 방식으로 문제해결을 시도하는 두 가지 접근방식 존재^[2]
 - 기계학습 알고리즘은 대부분 벡터(길이 N) 또는 행렬($N \times N$) 연산을 수반, 따라서 계산 복잡도는 $O(\text{다항식}(N))$ 수준인 반면, 양자알고리즘은 작게는 $O(\text{다항식}(\sqrt{N}))$ 수준의 제곱 개선, 크게는 $O(\text{다항식}(\log \sqrt{N}))$ 수준의 지수적 성능 향상 기대
 - 양자어닐링 방식은 최근 각광받는 딥러닝 기법에 필요한 비용함수(Cost Function)의 최소값을 찾는 문제에 응용될 경우 지수적 성능개선이 기대되며, D-Wave System과 같이 현재 기술로 구현 및 즉시 적용이 가능하다는 측면에서 관심이 집중됨

■ 양자컴퓨팅과 금융

- 금융시장의 발전과 더불어 금융데이터에 대한 투명성 및 접근 용이성이 개선되면서 보다 세밀한 정량적(Quantitative) 금융 분석이 가능해지고 있음
 - 포트폴리오 최적화, 금융상품 프라이싱(Pricing), 정량적 리스크 측정 등에 동원되는 금융공학(Financial Engineering) 기법들은 공통적으로 장시간 연산이 요구되며, 이에 양자컴퓨터 연산속도 개선을 이용한 문제해결에 금융기관의 관심이 높아짐
- 금융공학 기법 중 몬테카를로 시뮬레이션(Monte-Carlo Simulation)은 프라이싱 및 VaR(Value at Risk) 산출 등 정량적 리스크관리 분야에 필수 요소
 - 몬테카를로 방법은 무작위로 추출된 난수(Random Number) 집합을 이용하여 어떤 함수의 값을 확률적으로 계산하는 기법이며, 정답(Exact Solution)에 대한 근사치이므로 어느 정도의 오차(ϵ)가 존재
 - 대수의 법칙(The Law of Large Numbers)에 의하면 N 개 샘플 평균 $\tilde{\mu}$ 는 N 이 충분히 크면 참값 μ 에 높은 확률로 수렴, 즉 아래 식이 성립함(σ 는 표준편차)

$$\Pr(|\tilde{\mu} - \mu| \geq \epsilon) \leq \sigma^2 / (N\epsilon^2)$$

- 오차를 줄이거나 참값에 근접한 결과를 얻으려면 시뮬레이션 횟수를 늘리는 방법뿐이나, 계산시간 제약 및 이에 따른 병렬처리 비용 증가 등 현실적인 한계가 존재
- IBM은 최근 자체개발 양자알고리즘을 이용한 VaR, ES(Expected Shortfall) 등, 정량적 리스크 측정 계산속도 개선(Quadratic speed-up) 발표^[7]
 - 연산속도 개선은 시행횟수 증가에 따른 보다 정교한 리스크량 측정뿐만 아니라, 시간 제약의 한계로 반기나 분기별로 실시하던 주요 리스크 모니터링 지표산출과 시나리오 분석 등의 주기를 짧게 하여 금융시장 변동에 따른 선제적 대응을 가능케 할 것임

3. 양자컴퓨터의 미래와 시사점

■ 주요국 양자컴퓨터 개발 동향

- 1982년, 미국 물리학자 파인만(R. Feynman)이 최초로 양자컴퓨터의 가능성을 제시¹⁸⁾한 이후 주요 국가들은 양자컴퓨터 구현과 알고리즘 개발에 박차를 가하고 있음

〈주요국 양자컴퓨터 개발 동향〉

구분	주요 내용
미국	▪ 벨 연구소, Shor 알고리즘 및 Grover 알고리즘 개발 ▪ NSA(국가안보국), 기존 RSA 암호체계를 무력화 할 수 있는 양자컴퓨터 개발에 7,970만 달러 투자계획 발표('15.2) ▪ LogiQ 프로젝트: IBM을 연구수행 기관으로 선정, '16년부터 시작된 5개년 프로젝트. 불완전한 물리적 큐비트로부터 논리적 큐비트 구축 ▪ QEO 프로젝트: 조합 최적화 문제를 양자 어닐링으로 해결 목표. 기존 컴퓨터 대비 10,000배 빠른 양자컴퓨터 구축 목표
캐나다	▪ 정부와 대학이 연합하여 IQST, IQC등 양자정보 분야 연구소 설립, 연간 예산은 300~500만 달러 수준
유럽	▪ '10년부터 AQUTE, Q-ESSENCE, SOLID 등의 프로젝트 진행, 광자, 원자 기반 양자컴퓨터 개발, 예산은 약 500만~1,000만 유로 ▪ '16년 'Quantum Manifesto' 프로젝트 발표, '18년부터 10년간 4대 분야(양자통신, 양자소자 계측, 양자컴퓨터, 양자시뮬레이션)에 10억 유로 투자
영국	▪ '14년 공학·물리과학 연구위원회, 5년간 2억 7,000만 파운드의 연구자금을 투입하는 National Quantum Technologies Programme 시작
중국	▪ 중점과학연구분야 중 하나로 양자컴퓨터를 선정하고, 양자통신, 양자컴퓨터 산업 육성을 골자로 한 로드맵 공개('15) ▪ Alibaba와 공동 출범한 양자컴퓨터 연구소를 통해 오는 2025년까지 세계 최고속 슈퍼컴퓨터 수준 양자컴퓨터를 개발하며, 2030년까지는 500~1,000 큐비트의 양자컴퓨터 개발 계획 ▪ '18부터 5년간 1,000억 위안(약 17조 원)을 투입, 원거리 양자통신망 구축 및 양자컴퓨터 개발 ▪ '18년, 늦어도 '20년까지 기존 컴퓨터보다 연산 능력 100만 배 이상 빠른 양자컴퓨터 개발 목표
일본	▪ 레이저 네트워크 방식 신형 양자컴퓨터 등 다양한 연구 진행 ▪ 문부과학성, 양자컴퓨터 실용화 방침 아래 '18년부터 10년간 약 ¥300억 투입 예정
한국	▪ 향후 5년 간 양자컴퓨터 핵심 원천 기술개발과 양자알고리즘 기반 소프트웨어 등에 총 445억 원 투자, 2019년에는 총 60억 원 투입 예정

※ 자료 : 참고문헌[3] 조성선, “양자컴퓨터 개발 동향과 시사점”, 정보통신기술진흥센터, 2018, 표5 재구성

■ 해결 과제 : 큐비트 확장 vs. 오류 보정

- 중첩과 얽힘 특성, 그리고 양자알고리즘 등은 이론적으로는 완벽하나 시스템으로 구현하고 활용성이 높아지려면 오류 발생 가능성이 충분히 낮아져야 함
 - 안정적인 큐비트 구현과 연산능력 확대를 위한 큐비트 수 확장은 필수, 그러나 양자역학이 지배하는 미시세계의 고유상태는 외부 환경에 의해 끊임없이 간섭을 받아 본래 상태, 즉 결맞음을 장시간 유지하기 어려움
- 외부간섭에 의한 고유상태 및 큐비트 얽힘 상태 변화, 연산게이트 부정확성 등에서 발생하는 오류로 인해 최종결과에 대한 신뢰성 저하
 - 외부환경과 완전히 격리된 환경조성이 필수이나, 불가피하게 발생할 수 있는 오류를 보정하는 ‘오류보정 큐비트 시스템’이 추가로 필요
- 현재 50큐비트 수준의 양자컴퓨터는 ‘오류가 존재하는 중간 규모의 양자 (NISQ : Noisy Intermediate-Scale Quantum)’ 기술로 평가¹⁰⁾
 - 양자컴퓨터가 실제로 유용한가의 관점에서, 큐비트 구현 및 확장이 중요한 것이 아니라 양자오류에 의한 불완전성을 어떻게 극복할 것인가가 불확실하기 때문에 가까운 미래에 적용될 수 있는 응용 분야는 매우 제한될 전망
- 양자 오류보정은 결함 없는 진정한 양자컴퓨팅 기술 구현에 핵심 요소로서, 엄청난 비용부담을 얼마나 빨리 감소시키는가에 따라 상용화 시기 판가름
 - 1-큐비트 오류 보정에 수백 내지는 수천 규모 큐비트가 추가로 필요할 것으로 예상
 - D-Wave Systems 같은 아날로그 방식은 아직 오류보정에 대한 알고리즘 또는 대책이 불완전하여 컴퓨팅 결과에 대한 신뢰성에 의문이 제기되고 있는 상황

■ Quantum Jump 대비

- 양자컴퓨터는 기초과학, 의료, 교통·물류, 제약, IT, AI, 금융 등 실생활과 관련된 거의 모든 분야에 적용 가능
 - 상용화 시 기존 기술로는 불가능했던 또는 미루어왔던 것들이 실제로 구현되면서 경제·사회적으로 커다란 변화를 가져올 것이 확실
- 1940년 대 18,000여 개의 진공관을 이용한 초기 컴퓨터(ENIAC: Electronic Numerical Integrator And Computer)는 거의 건물 크기였으나 현재는 손바닥에 올려놓을 수 있는 수준임을 고려할 때 집중적인 투자와 경쟁이 지속된다면 양자컴퓨터 상용화 시대는 곧 도래할 것으로 예상

- 1996년, ENIAC 탄생 50주년을 기념하기 위해 미국 펜실베니아 대학 전기전자과 학생들 주축으로 ENIAC 회로를 실리콘 칩에 복원했을 때, 그 크기는 가로 7.44밀리미터, 세로 3.29밀리미터에 불과했음^[11]
- 우리나라는 국가차원 지원이 부족하고 민간기업 연구 또한 초기 단계이긴 하나, 양자컴퓨터 상용화를 위한 해결과제가 많은 만큼 집중적·정책적 투자를 통한 경쟁력 확보가 요구됨
- 세계 각국 및 글로벌 기업들의 기술 선점을 위한 경쟁이 치열한 가운데 양자컴퓨터에 대한 영향력과 파급력에 대한 이해도 제고 필요
- 양자컴퓨팅 기술 개발은 선택이 아닌 필수이며, 다가올 4차 산업혁명 시대의 주도권을 획득할 수 있는 필수 요소임을 인지

<참고문헌>

- [1] 김재완, “양자원리와 컴퓨터”, 물리학과 첨단기술, 2012.12
- [2] 정원주, 이성환, “양자 기계학습 기술의 현황 및 전망”, Journal of KIISE, Vol. 43, No. 7, 2016
- [3] 조성선, “양자컴퓨터 개발 동향과 시사점”, 정보통신기술진흥센터, 2018
- [4] 과학기술정보통신부, ‘양자컴퓨팅 기술개발사업 추진계획’, 2019.02
- [5] D. P. DiVincenzo, “The Physical Implementation of Quantum Computation,” Fortschritte der Physik. 48, 771 (2000)
- [6] R. Orus et al, “Quantum computing for finance, overview and prospects”, arXiv:1807.0389, 2018
- [7] S. Woerner et al, "Speeding up risk assessment through quantum algorithms", IBM Research-Zurich, 2019
- [8] R. Feynman, "Simulating Physics with Computers", International Journal of Theoretical Physics 21, no 6/7, 467, 1982
- [9] M. Russo et al, “The Coming Quantum Leap in Computing”, BCG(The Boston Consulting Group), 2018
- [10] J. Preskill, “Quantum Computing in the NISQ era and beyond”, arXiv:1801.00862, 2018
- [11] G. Johnson, “A shortcut through time : The path to the quantum computer”, 2003

■ 작성자 : 송원영 연구위원 (051-663-8157 / wysong@hf.go.kr)

■ 본고의 내용은 집필자의 개인의견으로 주택금융연구원의 공식적인 견해와 다를 수 있습니다.