양자 거북이와 고전 토끼

- 양자 컴퓨팅은 어떤 문제를 빠르게 풀 수 있을 것인가?

최석웅 뉴욕주립대 알바니 경영대학(University at Albany, State University of New York) 교수
sukwoongchoi@gmail.com

서론

무어의 법칙(Moore's Law)대로 발전한 기존 (혹은 고전) 컴퓨팅(Classical Computing)이 효율성의 한계를 맞았고 여러 가지 대안이 모색되고 있는 상황이다. 그중 양자 컴퓨팅(Quantum Computing)이 한 가지 대안으로 떠올랐고 현재 많은 관심을 받고 있다. 양자 컴퓨팅이 기존 컴퓨팅보다 빠른 속도 향상을 가질 수 있는 이유는 단순히 말하자면 근본적인 연산 방식의 차이 때문에 발생한다. 기존 컴퓨팅이 Bit 단위의 연산(0과 1로 구분해 계산)을 진행했다면, 양자컴퓨팅은 Qubit 단위의 연산(0과 1을 동시에 계산)을 진행해서 기존 컴퓨터보다 계산 속도가 빠를 수 있다는 것이 양자 컴퓨팅에 대한 현재의 기술적 기대이다.

이에 따라 IBM, 구글, 마이크로소프트, IONQ 등 많은 기업들이 양자 컴퓨터를 연구 개발하고 있다. 이 기업들은 초전도체(Superconducting) Qubit와 이온 트랩(Ion Trapped) Qubit와 같은 다양한 기술을 활용하여 양자 컴퓨터의 성능을 향상시키고 있다. 예를 들어, 초전도체 기반의 양자 컴퓨터는 매우 낮은 온도에서 작동하여 전기 저항이 없는 상태를 이용해 높은 처리 속도를 가능하게 하며, 이온 트랩 기술은 개별 이온을 전자기장으로 포획하여 안정적인 Qubit를 제공한다.

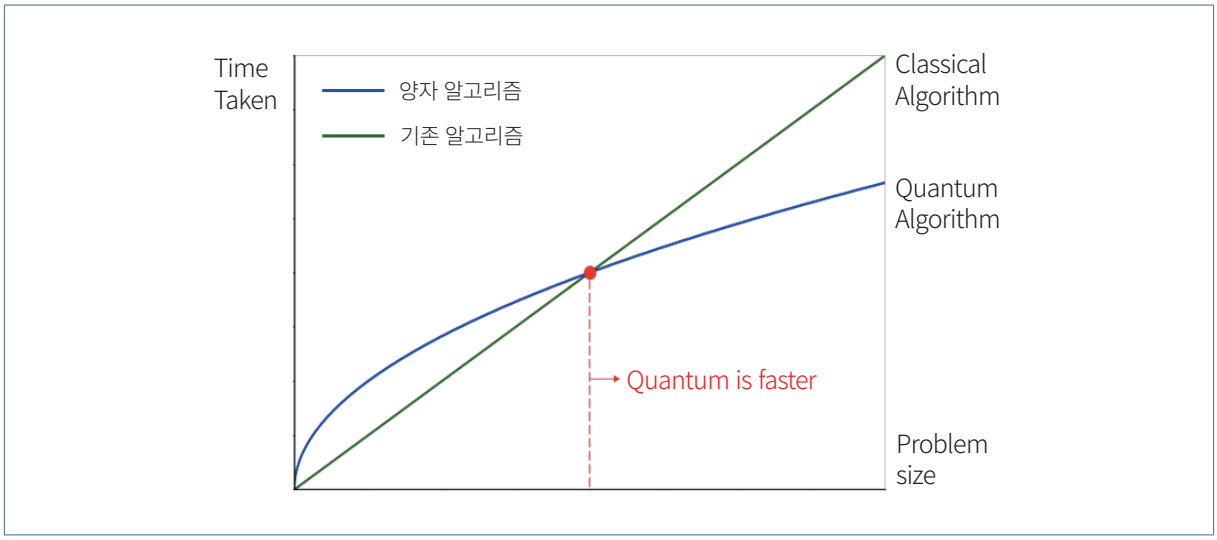
양자 알고리즘 측면에서는 쇼어 알고리즘(Shor's algorithm)과 그로벌 알고리즘(Grover's Algorithm)이 대표적인 예로 꼽힌다. 쇼어 알고리즘은 큰 수를 소인수분해하는 데 있어 고전 컴퓨터보다 훨씬 빠른 속도를 제공하며, 그로벌 알고리즘은 데이터베이스 검색에서 획기적인 성능 향상을 제공한다.

국가 단위에서는 미국이 2023년 $1 Billion 정도의 큰 금액을 향후 4~5년간 양자 컴퓨팅에 투자한다는 발표를 했고, 중국과 EU 역시 마찬가지로 큰 투자를 향후 해 나갈 계획이다.
이러한 양자 컴퓨팅에 관한 관심은 양자 컴퓨팅이 곧 상용화될 것처럼 그리고 모든 분야에 양자 컴퓨터가 적용된다면 게임 체인저가 될 수 있다는 기대와 이야기들이 많이 있는 것도 사실이다. 하지만 현재 양자 컴퓨터의 발전 속도와 어떤 문제에서 기존 컴퓨팅 대비 양자 컴퓨팅이 속도를 더 빨리 가져갈 수 있을지는 아직 불명확하다.

양자 경제적 우위 프레임워크

이 글의 목표는 기술에 능통하지 않은 비전문가도 접근할 수 있는 양자 컴퓨팅 사고방식을 제공하고 아직 양자 알고리즘이 발명되지 않았더라도 실제 문제에 대한 양자 컴퓨팅의 잠재력을 이해하는 것을 목표로 하고 있다.
양자 알고리즘의 속도를 결정하는 것은 시간 복잡도(Time Complexity)와 입력 데이터의 크기(Problem Size)에 따라 달라질 수 있다. 시간 복잡도는 n개의 입력 데이터에 대하여 알고리즘이 문제를 해결하는 데 얼마큼의 시간이 걸리는지를 나타내며, 이 복잡도는 알고리즘 수행에 필요한 Step 수로 측정된다. 이는 입력 데이터의 크기에 달려 있으며, Step 수가 많을수록 복잡도가 높다는 것을 의미하고 이는 알고리즘의 속도가 더 느리다는 것을 의미한다.

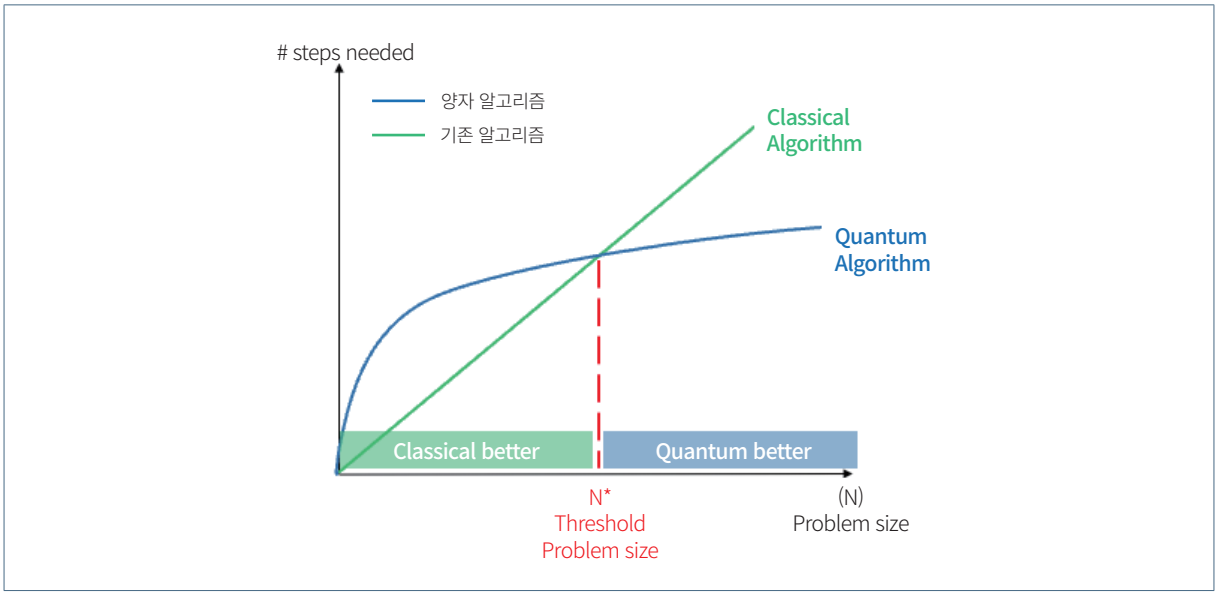
[그림 1] 왜 더 나은 양자 알고리즘이 입력 크기가 충분히 클 때만 기존 알고리즘을 능가하는지에 관한 개념적 설명[1]



1 양자 컴퓨터(하드웨어)는 현재 더 느리게 작동하므로, 동일한 시간 단위(Y축에서) 내에 고전 컴퓨터보다 훨씬 적은 계산을 수행할 수 있다.

[그림1]은 알고리즘 성능에 대한 기존 알고리즘(Classical Algorithm)과 양자 알고리즘(Quantum Algorithm)의 경쟁을 개념적으로 보여준다. Y축은 시간이 얼마나 걸리는지를, X축은 입력데이터의 크기를 나타내는데, 같은 기능을 가진 알고리즘이 기존방식이나 양자방식에 따라서 그 성능이 다를 수 있음을 보여주고 있다. 특히, 이 모델은 초기에는 기존 알고리즘의 성능이 우수하지만, 시간이 지나 특정 입력 데이터 크기를 지났을 경우는 양자 알고리즘이 더 우수하다는 것을 나타내고 있다.

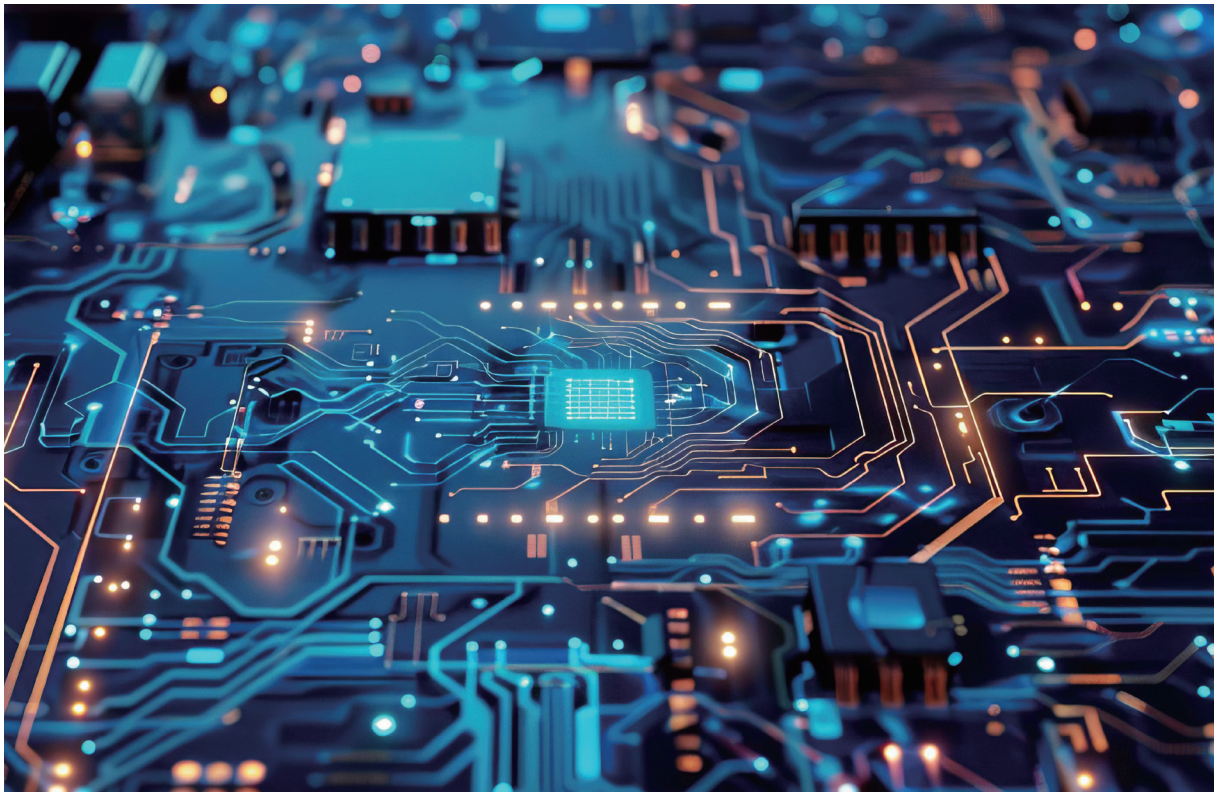
[그림 2] 왜 더 나은 양자 알고리즘이 입력 크기가 충분히 클 때만 기존 알고리즘을 능가하는지에 관한 구체적 설명[2]



좀 더 구체적이면서 기술적 설명을 위해 [그림 2]에서 Algorithm 1은 n개의 입력 데이터 사이즈를 가지고 있고, Algorithm 2는 1,000,000$\sqrt{n}$이 있다고 가정하자. 그림과 같이 하나는 기존 알고리즘(Classical Algorithm)을 가리키고, 다른 하나는 양자 알고리즘(Quantum Algorithm)을 가리키며, 특정 입력 데이터 크기에서 양자 알고리즘이 더 빨라지는 것을 볼 수 있다.

다시 말해, 해당 프레임워크의 시사점은 기존 컴퓨터가 더 빠르기 때문에, 양자 컴퓨터는 더 나은 알고리즘을 가졌을 때만 기존 컴퓨터보다 더 빠를 수 있다는 것이다. 하지만 그렇다 하더라도, 양자 컴퓨터가 충분히 큰 알고리즘적 이점을 제공하려면, 입력 데이터의 크기(N*)가 충분히 커야 한다. 이 경우, 기업들이 양자컴퓨터 개발 계획을 밝힌 양자 로드맵을 확인하여 N* 크기의 문제를 계산할 수 있는 충분한 Qubit가 언제쯤 가능한지 알 수 있다. 이때가 양자 컴퓨터가 경제적 우위를 가지는 순간일 것이다.

2 양자 컴퓨터 (하드웨어)는 현재 더 느리게 작동하므로, 동일한 시간 단위(Y축에서) 내에 고전 컴퓨터보다 훨씬 적은 계산을 수행할 수 있다.



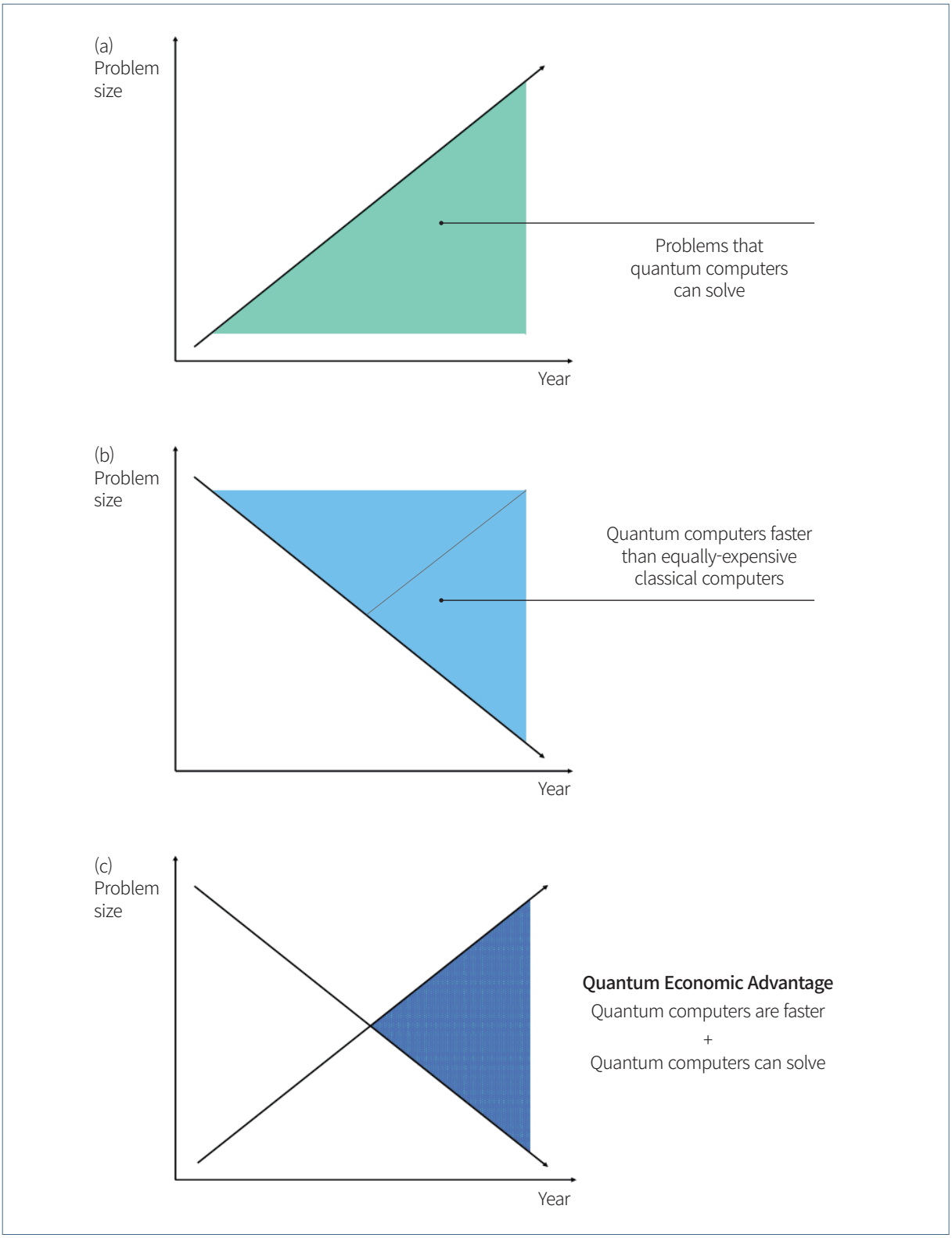
기존의 **양자 우위(Quantum Advantage)**는 '특정 문제에 대한 모든 기존 컴퓨터를 능가할 수 있는 양자 컴퓨터가 존재한다.'는 개념이다. 하지만, 이 글에서 말하는 양자의 우위는 **양자 경제적 우위(Quantum Economic Advantage)**로 '특정 문제(및 입력 데이터의 크기)에 대해 비슷한 비용의 기존 컴퓨터를 능가할 수 있는 양자 컴퓨터가 존재한다.'는 것이다.

위의 개념 차이는 중요한데, 그 이유는 이 글이 기존의 연구나 미디어에서 말하는 양자 우위와는 다른 양자 경제적 우위에 대해 다루기 때문이다. 양자 경제적 우위 정의에는 두 가지 중요한 조건이 포함된다. 첫째, 양자 컴퓨터는 문제를 실행할 수 있을 만큼 충분히 강력해야 한다. 둘째, 양자 컴퓨터는 고전 컴퓨터보다 더 빨리 실행해야 한다. 즉, 문제가 '실행 가능'하고 충분한 '알고리즘적 이점'을 가져야 한다.

1. 실행 가능성(Feasibility)

문제가 양자 컴퓨터에 대해 실행 가능해지려면, 그 컴퓨터가 실제로 문제를 실행할 수 있을 만큼 충분히 강력해야 한다. 오늘날의 하드웨어에서, 양자 실행 가능성에 가장 중요한 기여 요소는 시스템이 구현 가능한 오류 수정 기능을 사용하여 문제를 실행할 수 있을 만큼 충분한 Qubit를 가지고 있는지 여부이다. Qubit 수가 증가하고 오류 수정이 개선됨에 따라 더 많은 문제가 실행 가능해질 것이다. 이 정의에서 알 수 있듯이, 양자 실행 가능성은 해결할 수 있는 문제에 대한 제약 조건이다. 이 해석은 도식적으로 [그림 3(a)]에 나타나 있다.

[그림 3(a), (b), (c)] 양자 경제적 우위가 발생하는 시점에 대한 도식적 표현으로, 다음을 포함한다. **(a)실행 가능성**: 양자 컴퓨터가 특정 문제 크기를 해결할 만큼 충분히 강력한 경우 **(b)알고리즘적 이점**: 더 나은 양자 알고리즘이 고전 컴퓨터의 속도 이점을 극복할 만큼 충분한 이점을 제공하는 경우 이 제약 조건들을 종합하면 **(c)양자 경제적 우위**의 겹치는 영역이 나타난다.



2. 알고리즘적 이점(Algorithmic Advantage)

문제가 알고리즘적 이점을 가지려면, 그 문제 크기에 대해 양자 컴퓨터가 비슷한 비용의 고전 컴퓨터보다 더 빠르게 계산할 수 있어야 한다. 이 글의 제목에서 비유한 '경주'와 같이 양자 컴퓨터와 비슷한 비용의 고전 컴퓨터는 서로 경쟁한다. 양자 컴퓨터가 알고리즘적 이점을 가지려면, 더 나은 알고리즘이 고전 컴퓨터의 속도를 극복할 만큼 충분한 이점을 제공해야 한다. 또한, 필요한 오류 수정 오버헤드도 극복해야 한다. 이러한 요소들을 충족하기 위해서는 문제의 크기가 충분히 커야 한다. 이는 [그림 3(b)]의 파란색 영역에 나타나 있다. 여기서는 시간이 지남에 따라 양자 컴퓨터가 고전 컴퓨터보다 더 빠르게 개선된다는 가정 아래에 곡선이 하향 기울기로 나타난다.

이 두 가지 제약 조건을 결합하면, [그림 3(c)]의 겹치는 영역에서 알 수 있듯이 양자 우위는 쐐기 모양의 패턴으로 나타날 것이다. 더 구체적으로 말하면, 이 프레임워크는 양자 컴퓨터가 문제에 따라 우위의 위치가 달라진다는 것을 시사한다. 초기에는 해당 연도의 양자 컴퓨터에 적합할 만큼 작지만 특정 문제 크기에만 더 나은 알고리즘에서 충분한 이점을 얻을 수 있다는 것이다. 그 이후에는 양자 컴퓨터가 더 빠르고, 저렴하며, 더 유능해짐에 따라 문제 크기의 범위("양자 우위 문제 크기")가 확대될 것이다.

3. 예시 – DNA 검색

위의 프레임워크를 적용할 예시를 찾는다면 DNA 검색을 들 수 있다. 사람의 유전체는 약 30억 개의 염기쌍으로 구성되어 있으며, 이를 입력 데이터 크기로 표현하자면 10^9 정도의 크기다. 기존의 선형 검색 알고리즘은 n개의 입력 데이터 크기가 필요했다면, 양자 선형 검색 알고리즘은 $\sqrt{n}$의 크기가 필요하다. 기존 컴퓨터와 현재의 양자 컴퓨터 성능의 차이 등을 고려하는 상숫값이 10^6이라면, 위의 프레임워크에서 말한 N*의 식은 n=1,000,000$\sqrt{n}$이고, n=10^{12}이다. 이 입력 데이터 값을 필요한 Qubit의 값으로 치환한다면, log_2=(10^{12})=40 logical qubits[3]이 필요하다. 현재 많은 연구들로 양자 기술의 에러율[4]이 줄어들고 있지만, 한 개의 Logical Qubit을 만들기 위해서 현재 1,000개의 Physical Qubit[5]이 필요하다고 가정한다면 이는

3 Logical Qubit은 오류 수정 코드와 같은 기법을 통해 오류가 거의 없는 안정적인 Qubit을 의미한다. 이는 여러 Physical Qubit을 조합하여 만들어지며, 안정적인 양자 연산을 수행하기 위해 필수적이다.

4 Qubit의 에러율: Qubit의 에러율은 양자 컴퓨팅에서 중요한 문제로, 이는 Qubit가 원하는 상태를 유지하지 못하고 오류가 발생하는 빈도를 의미한다. 에러율은 주로 다음과 같은 요인에 의해 결정된다.
1. 디코히런스(Decoherence): Qubit가 외부 환경과 상호작용을 하여 양자 상태를 잃는 현상. 이는 Qubit가 초전도체, 이온 트랩 등 다양한 기술로 구현되는 과정에서 발생할 수 있다.
2. 게이트 오류(Gate Errors): 양자 게이트를 적용하는 동안 발생하는 오류. 이는 제어 신호의 불완전성이나 하드웨어의 한계로 인해 발생할 수 있다.
3. 읽기 오류(Readout Errors): Qubit의 상태를 측정하는 과정에서 발생하는 오류. 이는 측정 장비의 정밀도와 관련이 있다.
현재 대부분의 Physical Qubit은 비교적 높은 에러율을 가지고 있으며, 이는 안정적인 양자 연산을 위해 오류 수정 기법이 필요함을 의미한다. 여러 Physical Qubit을 조합하여 Logical Qubit을 만들고, 이를 통해 에러율을 낮추고 신뢰성을 높이는 것이 현재 양자 컴퓨팅 기술의 핵심 과제 중 하나이다. 현재 알려진 에러율은 Logical Qubit 1개당 Physical Qubit 1,000개 정도로 가정하고 있다.

5 Physical Qubit은 실제 하드웨어에서 구현된 기본 단위 Qubit를 의미한다. 이는 오류에 취약하며, 여러 Physical Qubit이 모여 하나의 Logical Qubit을 형성하게 된다. 안정적인 양자 연산을 위해서는 많은 수의 Physical Qubit이 필요하다.

40,000개의 Physical Qubit을 필요로 한다. 이 가정을 바탕으로 IBM Quantum Roadmap에 적용해 본다면, 2028년 이후에 퀀텀 컴퓨팅(Quantum Computing)이 경제적 우위를 차지할 수 있으리라 보인다.

[그림 4] 시간 복잡도를 고려해 일반적인 분석을 했을 경우, 양자 컴퓨터가 우위에 있는 경우

Quantum time complexity

Classical time complexity	$exp(n)$	n^3	n^2	$nlogn$	n	$logn$
$exp(n)$		23	20	18	17	15
n^3			10^6	2,819	1,000	173
n^2				10^7	10^6	2,819
$nlogn$					$10^{434,248}$	10^6
n						10^7
$logn$						

If classical is exponential and quantum not, then quantum wins

If classical is near-linear, quantum only wins for very large problems

[그림 4] 안의 숫자의 값들은 기존 시간 복잡도와 양자 시간 복잡도의 차이를 바탕으로 N* 값을 구했을 때 나오는 값들이다. 만약에 기존 시간 복잡도가 지수적인 크기이고 양자 시간 복잡도가 아니라면, 양자 컴퓨팅이 경제적 우위를 차지할 것이다. 하지만, 기존 시간 복잡도가 선형적 값을 보인다면, 양자 컴퓨팅이 경제적 우위를 갖는 경우는 아주 큰 입력 데이터 크기일 경우만일 것이다.

결론

양자 컴퓨팅이 모든 면에서 경제적으로 우위에 있는 것은 아니다. 특정한 상황에 따라 이점이 다르다. 제목의 비유처럼 고전적인 토끼(기존 컴퓨팅)는 더 빠르고, 작은 입력 데이터 크기에 적합한 반면, 양자 거북이(양자 컴퓨팅)는 더 느리지만, 더 나은 알고리즘으로 큰 입력 데이터 크기에 적합하다. 양자 경제적 우위 프레임워크는 (1)실행 가능성과 (2)알고리즘적 이점이라는 두 가지 차원을 통해 경제적 우위를 확인하게 한다.

실행 가능성은 양자 컴퓨터가 문제를 해결할 만큼 충분히 큰 경우를 의미하고, 알고리즘적 이점은 입력 데이터 크기가 충분히 커서 양자 알고리즘의 이점이 동일한 비용의 기존 컴퓨터보다 더 나은 경우이다. 우리가 논의한 프레임워크를 기준으로 혜택을 볼 분야는 매우 큰 문제들(예: 모든 알려진 유전체를 검색)이나 훨씬 더 나은 양자 알고리즘이 필요한 어려운 고전적 문제들(예: 소인수분해) 등이 있다. 반면에, 혜택을 보지 못할 분야로는 이미 충분히 좋은 성능을 가지고 있는 기존 알고리즘이 해결하는 중요한 문제들이나 대부분 일상의 비즈니스 문제들이기 때문에, 양자 컴퓨팅이 어느 경우에도 다 좋다고 말하기는 어렵다.

이 연구를 바탕으로 할 수 있는 미래의 연구들은 다음과 같다. 첫째, 현재는 IBM의 양자 로드맵을 활용한 분석을 하였지만 IONQ와 같이 다른 기술들에 이 프레임워크를 적용할 수 있다. 둘째, 기업들의 알고리즘 사용 정보를 활용하여 그들이 어떻게 양자 기술을 적용할지 예측할 수 있다. 셋째, 기업이나 산업 수준으로 양자 노출 지수를 계산할 수 있다. 넷째, 양자 컴퓨팅이 거시 경제 생산성에 미칠 영향을 예측할 수 있다.

⊙ 참고문헌

Choi, S., Moses, W., & Thompson, N. (2024) The Quantum Tortoise and the Classical Hare: A simple framework for understanding which problems quantum computing will accelerate (and which it will not). Available here: https://arxiv.org/pdf/2310.15505

Thompson, N., Dukatz, C., Shukla, P. P., & Choi, S. (2024). Practical Quantum Computing is about More Than Just Hardware Quantum Economic Advantage : A New Practical Framework. *California Management Review*. Available here: https://cmr.berkeley.edu/2024/03/practical-quantum-computing-is-about-more-than-just-hardware/