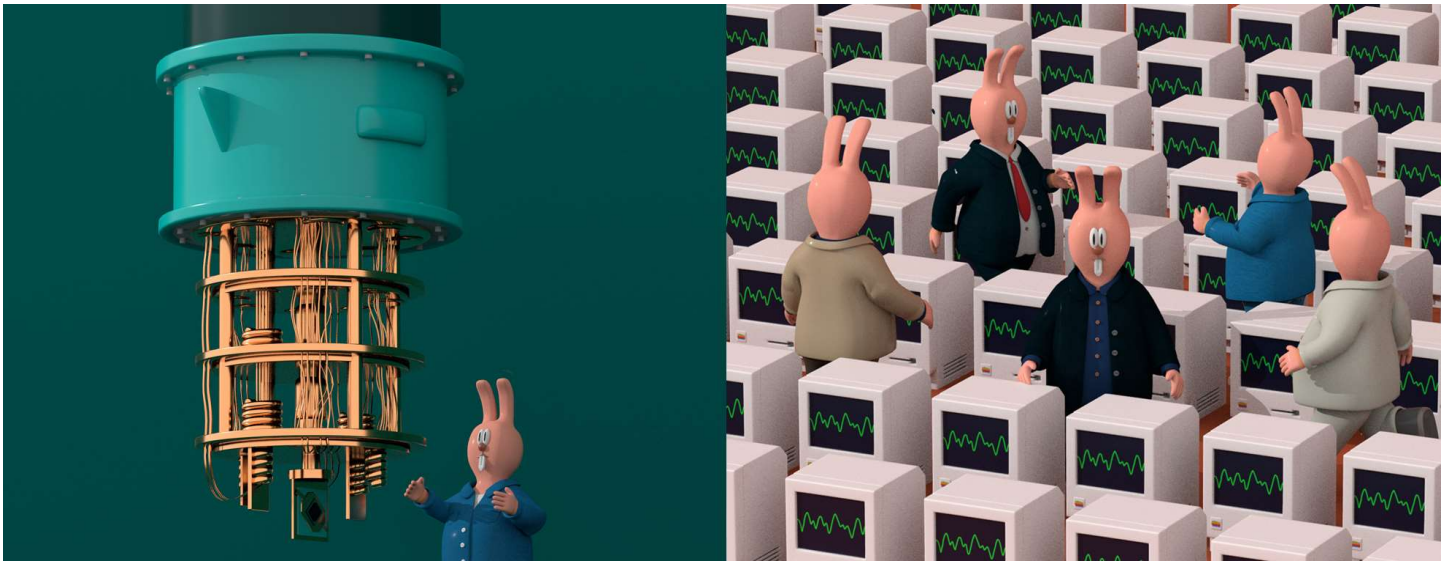
양자 컴퓨터

양자 우월성

2020년 12월 15일

김한영

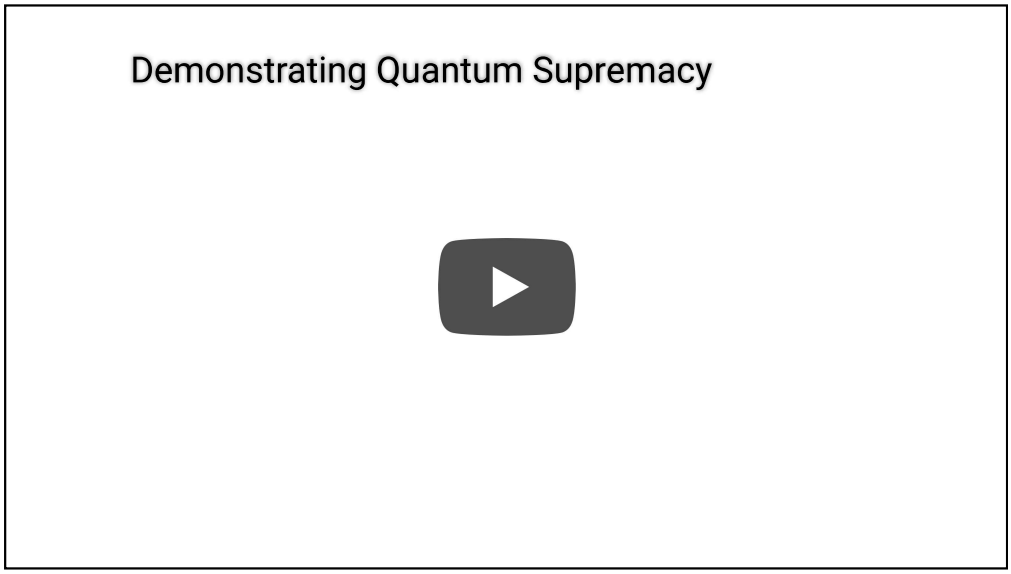


지난 2019년 10월 구글의 양자 컴퓨터 팀은 양자 우월성Quantum Supremacy을 달성하는 데 성공했다고 발표했다. 구글의 최고 경영자인 선다 피차이Sundar Pichai까지 참여했던 발표 내용은 곧 각종 뉴스 매체를 통해 보도되기 시작했다. 이에 맞서 IBM의 양자 컴퓨터 팀은 구글의 주장에 무리가 있다는 발표를 냈다. 두 라이벌 사이에서 오가는 설전은 한동안 양자 컴퓨터 학계의 중요한 가십거리가 되었다.

필자가 기억하기로는 양자 컴퓨터가 뉴스 매체에서 이 정도로 큰 이슈가 된 적은 없었다. 양자 우월성이라는 개념이 도대체 무엇이길래 사람들이 이렇게 호들갑을 떠는 것일까? 간단히 말하자면 양자 우월성은 고전 컴퓨터로는 꿈도 꿀 수 없을 만큼 어려운 계산을 양자 컴퓨터를 사용해 손쉽게 해낸다는 것을 말한다. 즉, 구글의 주장은 자신들의 양자 컴퓨터를 이용해서 고전 컴퓨터로는 사실상 하기 불가능한 연산을 해냈다는 것이다.

실제로 구글은 자신들이 양자 컴퓨터로 해낸 연산을 고전 컴퓨터로 수행하려면 수만 년 이상의 시간이 걸릴 것이라고 예상했다. 하지만 IBM은 이에 반박하는 성명을 내면서 현재 존재하는 고전 슈퍼 컴퓨터를 이용하면 몇 주 내지 몇 달 안에 충분히 같은 계산을 할 수 있을 것이라고 주장했다. 마치 라이벌 스포츠 팀이 기자회견에서 서로 신경전과 설전을 벌이는 장면을 연상케 하는 이러한 발표는 최근 양자 컴퓨터계에서 벌어진 흥미로운 일이 아닐 수 없다.

여하튼 확실한 건 구글의 양자 컴퓨터가 한 계산을 고전 컴퓨터로 하려면 엄청난 연산량이 필요하다는 점이다. 연산하는데 필요한 시간이 매우 길 뿐 아니라, 이를 계산하기 위해서는 고전 컴퓨터에 수만 개의 CPU와 GPU란 연산장치가 들어가야 한다(일반 개인용 컴퓨터에는 불과 몇 개의 CPU와 GPU만 들어간다). 이에 비해서 같은 계산을 수행한 양자 컴퓨터의 크기는 (불과 50개 남짓한 큐빗만 있으니) 매우 작은 편이다. 때문에 구글이 일종의 양자 우월성을 달성했다는 것에 대해 큰 이견은 없는 편이라고 보는 것이 좋다.



그렇다면 구글은 도대체 어떠한 연산을 했기에 고전 컴퓨터로는 하기 어려운 계산을 했다고 주장하는 것일까? 또 구글이 양자 우월성을 달성했다는 사실은 과학적으로나 사회적으로 보았을 때 어떤 의미가 있는 것일까? 이번 글을 통해 알아보도록 하자.

양자 우월성 실험

우선 구글의 양자 컴퓨터 팀이 한 일이 무엇인지에 대해서 알아보도록 하자. 구글 팀이 한 일을 이해하기 위해서는 양자 우월성 실험을 두 부분으로 나누어서 이해하는 것이 좋다. 한쪽은 양자 컴퓨터를 이용해 어떤 연산을 했느냐이고, 다른 쪽은 고전 컴퓨터를 이용해서 이 결과를 어떻게 분석했는지에 관한 내용이다. 일반적으로 과학 실험이 어떻게 이루어지는지 생각해 보면 전자는 실험실에서 흔히 이루어지는 실험으로 생각할 수 있고 후자는 이 실험 결과를 분석하는 과정이라고 생각할 수 있다.

구글의 양자 컴퓨터 팀은 실험에서 시카모어Sycamore라는 양자 컴퓨터 칩을 이용했다. 시카모어는 총 53개의 큐빗이 2차원의 격자 구조로 배열되어 있다. ([그림1] 참조) 각각의 큐빗에는 최대 네 개의 이웃하는 큐빗이 있고, 서로 이웃하는 큐빗들 사이에서는 구글의 연구자들이 원하는 임의의 양자 연산을 할 수 있게끔 되어 있다.

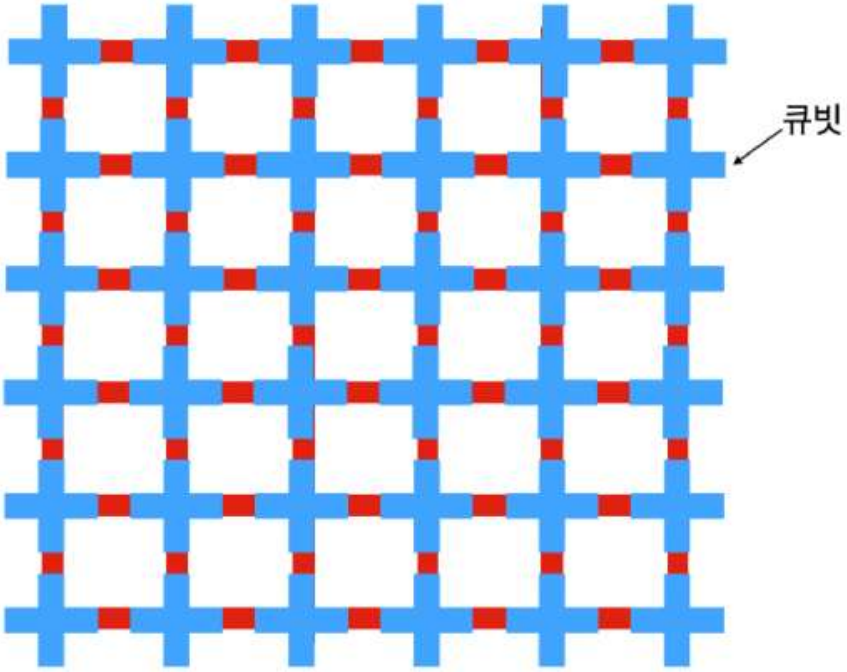


그림1 시카모어Sycamore칩의 격자 구조. 파란색 " + " 형태의 소자가 큐빗 하나에 해당되고 각각의 큐빗은 최대 네 개의 이웃하는 큐빗과 연결되어 있다. 실제 칩에는 53개의 큐빗이 있다. / 김한영 제공

구글은 이 칩을 가지고 다음과 같은 일을 했다. 우선, 이웃하는 큐빗들의 쌍을 전부 찾아서 정리해 보자. 각각의 큐빗은 최대 네 개의 이웃하는 큐빗과 연결되어 있는데, 각각의 쌍마다 임의의 연산을 적용하는 것이다. 예를 들어 보자. 한 쌍의 큐빗이 있을 때 "양자 오류 보정"에서 말했던 CNOT라는 연산을 할 수도 있고

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |11\rangle \\ |11\rangle &\rightarrow |10\rangle \end{aligned} \quad \cdots \quad (1)$$

큐빗 하나를 정해서 임의로 위상을 바꿔 버릴 수도 있다:

$$\begin{aligned} |0\rangle &\rightarrow |0\rangle \\ |1\rangle &\rightarrow e^{-i\theta}|1\rangle. \end{aligned} \quad \cdots \quad (2)$$

아니면 $|0\rangle$과 $|1\rangle$의 진폭을 바꿀 수도 있다.

$$\begin{aligned} |0\rangle &\rightarrow \cos(\theta)|0\rangle + \sin(\theta)|1\rangle \\ |1\rangle &\rightarrow -\sin(\theta)|0\rangle + \cos(\theta)|1\rangle \end{aligned} \quad \cdots \quad (3)$$

임의의 연산을 한다는 것은 이렇게 가능한 여러 가지 연산 중 하나를 무작위로 골라서 그 연산을 양자 컴퓨터에서 직접 한다는 것을 의미한다. 이 과정을 모든 큐빗 쌍에 적용하는 과정을 대략 14번 정도 반복한 뒤, 모든 큐빗들의 값을 읽어 들이는 것이 실험을 한번 한 것에 해당한다.

만약 정확히 똑같은 실험을 고전 컴퓨터에서 반복했다면, 최종 측정에서 나오는 연산 결과는 매 실험마다 똑같을 것이다. 하지만 양자 역학적으로는 최종 큐빗 상태를 측정하면서 상태가 붕괴되기 때문에 같은 실험을 해도 결과가 계속해서 다르게 나올 수 있다. 중요한 점은 여기서 나오는 결과의 확률 분포가 무엇인지이다. 이는 바로 Porter-Thomas 분

포라는 확률 분포를 따른다.

Porter-Thomas 분포는 완벽한 난수와는 다른 패턴을 보인다. 예를 들어서 n개의 비트로 이루어진 **비트 스트링**을 생각해 보자. 여기서 비트 스트링은 0이나 1로 이루어진 배열을 말한다. 예를 들어, 5개의 비트로 이루어진 비트스트링의 한 예로는 01110을 들 수 있다. 완벽한 난수라면 각각의 비트 스트링이 나올 확률은 정확히 2^{-n}일 것이다. 가령 구글의 실험 결과가 완벽한 난수라면 다음과 같은 비트스트링이 나올 확률은 정확히 $2^{-53} \approx 1.11 \times 10^{-16}$이 된다.

$$10110101111101000010101010010010110101111101000010101 \quad \cdots \quad (4)$$

구글의 양자 연산이 만들어낸 확률 분포에서 위와 같은 비트 스트링이 나올 확률은 2^{-n}에 비례하긴 하지만, 어떤 특정한 비트 스트링이 나올 확률은 2^{-n}보다 조금 크고 또 다른 비트 스트링들이 나올 확률은 2^{-n}보다 작다. 어차피 특정한 비트스트링이 나올 확률이 지수적으로 매우 작은 숫자인데, 거기에 살짝 변화가 생기는 게 무슨 차이를 줄까 싶겠지만, 총 가능한 비트 스트링의 숫자가 2^n개나 되기 때문에 이 작은 차이가 확률 분포 전체로 보았을 때는 큰 차이를 가져올 수 있다.

구글의 양자 컴퓨터 팀은 자신들이 만들어낸 통계 분포가 이론적으로 예측되는 Porter-Thomas 분포와 얼마나 가까운지 계산하기 위해 교차 에트로피cross entropy라고 불리는 다음과 같은 양을 계산했다:

$$\sum_x p(x) \log q(x). \quad \cdots \quad (5)$$

여기서 $p(x)$는 x라는 결과가 실험에서 실제로 관측될 확률이고 $q(x)$는 이론적으로 그러한 결과가 나올 확률을 계산한 값이다. 하지만 $q(x)$를 실제로 계산하기 위해서는 굉장히 많은 연산이 필요하다. 가능한 x의 경우를 다 합해보면 $2^n = 2^{53} \approx 9 \times 10^{15}$이고, 주어진 x에 대한 $q(x)$를 일일이 계산하는 데도 지수함수적으로 오랜 시간이 필요하다. 더군다나 실제로 $p(x)$의 값을 정확하게 측정하기 위해서는 역시나 지수함수적인 시간이 필요하다.

이런 방법 대신 구글은 다음과 같은 방식으로 계산했다. 위에서 말한 실험을 수행한 후, 실험 결과를 읽어 들인다. 만약 그 결과가 x라면 그에 해당하는 $q(x)$를 직접 계산한다. 이런 작업을 여러 번 반복해서 얻어진 $q(x)$값에 대해 평균을 취하는 대신, $\log q(x)$의 평균을 취하면 그것이 바로 우리가 원하는 교차 엔트로피가 된다. 비록 $q(x)$ 하나하나를 계산하는 일은 여전히 지수함수적으로 어려운 일이지만, 구글은 회사 내에 있는 많은 컴퓨터들을 이용해서 이를 직접 계산해냈다.

이러한 방식을 통해 구글 양자 컴퓨터 팀은 측정된 교차 엔트로피의 값이 이론적으로 예측한 값에 가깝다는 사실을 보였다. 이는 우리가 이론적으로 양자 컴퓨터에게 기대하는 일을 구글이 실제로 했다는 데 대한 중요한 증거로 작용한다. 즉 우리는 구글이 만든 양자 컴퓨터가 이론이 예측하는 대로 잘 작동하고 있다고 유추할 수 있다.

복잡도 이론

구글 측은 위에서 필자가 설명한 실험을 통해서 양자 우월성을 달성했다고 주장한다. 그 주장의 골자는 다음과 같다. 구글의 양자 컴퓨터로는 Porter-Thomas 분포를 따르는 비트 스트링들을 손쉽게 만들어 낼 수 있다. 이에 반해, 고전 컴퓨터로 같은 연산을 하려면 지수함수적으로 증가하는 연산량이 필요하다. 앞에서 말한 실험은 간단한 양자 회로를 약 14번만 반복해서 적용하면 되는, 어렵지 않은 실험이다. 그런데 고전 컴퓨터로는 지수함수적인 연산량이 필요하다는 주장은 왜 나온 것일까?

연재글

양자 컴퓨터 시대의 문턱에서

1. 양자 컴퓨터의 기원
2. 양자 알고리즘: 소인수 분해 알고리즘
3. 양자 알고리즘의 세계
4. 양자 오류보정
5. 양자 우월성
6. NISQ[Noisy Intermediate-scale quantum] 시대

이를 이해하기 위해서는 컴퓨터 과학의 기반 중 하나인 **복잡도 이론**[Complexity theory]이라는 분야에 대해서 잠깐 이야기해볼 필요가 있다. 복잡도 이론에서는 다양한 연산을 하기 위해서 얼마나 많은 시간과 저장 공간이 필요한지에 대한 연구를 한다. 구글의 실험이 중요한 이유는, 이미 복잡도 이론에서 구글이 수행한 연산이 어렵다고 "증명"되어 있기 때문이다. 여기서 증명이라는 것은 수학적으로 완벽한 증명을 의미하는 것은 아니다. 구글이 정말로 주장하고 싶은 것은 수학적으로 봤을 때 구글이 한 일을 고전 컴퓨터로 하기 위해서는 지수함수적으로 많은 연산량이 필요할 것이라는 점이다.

하지만 복잡도 이론에서 이러한 주장을 아무런 가정 없이 증명하는 것은 매우 어려운 문제이다. 한 예로 클레이 수학연구소[Clay Institute]에서 백만 불의 상금을 내건 P vs. NP 문제를 들 수 있다. 여기서 P는 다항식처럼 증가하는 시간 안에 풀 수 있는 "쉬운" 문제들을 말하고, NP는 다항식 시간 안에 답이 맞는지 "쉽게" 확인할 수 있는 문제들을 말한다. 다항식 시간 안에 풀 수 있으면 당연히 답이 맞는지 확인도 할 수 있기 때문에 P는 NP에 속한다. 하지만 답을 쉽게 확인할 수 있다고 해서 그 문제를 쉽게 풀 수 있는 것은 아니다. 좋은 사례로 이전 글 "양자 알고리즘:소인수 분해"에서 언급한 소인수 분해를 들 수 있다. 자연수 두 개가 주어졌을 때 둘을 곱하는 것은 쉽지만, 자연수 하나가 주어졌을 때 이를 소인수 분해하는 것은 어려운 일이라는 것이 중론이다. 비록 NP에 있는 일반적인 문제들을 풀기 위해 필연적으로 지수함수적으로 많은 시간이 필요한 것인지에 대한 수학적인 증명이 있는 것은 아니지만, 대다수의 컴퓨터 과학자들은 NP에 속한 일반적인 문제들은 P에 속하지 않는다고 생각한다. 이것이 유명한 P vs. NP 문제이다.

[1] 이는 단순히 예를 든 것이고, 실제로 그렇다는 것은 아니다.

[2] 이는 복잡한 내용이므로 자세히 이야기하지는 않겠다. 관심 있는 독자들은 위키피디아의 다항식 계층에 관한 문서를 참고하기를 권한다.[2]

이 때문에 복잡도 이론에서 "증명"은 이처럼 많은 사람들이 옳다고 생각하는 추정에 기반한다. 예를 들어 구글이 한 실험을 고전적으로 계산하기 어렵다는 점을 아무런 조건 없이 수학적으로 증명하기는 힘들다. 대신 이런 식의 증명을 할 수 있을지도 모른다.

만약 구글이 한 실험을 고전 컴퓨터가 다항식 시간 만에 쉽게 계산할 수 있다고 해 보자. 그리고 이 사실은 곧 NP에 속하는 어떤 문제를 다항식 시간 안에 풀 수 있음을 의미한다는 것을 누군가 증명해 보였다고 가정해보자.[1] 만약 그런 증명이 진짜 존재한다면, 우리는 다음과 같은 결론을 내릴 수 있다. 일단 P와 NP가 다르다는 것을 일종의 **공리**로 받아들이자. 한편 방금 가정한 상황에서는, 구글이 한 계산을 고전 컴퓨터도 손쉽게 할 수 있다면 P와 NP는 같다는 증명이 이미 존재한다. 하지만 이 정리는 애초의 공리, 즉 P와 NP는 서로 다르다는 공리에 위배한다. 따라서 구글이 수행한 실험이 고전 컴퓨터에서는 지수적으로 많은 연산량을 필요로 한다는 결론을 내릴 수밖에 없다. 논리의 흐름을 정리하면 다음과 같이 정리할 수 있다.

1. (가상의) 공리: P는 NP와 다르다.
2. (가상의) 명제: 만약 구글이 한 계산을 다항식 시간 안에 고전 컴퓨터를 이용해 계산할 수 있으면, P와 NP는 같아야만 한다.
3. 결론: 애초의 공리에 따르면 P와 NP는 같을 수 없다. 따라서 구글이 한 계산은 다항식 시간 안에 어떤 고전 컴퓨터를 이용해서도 계산할 수 없다.

복잡도 이론에는 P vs. NP에 대한 추정처럼 다양한 추정들이 있다. 비록 내용이 복잡하기 때문에 이번 지면에서 자세하게 다루기는 힘들지만, 중요한 건 복잡도 이론 내에서 맞다고 추정되는 중요한 명제 중 하나가 바로 구글이 한 실험과 밀접한 관련이 있다는 점이다. 이는 다항식 계층Polynomial Hierarchy의 붕괴에 관한 추정이다.[2] 좀 더 정확히 말하자면, 만약 구글이 한 연산을 고전적인 컴퓨터를 이용해서 다항식 시간 안에 풀 수 있다면 다항식 계층이 붕괴된다는 점은, 수학적으로 엄밀하게 증명된 명제이다. 복잡도 이론 내에서 다항식 계층은 붕괴되지 않는다는 것이 중론이므로 우리는 다음과 같은 논리를 펼칠 수 있다.

1. 공리: 다항식 계층은 붕괴하지 않는다.
2. 수학적인 명제: 만약 구글이 한 계산을 다항식 시간 안에 고전 컴퓨터를 이용해 계산할 수 있으면, 다항식 계층은 붕괴된다.
3. 결론: 다항식 계층은 붕괴되지 않으므로, 구글이 한 계산은 다항식 시간 안에 그 어떠한 고전 컴퓨터를 이용해서도 계산할 수 없다.

비록 다항식 계층이 붕괴되지 않는다는 명제가 수학적으로 엄밀하게 증명된 것은 아니지만, 이는 복잡도 이론을 연구하는 많은 연구자들이 맞다고 생각하는 명제이다. 따라서 구글이 한 계산을 고전 컴퓨터로는 다항식 시간 안에 해낼 수 없다는 것이 양자 컴퓨터 학계 내의 중론이다.

양자 우월성의 의미

이처럼 최근 구글이 한 양자 우월성 실험은 첨단 물리실험과 복잡도 이론의 깊은 수학적인 결과에 기반한 작품이다. 비록 구글이 한 실험을 고전컴퓨터로는 어렵다는 주장이 수학적으로 완전히 엄밀한 것은 아니지만, 대다수의 연구자들은 구글이 한 일이 실제로 고전적인 컴퓨터를 이용해서는 계산하기 힘들 것이라는 점에 동의하고 있다. 물론 양자 우월성 실험 이전에도 양자 컴퓨터와 관련된 실험들은 항상 있어 왔다. 하지만 완전히 잘 제어된 환경에서 작동하는 양자 컴퓨터를 이용해, 고전 컴퓨터로는 사실상 불가능한 계산을 수행한 건, 2019년 구글 양자 컴퓨터 팀이 처음이었다. 이는 수학, 과학, 컴퓨터 과학에서 우리가 알고 있는 수많은 깊은 결과들을 동원한 양자 컴퓨터계의 기념비적인 사건이다.

하지만 그렇다고 해서 양자 컴퓨터가 몇 년 안에 상용화될 것이라고 생각하는 것은 곤란하다. 이전 글 "양자 오류 보정"에서도 말했듯이, 양자 컴퓨터에서는 많은 오류가 발생할 수 있고, 이를 고치기 위해서 오류보정에 대한 지속적인 연구가 이루어져야 한다. 뿐만 아니라, 사람들이 유용하다고 생각하는 알고리즘들은 지금보다 훨씬 대규모의 양자 컴퓨터를 필요로 한다. 비교적 소규모의 양자 컴퓨터로도 유용한 어플리케이션을 만들어 내는 것은 앞으로 양자 컴퓨터 연구자들에게 남겨진 중요한 숙제이다.

양자 우월성을 양자 컴퓨터의 유용성과 결부시켜서 생각하는 것에 대해 필자는 조심스러운 입장이다. 양자 우월성은 대규모의 양자 컴퓨터가 도래하는 시대의 서막을 나타낸다고 생각하는 것은 좋지만, 실제로 인류에게 도움이 되는 시대가 오기 위해서는 여전히 많은 연구가 이루어져야 한다. 그러므로 양자 컴퓨터라는 학문을 상용화가 임박한 분야로 생각하기보다는, 기초학문적으로 접근해서 장기적인 투자와 노력이 수반되어야 하는 분야라는 공감대가 필요한 시점이다.

참고문헌

1. Arute, F., Arya, K., Babbush, R. et al. Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510 (2019).
2. Polynomial Hierarchy (Wikipedia)