

양자컴퓨팅 & 양자머신러닝 연구의 현재와 미래

Research Trends in Quantum Machine Learning

방정호 (J.H. Bang, jbang@etri.re.kr)

양자컴퓨팅연구실 선임연구원

ABSTRACT

Quantum machine learning (QML) is an area of quantum computing that leverages its principles to develop machine learning algorithms and techniques. QML is aimed at combining traditional machine learning with the capabilities of quantum computing to devise approaches for problem solving and (big) data processing. Nevertheless, QML is in its early stage of the research and development. Thus, more theoretical studies are needed to understand whether a significant quantum speedup can be achieved compared with classical machine learning. If this is the case, the underlying physical principles may be explained. First, fundamental concepts and elements of QML should be established. We describe the inception and development of QML, highlighting essential quantum computing algorithms that are integral to QML. The advent of the noisy intermediate-scale quantum era and Google's demonstration of quantum supremacy are then addressed. Finally, we briefly discuss research prospects for QML.

KEYWORDS 양자머신러닝, 양자시뮬레이션, 양자알고리즘, 양자컴퓨팅

I. 양자컴퓨팅: 과거와 현재

1. 고전 vs 양자 컴퓨팅 기본개념

컴퓨팅은 데이터와 정보를 가공하여 원하는 문제를 해결하는 일련의 과정을 의미한다. 이를 위해 물리적 장치인 컴퓨터는 언어와 같은 구성요소들을 가지고 있다. 이러한 언어를 이해하기 위해서는 데이터 또는 정보의 기본 단위 "비트(Bit)"인 "0"과 "1"의 디지털 값을 이해해야 한다. 기존 컴퓨팅에서는

이러한 연속된 비트의 값들로부터 정보를 나타내며, 이 정보를 변환하거나 분류하고 가공하는 일련의 명령을 순차적으로 수행하여 최종 목적값을 얻어낸다. 이러한 명령들의 집합을 "알고리즘"이라고 한다.

양자컴퓨팅은 기본적으로 고전컴퓨터와 기초 틀은 동일하지만, 양자이론을 포함하여 기존 정보이론을 확장한다. 따라서 양자컴퓨팅의 동작 특성은 기존 컴퓨팅과 완전히 다르다는 사실을 우선 알아

* DOI: <https://doi.org/10.22648/ETRI.2023.J.380505>

* 이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임[2019-0-00003, 결합 허용 양자컴퓨팅 시스템 프로그래밍, 구동, 검증 및 구현을 위한 요소기술 개발].

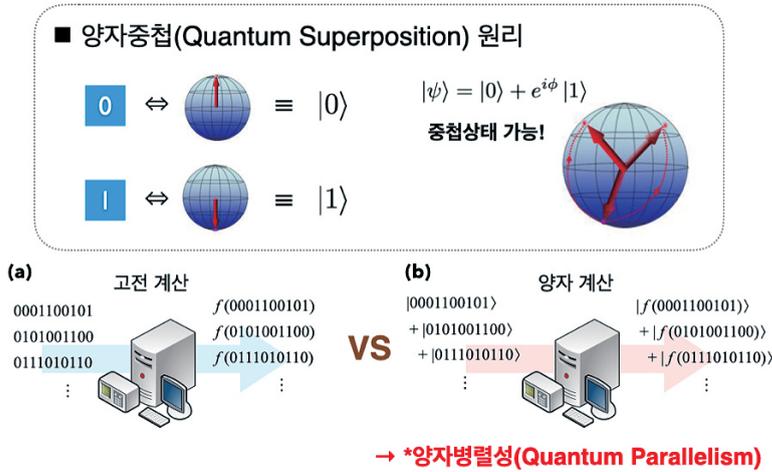


그림 1 (a) 기존 컴퓨팅 vs (b) 양자컴퓨팅

야 한다. 양자정보과학에서 정보의 기본 단위는 고전적인 비트가 아니라 큐비트(Qubit)로 정의된다. 큐비트는 “0”과 “1”을 각각에 해당하는 양자상태로 부호화한 것을 의미한다. 즉, “0”은 “ $|0\rangle$ ”, “1”은 “ $|1\rangle$ ”과 같이 표현된다. 양자컴퓨팅은 큐비트로 구성된 양자정보를 처리하여 원하는 목적값을 얻어내는 과정으로, 이를 수행하는 순차적인 양자연산들의 집합을 “양자알고리즘”이라고 한다[1].

양자이론은 큐비트 상태들 간의 양자중첩(Superposition)과 양자얽힘(Entanglement) 등을 허용한다. 이러한 특성으로 큐비트는 결정론적(Deterministic) 상태표현과 동시에 양자중첩표현도 가능하다(예: $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$). 양자알고리즘 구성을 위한 양자연산들은 양자중첩을 적극적으로 활용한다. 이는 여러 번의 입/출력 과정이 양자컴퓨팅에서는 소위 “양자병렬성”을 이용하여 단 한 번의 연산으로 처리하는 것을 가능하게 한다(그림 1). 이와 같은 양자병렬성은 양자컴퓨팅에의 속도향상에 가장 중요한 물리적인 기작으로 밝혀졌다.¹⁾

양자병렬성의 활용을 위해서는 큐비트 상태들을 원하는 기준상태로 잘 초기화해야 하고, 범용컴퓨

팅을 위한 단위 양자연산들이 잘 정의되어 있어야 하며, 정밀한 양자측정이 가능해야 한다. 또한, 컴퓨팅 과정에서 양자중첩이 파괴되거나 변형되는, 이른바 양자결풀림(Decoherence)에 가급적 강건해야 한다. 현재, 양자광학계, 이온포획, 초전도체, 양자점 등 여러 가지 물리적 기반 고품질 큐비트 생성/제어 기술 개발이 진행되고 있다.

2. 초창기 및 현재 양자컴퓨팅 연구

- 초창기: 1990년대 후반, Shor의 소인수분해 알고리즘[2], Grover의 양자데이터검색 알고리즘[3] 등과 같이 고전알고리즘 대비 극적인 속도향상을 갖는 몇몇 기념비적 알고리즘들이 개발되었다. 이때부터, 양자컴퓨팅 연구는 집중조명을 받기 시작했다. 현재 양자정보/컴퓨팅 연구는 이론적 측면에서 지난 20~30여 년간

1) 양자병렬성이 필수불가결 양자요소이기기는 하지만 그 전부는 아니다. 최근 연구에 따르면, 양자컴퓨팅에의 성능향상은 양자얽힘 등과 관련하여 보다 포괄적인 형태의 양자기작으로 기술되어야 한다.

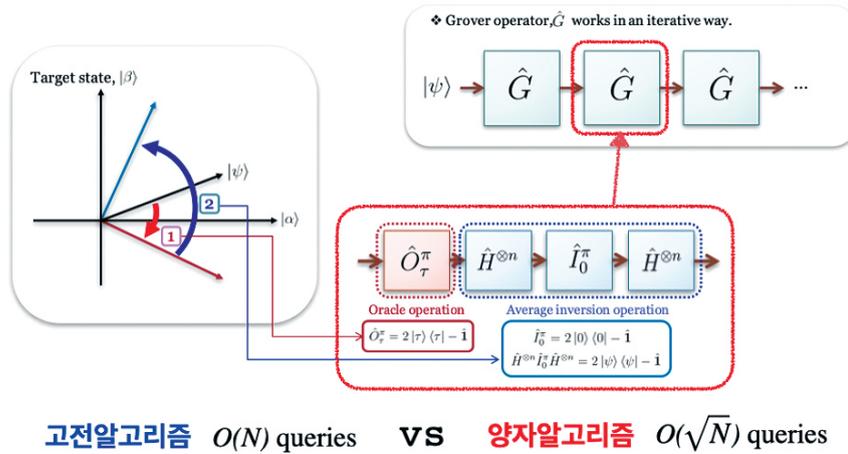


그림 2 양자진폭증폭 프로세스

상당한 성과를 이루어냈다. 하지만, 실제 구현 측면에서 해결해야 할 문제들이 산재해 있는 것도 사실이다. 현시점에서 양자컴퓨팅 속도 향상 및 이론/SW 연구는 이미 완성단계에 있다는 일부 주장이 있지만 이는 전혀 사실이 아니다.

현재까지 개발된 양자알고리즘은 Deutsch-Jozsa, 소인수분해, Hidden-Subgroup 문제, 양자데이터검색 등 소수에 불과하다. 따라서, 양자컴퓨팅 개발에의 연구동기를 보다 강화하기 위해서는 새로운 양자알고리즘 및 양자소프트웨어가 개발되거나 새로운 형태의 문제구성 및 해결 스토리가 필요한 실정이다.

- 현재: 최근, 오류를 허용하며(Noisy), 중간 규모(Intermediate-Scale)에서, 실현 가능한 양자기술(Quantum)을 추구하자는, 소위 “NISQ 원리”에 입각한 연구가 현실적/실용적 관점에서 크게 주목받고 있다[4]. 특히, NISQ 원리에 충실한 문제구성 및 해결방법을 찾는 연구 방향이 양자정보 과학기술 분야의 중장기 대세이다. NISQ 비전에 적합한 연구 콘텐츠로서, 최근

고전-양자 융합 알고리즘 및 계산화학/다체계 문제 응용연구가 “양자시뮬레이션” 혹은 “양자인공신경망” 등과 같은 하위분야로 체계화되고, 여러 선도그룹 중심으로 깊은 연구가 수행되고 있다[5].

보다 최근에는 방대한 데이터의 가공/분류 및 고차원적 지식체계의 구조화 등에 이용되는 머신러닝에의 양자성능향상이 가능한지에 대한 이론연구 또한 매우 활발하다. 이와 더불어 양자성을 이용한 머신러닝에의 속도향상 기작이 구체적으로 증명됨에 따라, “양자머신러닝”과 같은 부속분야가 형성되었다. 양자머신러닝은 현재 양자정보/컴퓨팅 이론 전반에 새로운 키워드를 제공하고 있다[6].

3. 주요 양자컴퓨팅 알고리즘

가. 양자 소인수분해 알고리즘

주어진 두 수의 곱은 일반적으로 컴퓨터가 쉽게 계산할 수 있지만, 그 역인 소인수분해는 큰 수의 경우 기존 컴퓨터에서는 지수함수적 연산 노력(시

간)이 필요하다.²⁾ 그러나, Shor는 양자컴퓨터를 이용하면 지수함수적 속도향상이 가능함을 입증하였다[2].

Shor 알고리즘은 “양자-푸리에 변환(Quantum Fourier Transform)”이라고 불리는 양자병렬연산 모듈을 활용한다. 푸리에 변환은 과학과 공학 전반에서 매우 유용한 연산 도구이다. 양자-푸리에 변환은 푸리에 변환의 양자 버전으로서, 특정 양자상태를 켈레공간의 양자상태 증첩으로 표현할 수 있게끔 한다. 양자 소인수분해 알고리즘은 이러한 양자-푸리에 변환을 이용하여 양자병렬성을 극대화하고, 소인수분해의 핵심 작업인 주기성 문제를 빠르게 해결하여 지수함수적 속도향상을 이룬다.

이와 같은 양자 소인수분해 알고리즘의 등장으로 양자컴퓨팅 연구는 새로운 전기를 맞게 되었다. 특히, 소인수분해의 난해성에 기반한 기존 암호체계가 양자컴퓨팅 관점에서는 더 이상 그 안전성을 확보할 수 없게 됨으로써 양자암호 등의 분야가 시작되었다.

나. 양자 데이터검색 알고리즘

일반적으로 정리되지 않은 데이터들 중 원하는 데이터를 검색하거나 추출하는 데는 데이터의 개수만큼의 계산 노력(시간)이 필요하다. 예를 들어, 전화번호부에서 특정 이름으로 전화번호를 검색할 때, 이름이 “가나다...” 순으로 정렬되어 있지 않다면, 최악의 경우 모든 사람의 이름을 확인해야 한다. 결국, 일반적으로 검색 문제는 데이터 개수만큼의 단위 검색이 필요하다.

반면에, 양자컴퓨팅을 활용하면 데이터 개수의 제곱근만큼의 단위 검색만으로도 원하는 데이터를

찾을 수 있다. 이를 위해 데이터에 해당하는 모든 레이블의 양자중첩을 준비해야 한다. 데이터 검색(혹은 접속)에 해당하는 연산 모듈을 통해 찾고자 하는 데이터의 확률 진폭은 해당 상태의 보강 간섭을 통해 증가시키고, 다른 데이터들의 확률 진폭은 상쇄 간섭을 통해 감소시키는 원리로 이러한 연산이 가능하다. 이에 해당 알고리즘은 일종의 클래스 네임으로서 “양자진폭증폭(Quantum Amplitude Amplification)”이라고 한다(그림 2)[3].

다. 양자 선형문제 알고리즘(HHL)

대부분의 선형시스템의 문제들은 과학/공학은 물론, 경제학, 생물학 등 학문 전반에서 다루지는 중요한 문제로, 수학적으로는 다음과 같은 선형 방정식의 풀이로 환원된다.

$$Ax=b. (A \in \mathbb{R}^{N \times N}, x, b \in \mathbb{R}^N)$$

여기서 A 는 탐구대상인 시스템과 관련된 $N \times N$ 행렬이고, 목적은 주어진 벡터 b 에 대하여 벡터 x 를 구하는 것이다. 이 문제는 결국 A 행렬의 대각화 과정 문제로 귀결된다.

알려진 고전알고리즘의 경우(예: QR factorization), 탐구 대상 시스템의 차원 N 에 대하여 $O(N^3)$ 정도에 해당하는 계산 노력³⁾ 정도로 문제를 해결할 수 있다. 대상 시스템에 특별한 외부조건을 부여하지 않을 경우, 보다 효율적으로 문제를 풀 수 있는 알고리즘은 기존 컴퓨팅에서는 아직 알려지지 않았다.

반면에, 양자컴퓨팅의 경우, $O(\log(N))$ 정도의 계산 노력만으로 문제를 해결할 수 있는 세팅이 가능

2) 약 190자리의 소인수분해는 2.2GHz CPU 30개의 병렬계산으로 5개월 이상의 시간이 걸린다.

3) 여기서 “ $O(\cdot)$ ”은 점근표기법의 하나로 Big-O 혹은 란다우 표기법이라고 한다. 계산이론에서 시간복잡도를 나타낼 때 흔히 사용한다.

하다.⁴⁾ 이와 같은 양자알고리즘을 최초 연구자들의 이름(Harrow, Hassidim, Lloyd)을 차용하여, “HHL” 알고리즘이라고 명명하였다[7]. HHL 역시 핵심은 앞서 설명한 양자(데이터)샘플의 중첩 및 양자병렬성의 적극 활용에 있다.

II. 양자머신러닝 연구

1. 양자머신러닝이란

최근, 머신러닝과 양자이론을 결합한 “양자머신러닝(QML: Quantum Machine Learning)” 연구가 매우 활발히 진행되고 있다. QML의 주요 연구 이슈는 머신러닝의 기반이론을 양자물리학 영역으로 확장하여 기존의 고전 머신러닝보다 의미 있는 양자 속도향상을 얻을 수 있는지, 그리고 이런 속도향상이 가능하다면 어떤 물리적 기작으로 설명할 수 있는지, 그리고 현실적인 문제에 어떻게 적용할 수 있는지 등이다. 이러한 내용은 계산학습이론의 학습성능 평가지표에 대한 일반적인 연구와 유사한 측면이 있으며, 일부 연구들은 십수 년 전에 이미 시도되었다. 하지만, QML 연구의 필요성과 유용성에 대한 논의는 최근까지 깊이 이뤄지지 않았다. 그러던 중, MIT의 Seth Lloyd 교수팀 등에 의해 “양자 서포트 벡터머신”과 같은 연구 결과가 발표되면서 QML 분야 연구에의 강력한 연구동기가 생겨났다[8].

하지만, 아직 QML 연구는 초기 단계로서, 견고하게 정립된 용어나 개념이 없다. 또한, 관련 후속 연구들은 주로 선형시스템을 다루는 양자컴퓨팅과 알고리즘의 속도향상에 기반하고 있으며, 현시점에서 속도향상을 가능케 하는 양자성의 물리적 기작

과 효율적인 활용 방안에 대해서는 아직 구체적으로 증명되지 않았다.

2. 양자학습속도향상: 양자 샘플 복잡도

양자병렬성을 적극 활용하여 계산과학 전반에 새로운 활력을 불어넣는 동시에 정보 및 컴퓨팅 이론의 기반이론을 양자이론으로 확장하고자 했던 초창기 노력과 더불어, 머신러닝에의 양자속도향상에 대한 일반적인 증명 역시 이때 시도된 바가 있다.

특히, 계산 복잡도(Computational Complexity) 측면에서 정의된 학습에의 성능지표를 바탕으로 일반적인 형태의 양자학습속도향상을 증명하고자 하는 연구는 지금까지도 계속 시도되고 있다.

계산과학에서의 “복잡도(Complexity)”란 흔히 어떤 알고리즘을 실행에 옮길 때 드는 총비용을 뜻하는데, 대체로 컴퓨터가 해당 작업을 성공적으로 마치는 데 드는 시간 혹은 메모리를 양을 의미한다. 머신러닝에서는 원하는 작업을 마칠 때까지 수행하는 의미 있는 정보추출과정으로서의 “질의(Query)” 연산 총횟수 혹은 필요한 “샘플 데이터의 사이즈” 등으로 정의된 학습 성능지표가 존재한다.

이 같은 프레임의 연구에서, 기본적으로 머신러닝은 주어진 훈련 데이터 샘플들($x \in X$)을 원하는 목적 출력($y \in Y$)과 대응시키는 어떤 목적함수($c \in C$)에 대한 가설($h \in H$)들을 식별하는 일련의 모든 과정이라고 정의할 수 있다. 계산과학적으로 어떤 학습모델의 우수성은 다음과 같이 평가할 수 있다: 1) 우선, 비교적 학습하는 데 필요한 데이터 사이즈가 작을수록 좋은 학습이라고 할 수 있다. 2) 그리고, 학습한 이후 식별된 가설들의 정확도가 높을수록, 또 학습이 원리적으로 불가한 상황들이 없을수록 좋다. 이와 같은 요소들을 반영하여 일반적인 학습에의 평가지표를 정의하고 다양한 학습모델에 적용

4) HHL에 대한 몇 가지 오해 중 하나가, HHL이 선형시스템의 온전한 풀이를 가능케 한다는 점이다. 하지만 실제로 HHL은 벡터 x 를 온전히 특정할 수 없으며 오직 x 의 기댓값만을 준다.

하는 분야를 “계산학습이론(Computational Learning Theory)”이라고 한다.

어떤 학습 주체(내지는 학습 알고리즘) A 는 최종적으로 식별하고자 하는 목적함수와 관련된 주요정보를 추출하기 위해 질의연산을 호출할 수 있다고 가정해 보자. 이 질의연산은 알고리즘 내에서 실제 문제정보에 접근할 수 있는 유일한 연산으로서, 흔히 “오라클(Oracle)”이라고 부른다. 어떤 주어진 학습 알고리즘 A 가 오라클을 최대한 활용하여, 최소 $1-\delta$ 의 확률로 최종 가설 h 를 식별했을 때(Probably Correct), 그리고 동시에 이때 식별된 가설 h 의 정확도가 $1-\epsilon$ 이상일 때(Approximately Correct), 해당 학습 알고리즘과 목적함수의 탐색이 가능한 혹은 해가 존재하는 공간 등을 바탕으로 “Probably-Approximately-Correct(PAC)”라고 부르는 계산학습모델이 정의된다. PAC 학습모델에서는 최종 학습까지의 오라클 질의횟수 관점에서 학습에의 난이도가 결정되는데, 이 같은 방식으로 정의된 학습에의 성능지표를 “샘플 복잡도(Sample Complexity)”라고 한다.

양자컴퓨팅 연구 분야에서 지수함수적 속도향상의 가능성이 같은 방식으로 확인되었던 만큼, 머신러닝 영역에서 역시 긍정적인 결과가 기대되었으나, 아쉽게도 양자 샘플 복잡도를 실제 계산한 결과 계산과학적으로 큰 의미가 없는 아주 약간의 속도향상 정도만 확인되었다. 하지만, 특수한 목적에의 학습을 가정할 경우, 혹은 어떤 특정한 변수 가정하에서는 다항함수적 속도향상을 기대할 수 있다는 결과 또한 밝혀졌으나, 초창기 연구에서 해당 결과들은 양자머신러닝 연구에 새로운 모멘텀을 부여할 만큼 어필하지는 못하였다[9].

3. 양자 서포트벡터머신 개발

QML 연구는 2014년 양자 버전의 서포트벡터

머신(SVM: Support Vector Machine)의 개념과 양자이득 증명으로 인해 의해 새로운 전기를 맞게 되었다. SVM이란 주어진 (빅)데이터들의 분류 알고리즘 내지는 메커니즘으로서 정의되는데, 이 SVM은 매우 중요한 머신러닝 방법론들 중 하나로, 학술적 맥락에서뿐만 아니라 데이터의 분류/가공 등의 실용적 목적으로도 활용되는 매우 중요한 방법론이다. MIT의 Seth Lloyd 교수팀은 이러한 SVM의 주요 연산커널을 양자작업으로 확장하여, 이를 기반으로 한 양자-SVM을 정의하였고, 해당 연구에서 지수함수적 양자 속도향상이 가능함을 이론적으로 증명하였다.

SVM은 앞서 언급했듯이, 주어진 많은 양의 데이터들을 분류하는 방법론으로서 임의의 차원의 공간에 분포하고 있는 포인트들로서의 분류 데이터들을 “최적으로” 분류하는 초평면(Hyperplane)을 구하는 알고리즘이다(그림 3). 이 과정에서 문제는 분류범주의 최외각 데이터에 접하는 초평면들과 그들 사이의 거리(Margin)를 극대화하는 초평면을 찾는 것이다. 이러한 문제는 결국 분류범주의 결정법칙에 대응하는 제약식과 라그랑지안 승수를 곱한 항의 최적화 문제(라그랑지안 최적화 문제)로 환원된다. 이 문제를 풀기 위해서 필요한 가장 큰 계산량이 바로 데이터의 개수 N 에 대한 선형 방정식, 즉 $N \times N$ 행렬의 대각화(Diagonalization)에 집중되어 있다.

따라서, 매우 많은 양의 (빅)데이터 샘플에 대해 해당 작업을 수행하기 위해서는 엄청나게 큰 계산노력이 필요하다. Seth Lloyd 교수 연구팀은 바로 이 부분에 HHL 알고리즘을 적용하였다. 즉 첫째로, 분류에 필요한 데이터 샘플을 모두 양자상태로 “변환”하고, 이들의 “증첩”상태를 최종 준비한다. 다음으로, 풀고자 하는 행렬 A 와 관련된 유니타리를 구성한 후 “단일동작”으로서의 양자상태 변환식을 정한다. 여기에, HHL 알고리즘을 적용함으로써 양자

Decision Rule:

$$\mathbf{w} \cdot \mathbf{x}_+ + b \geq +1 \quad (y = +1 \text{ for } \mathbf{x}_+)$$

$$\mathbf{w} \cdot \mathbf{x}_- + b \leq -1 \quad (y = -1 \text{ for } \mathbf{x}_-)$$

$$\frac{2}{|\mathbf{w}|} \quad (\text{Margin})$$

Optimization Problem:

$$\mathcal{L} = \frac{1}{2} |\mathbf{w}|^2 - \sum_k \lambda_k y_k (\mathbf{w} \cdot \mathbf{x}_k + b) - 1$$

Solving Eq. $\partial \mathcal{L} = 0$

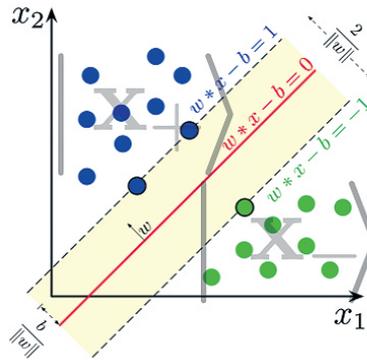


그림 3 2차원 공간에서의 SVM

Problem	Speedup (classical ⇨ quantum)	QML
HHL for linear system	$O(s\kappa N \log(1/\epsilon)) \Leftrightarrow O(s^2\kappa^2 \log(N)/\epsilon)$	Quantum SVM* Quantum Regression Kernel Least Squares
SVE	$O(k^2 N \log(1/\delta)/\epsilon) \Leftrightarrow O(\log(N)/\epsilon^3)$	Recommendation System Quantum Linear Regression Principal Component Analysis

그림 4 선형시스템 vs 알고리즘의 양자속도향상

병렬성을 극대화한 양자이득을 얻는다는 것이 아이디어다[9]. 이와 같은 접근법은 HHL 알고리즘 혹은 양자-SVE 알고리즘을 커널로 사용할 수 있는 대부분의 머신러닝 작업에의 양자이득 획득 방법론으로 일반화되었다(그림 4).

4. NISQ 컴퓨팅과 머신러닝

앞서 기술한 소인수분해, 데이터검색, HHL을 비롯한 양자머신러닝 알고리즘들은 양자우위성의 이론적 가능성을 시사하는 매우 중요한 알고리즘들로

서, 현재까지도 활발히 연구되고 있다. 하지만, 현재까지 진행된 큐비트 및 양자컴퓨팅 구현기술로는 앞서 기술한 이론적으로 증명된 “양자우위성”을 눈앞에 도출하는 것은 현재 수준의 양자 하드웨어로는 거의 불가능하다. 앞서 지수함수적 속도향상이 증명된 양자알고리즘들의 양자우위성 증명을 위해서는 최소 수억 이상의 큐비트 회로가 필요할 것으로 예상되나[10], 지금까지 구현/연산 가능한 큐비트의 최고 개수는 알려진 결과들에 비추어 대략 몇백 정도이고 그나마도 온전하게 동작한다고 보기 어렵다. 이에 최근까지 대규모 큐비트가 필요한 소인

Google's quantum supremacy proof

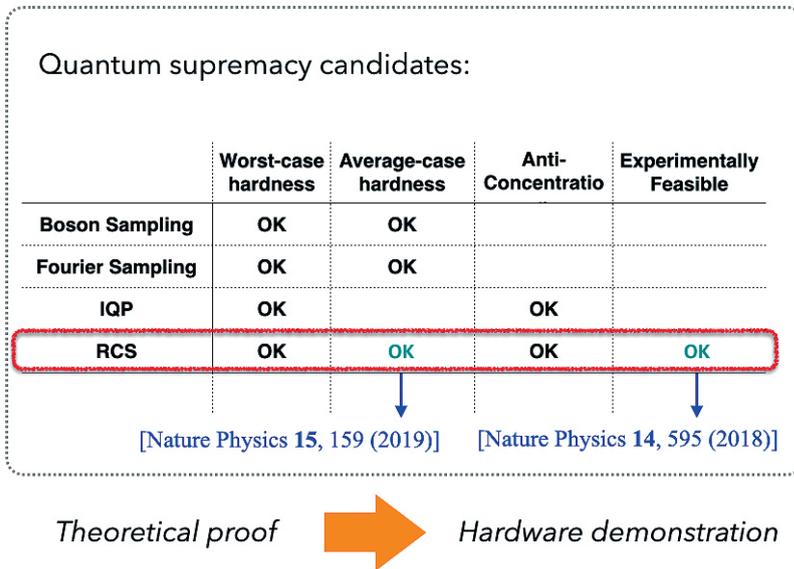


그림 5 양자우월성 증명을 위한 후보문제들

수분해 등의 작업을 배제하고, 오류가 있는(Noisy), 중간 규모의(Intermediate-Scale) 의미 있는 양자기술(Quantum)로 구현 가능한 수준의 새로운 문제/방법론 등을 구성하는 데 좀 더 집중적인 연구를 해 보자는 일종의 연구방향성이 생겨났다—이를 “NISQ”라고 한다[4].

최근까지의 성공적인 NISQ 연구 제안들은 대부분 표본추출문제 혹은 샘플링 문제이다. 이와 같은 문제 구성에 있어서의 관점의 변화는 표준적인 컴퓨팅에서의 기능 최적화 개념보다 출력물을 샘플링할 수 있는 확률 분포에 좀 더 집중해 보고자 하는 아이디어에서 출발한다. 실제로, 양자컴퓨터의 원시 출력값들은 대부분 양자측정에 따른 확률분포 표본이기 때문에 이 같은 아이디어는 매우 성공적이었다. 특히, “보존 샘플링(Boson Sampling)” 등에서 매우 성공적인 사례들을 도출하였다. 하지만, 보존 샘플링의 구현은 광자 생성기 혹은 측정기의 낮은

효율 등으로, 양자우월성의 직접관측이 가능한 정도의 실험규모가 되기에는 다소 어려움이 있었다.

양자우월성의 실험증명의 핵심은 결과적으로 고품질의 큐비트를 구축하는 데 있다. 이에 최근 극적인 실험적 진보를 이룩한 Google 그룹은 본인들이 구축한 양자 프로세서—“Sycamore Processor”라고 명명하였음—맥락과 일치하는 자연 샘플링 문제를 구성하였다. 이를 “무작위 회로 샘플링(RCS: Random Circuit Sampling)”이라고 부른다. 해당 문제는 기본 양자연산들을 무작위로 선택하는 특정 형태의(예를 들어, 어떤 효율적 양자 알고리즘을 구성하는) 양자회로를 취하여 출력분포의 샘플을 생성하는 알고리즘이다. 이전의 대부분의 양자컴퓨팅/시뮬레이션 방법론 등이 양자잡음에 의해 너무 쉽게 파괴되는 양자중첩의 분포 때문에 구현이 힘들었던 반면, RCS는 큐비트들 간의 일반적인 형태의 상호작용 패턴을 재현 가능하도록 재구성되었다. 매우 최근까

지만 해도 이와 같은 패턴의 출력분포가 기존 컴퓨팅에서는 매우 얻기 힘들다는 이론적 검증과정이 존재하지 않았다. 하지만, 2018년 이론적 검증 연구를 통해 RCS가 주어진 실험적 오류에 대하여, 의미 있는 양자이득이 가능하다는 것이 명확하게 증명되었다(그림 5)[11,12]. 따라서, RCS는 NISQ기반의 양자우위성 증명의 매우 중요한 후보가 되었고, 곧바로 Google 연구팀은 이를 실험으로 증명하였다[13]. 이것이 유명한 Google의 양자우월성 증명 시나리오이다.

III. 결론

다소 극단적인 분위기에서 과도하게 가속화된 양자컴퓨팅 연구는 이제 양자이득 증명과 단기활용이라는 현실적 목표설정 단계에 있다. 따라서, 양자컴퓨팅 및 양자머신러닝 연구는 구체적이고 적용 가능한 문제 내에서 양자 성능향상을 보여주는 형태로 진행될 것으로 예상된다. 따라서, 이미 현시점에서 “양자컴퓨팅/머신러닝 연구” 등과 같은 과도하게 포괄적이고 추상적인 개념과 일반적인 가치비전만으로는 선구적인 연구 콘텐츠를 생산하는 것은 불가능하다.

이러한 맥락에서, 현재 양자컴퓨팅 연구 전반의 관심은 가능한 한 실험 규모에 적합한 새로운 문제/방법론을 구축하는 데 집중되고 있다. 물론, 고품질의 큐비트 구현/조작 기술을 확보하는 것이 양자 기술 전반의 핵심이기는 하지만, 앞서도 언급했듯이 이러한 너무나 일반적이고 추상적인 비전은 이제 더 이상 양자컴퓨팅/머신러닝 연구에의 콘텐츠를 제시하는 틀이 되지 못한다. 따라서 양자 기술의 미래는 NISQ 혹은 그 이후 시대의 아젠다를 정확히 이해하고, 그 안에서 적절한 문제들을 발굴하는 것과 올바른 개념을 정립하는 것으로 시작될 것이다.

이에 당분간은 양자이론 및 양자소프트웨어 연구의 비중이 크게 높아질 전망이며, 하드웨어 구현과 이론연구 사이의 조화가 양자컴퓨팅/머신러닝 연구에서는 특히 더욱 중요해질 전망이다.

용어해설

양자병렬성(Quantum Parallelism) 양자중첩 성질을 활용하여 다수의 입력신호에 대한 다수의 출력신호를 특징하는 형태의 병렬성

양자결잃림(Decoherence) 주어진 양자상태가 양자성(중첩 혹은 얽힘)을 잃고 고전 통계적 상태로 변하는 양자잡음 프로세스

보존샘플링(Boson Sampling) 보존입자(예: 광자)들의 이산상태의 무작위성을 활용하여 복잡한 계산을 수행하고자 하는 목적으로 구성된 양자컴퓨팅의 대표적 응용문제들 중 하나

약어 정리

NISQ	Noisy Intermediate-Scale Quantum
QML	Quantum Machine Learning
RCS	Random Circuit Sampling
SVM	Support Vector Machine

참고문헌

- [1] N.D. Mermin, Quantum Computer Science: An Introduction, Cambridge University Press, Cambridge, UK, 2007.
- [2] P.W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Proc. Annu. Symp. Found. Comput. Sci., (Santa Fe, NM, USA), Nov. 1994.
- [3] L.K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," Phys. Rev. Lett., vol. 79, no. 2, 1997, article no. 325.
- [4] J. Preskill, "Quantum computing in the NISQ era and beyond," Quantum, vol. 2, 2018, p. 79.
- [5] S. McArdle et al., "Quantum computational chemistry," Rev. Mod. Phys., vol. 92, no. 1, 2020, article no. 015003.
- [6] J. Biamonte et al., "Quantum machine learning," Nature, vol. 549, no. 7671, 2017, pp. 195-202.
- [7] A.W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for linear systems of equations," Phys. Rev. Lett., vol. 103, no. 15, 2009, article no. 150502.
- [8] P. Rebentrost, M. Mohseni, and S. Lloyd, "Quantum support vector machine for big data classification,"

- Phys. Rev. Lett., vol. 113, no. 13, 2014, article no. 130503.
- [9] C. Ciliberto et al., "Quantum machine learning: A classical perspective," Proc. Royal Soc. A: Math. Phys. Eng. Sci., vol. 474, no. 2209, 2018.
- [10] T. Monzet et al., "Realization of a scalable Shor algorithm," Science, vol. 351, no. 6277, 2016, pp. 1068–1070.
- [11] A. Bouland et al., "On the complexity and verification of quantum random circuit sampling," Nat. Phys., vol. 15, no. 2, 2019, pp. 159–163.
- [12] S. Boixo et al., "Characterizing quantum supremacy in near-term devices," Nat. Phys., vol. 14, no. 6, 2018, pp. 595–600.
- [13] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, no. 7779, 2019, pp. 505–510.