양자컴퓨터와 양자머신러닝

서론

양자정보과학의 대표적인 응용 분야는 크게 세가지, 센싱, 통신, 컴퓨팅으로 분류할 수 있는데, 이 세 가지 모두 '데이터'와 밀접한 관련이 있다. 센싱은 데이터를 수집하는 과정이고, 통신은 데이터를 주고받는 과정이며 컴퓨팅은 일련의 연산 과정을 통해 데이터로 부터 유의미한 결과값을 얻어내는 과정이기 때문이다. 양자정보과학 기술은 이러한 과정들의 정확도, 효율성, 보안성 등을 현재의 기술의 한계점 이상으로 개선하는 것을 목표로 한다. 필자의 연구팀은 양자컴퓨팅, 그 중에서도 양자머신러닝 알고리즘을 개발하는 연구를 수행하고 있다. 양자머신러닝에는 크게 두 가지 연구 주제가 있는데, 첫째는 머신러닝을 위한 양자컴퓨팅, 둘째는 양자컴퓨팅을 위한 머신러닝이라고 할 수 있겠다. 첫번째 주제는 빅데이터, 머신러닝, 인공지능 분야가 직면한 다양한 문제들을 해결하기 위한 양자컴퓨팅 알고리즘을 연구 하는 것이고, 두번째 주제는 양자컴퓨터의 오류 및 결함을 통계적 분석 및 머신러닝으로 보완하는 방법을 개발하는 연구이다. 본 글에서는 첫번째 주제에 집중하도록 하겠다.

컴퓨팅과 물리학은 불가분의 관계이다. 왜냐하면 정보를 처리하여 유의미한 지식을 추출해내기 위해서는 먼저 정보가 물리적 장치에 저장이 되어 있어야 하고, 물리적 법칙에 의해 처리되어야 하기 때문이다. 즉 어떠한 컴퓨터 장치의 성능은 해당 장치가 따르는 물리 법칙에 의해 결정되게 되어있다. 따라서 고전물리학보다 더 정확한 이론으로 알려진 양자물리학의 법칙을 따르는 컴퓨터를 만든다는 것은 자연스러운 시도로 볼 수 있다. 지난 30 여년간 수많은 학자들의 노력으로 고전알고리즘들을 뛰어넘는 양자알고리즘들이 개발되어 왔으며 이론적 근거를 바탕으로 해외 대기업들도 양자기술에 뛰어들며 양자알고리즘의 상용화가 빠른 속도로 가시화 되고 있다.

양자알고리즘 시대의 개막

양자알고리즘의 탄생은 1980 년대로 거슬러 올라간다. 당시 몇몇 학자들은 자연은 양자역학을 따르므로, 자연계의 문제들을 풀기 위해서는 양자역학적 원리로 작동하는 양자컴퓨터가 필요하다고 생각하게 된다. 자연계의 문제를 푸는 것 매우 중요한 일인데, 현대 산업계가 직면한 수많은 난제들은 디지털 컴퓨터와 같이 고전 역학을 따르는 컴퓨팅 모델로 복잡한 자연계를 모사하는 것이 상당히 어렵기 때문에 발생된다. 예시로는 신약 개발, 신소재 개발, 단백질 구조 계산, 효율적 비료 생산, 차세대 배터리 개발 등이 있다. 아마도 양자역학 문제는 양자컴퓨터가 더 잘 풀 수 있다는 주장은 그리 불편하지 않게 받아들일 수 있을 것이다. 그런데 1990 년대 초부터 양자알고리즘이 양자역학과는 전혀 상관없는 몇몇 특정한 문제들을 고전알고리즘보다 지수함수[1]적으로 빠르게 풀 수 있다는 놀라운 사실이 발견되었다. 이러한 발견은 계산복잡도 이론의 테두리 안에서 양자컴퓨터와 고전컴퓨터는 근본적으로 다르다는 것과 특정 문제 해결에 대한 양자컴퓨터의 우위를 이론적으로 증명하여 학술적 가치는 높았지만 상업적 가치의 부재와 실제 구현의 어려움 등의 문제가 남아있었다.

1994 년 피터 쇼어는 소인수분해 문제를 기존에 알려진 고전알고리즘 대비 지수함수적으로 빠르게 해결하는 양자알고리즘을 개발하였다. 이 문제를 해결하면 널리 쓰이고 있는 RSA 암호 체계가 위협을 받으므로, 양자컴퓨터는 큰 관심을 받게 된다. 그러나 당시 일부 학자들은 오류 정정을 수행할 수 없다는 이유로 양자알고리즘의 구현이 불가능하다는 부정적인 반응을 보였다. 하지만 피터 쇼어는 다음 해 양자오류정정코드를 개발하여 양자컴퓨팅이 근본적으로 가능함을 입증하게 된다. 이에 힘입어 양자컴퓨팅 분야는 급격하게 발전하기 시작한다. 이 후 비정형화된 문제의 정답을 찾는 양자 검색 알고리즘, 양자푸리에변환, 고유값 분해 알고리즘, 선형연립방정식 풀이 알고리즘 등

---

[1] 알고리즘 A 가 알고리즘 B 보다 지수함수적으로 빠르다는 것은, n이라는 크기를 가지는 입력값에 대해 어떠한 문제를 풀기 위해 알고리즘 B 가 $T(n)$의 연산 시간을 필요로 한다면 알고리즘 A 는 $\log(T(n))$의 연산 시간을 필요로 한다는 것을 뜻한다.

고전알고리즘 대비 이차항[2](quadratic) 또는 지수함수적 속도향상이 가능한 다양한 양자알고리즘들이 개발되었다. 중요한 점은, 양자컴퓨팅 시대의 개막과 함께 개발된 모든 양자알고리즘들은 문제 해결 과정에서 특정 부분에만 적용되는 것이며, 데이터 전처리나 후처리 과정에서는 여전히 고전컴퓨터가 필요하다는 것이다. 따라서 양자컴퓨터는 고전컴퓨터를 완전히 대체해 버리는 것이 아니며, 기존의 고전컴퓨터와 협력하는 이기종 형태로 사용된다. 고전컴퓨터가 잘하는 것은 고전컴퓨터로 하고, 양자컴퓨터가 잘하는 것은 양자컴퓨터로 하는 것이다.

"양자역학을 이해했다고 생각한다면 양자역학을 이해하지 못한 것이다"라는 말이 있을 만큼, 양자역학은 어렵다고 알려져 있다. 하지만 양자정보과학에서 필요한 대부분의 양자역학적 계산들은 복소해석학과 선형대수학만 알면 어느 정도 되기 때문에 꽤 쉽다. 다만 그 결과를 해석하는 것이 어려운 것이다. 양자컴퓨터에서는 0 이면서 동시에 1 일 수도 있는 양자역학적 비트인 큐비트를 정보의 단위로 하여 연산을 수행한다. 0 이기도 하고 1 이기도 하다는 것을 어떻게 해석해야 할지는 어렵지만, 이것을 수학으로 표현하면 단순히 2 차원의 복소 벡터(complex vector)이다.

양자역학의 법칙을 따라 연산을 수행하는 양자컴퓨터의 수학적 모델은 선형대수를 통해 이해할 수 있는데, 흥미롭게도 양자컴퓨터는 특정 선형대수 문제들을 아주 빠르게 풀 수 있다. 예를 들어 2009 년도에 발표된 양자 선형연립방정식 풀이 알고리즘(저자들의 이니셜을 따와 HHL 알고리즘이라고도 한다)은 역행렬을 구하는 문제를 기존 알고리즘 대비 지수함수적으로 빠르게 풀 수 있다. 역행렬을 구하는 것은 회귀분석, 최소제곱 서포트 벡터 머신(least-squares support vector machine 또는 LS-SVM)등 다양한 데이터 기반 예측 문제에서 필요한데, 고전알고리즘은 여기에 많은 계산 비용을 소모하게 된다. 반면 양자컴퓨터는 이 문제를 지수함수적으로 빠르게 풀 수 있다. 이러한 놀라운 사실을 바탕으로 양자머신러닝이라는 분야가 탄생하게 되며, 실제로 회귀분석과 서포트 벡터 머신(SVM)을 지수함수적으로 빠르게 해결하는 양자머신러닝 알고리즘들이 등장하게 된다. 사실 HHL 알고리즘은 양자고유값 분해 알고리즘을 기반으로 하는데, 주어진 행렬을 대각화하면 역행렬도 쉽게 구할 수 있기 때문이다. 이 양자고유값 분해 알고리즘을 바탕으로 비지도학습의 대표적 예시 중 하나인 데이터 차원축소를 위한 양자 주성분분석(PCA) 알고리즘도 등장한다. HHL 알고리즘과 마찬가지로 여기서도 양자컴퓨터는 고유값 분해 문제를 고전알고리즘 대비 지수함수적으로 빠르게 풀어준다. 양자머신러닝에는 고전알고리즘 대비 지수함수적인 속도향상이 보장된 HHL 기반 회귀분석, 양자 서포트 벡터 머신, 양자 주성분분석 알고리즘 뿐 아니라, 고전알고리즘 대비 이차항적(quadratic) 속도향상이 보장된 알고리즘도 있다. 이는 양자 검색 알고리즘과 고유값 분해 알고리즘이 사용되는 양자 진폭 추정 알고리즘을 통해 모수를 추정하는 알고리즘이다. 이러한 예시들만 보아도 이미 충분히 고전머신러닝의 한계를 뛰어넘는 양자머신러닝의 시대가 열린 것 같다. 하지만 앞서 언급한 양자머신러닝 알고리즘들의 속도 향상은 어디까지나 이론적인 이야기이고, 현실에는 많은 어려움이 있다.

고전 데이터 **vs** 양자 데이터

앞서 언급한 양자머신러닝 알고리즘들은 공통적인 전제조건이 필요한데, 이는 분석의 대상이 되는 데이터가 양자 상태로 주어져야한다는 것이다. 지수함수적, 또는 이차항적 속도향상은 고전 데이터가 양자 데이터로 변환이 된 후에야 이루어진다. 그런데 고전 데이터를 양자 데이터로 바꾸는 과정 자체에 큰 계산 비용이 들어가며, 여기서 모든 양자적 속도 향상이 사라지게 된다. 즉 고전 데이터에 양자알고리즘을 적용하는 것은 일반적으로 매우 부자연스러운 시도이며 반드시 이에 대한 비용을 치러야한다. 특히 빅데이터와 같이 고차원, 대용량의 고전 데이터를 양자컴퓨터로 처리하려면 데이터 변환 과정에서의 비용이 매우 비싸다. 반대로 양자 데이터, 즉 양자 상태를 고전컴퓨터로 분석하는 것도 비용이 매우 비싸다. 예를 들어 N 개의 큐비트로 이루어진 양자장치가 출력하는 양자 상태를 표현하는 밀도 행렬은 최대 4^N-1 개의 실수 변수를 가지기 때문에, 해당 양자 상태에 대한 사전 지식이 없다면 밀도 행렬의 변수들을 추정하기 위한 측정 횟수는 큐비트 개수 대비 지수함수적으로 증가한다. 즉 일단 양자 상태를 고전 데이터로 바꾸는 과정 자체가 매우 비싸다. 따라서 양자 데이터를 분석해야 하는 문제는 양자 컴퓨터가 고전 컴퓨터보다 훨씬 빠르게 풀 것이라고 받아들여지고 있다. 어쩌면 양자 센싱 분야가 발전하면 양자 데이터가 증가하여

[2] 이차항적 속도 향상은 $T(n)$의 연산 시간을 $\sqrt(T(n))$로 줄일 수 있음을 의미한다.

자연스럽게 양자머신러닝도 함께 발전할 수 있겠다. 이는 고전 머신러닝 분야가 빅데이터 시대가 열리면서 급격한 발전을 경험한 것과 마찬가지일 것이다. 요약하자면 고전 데이터는 고전 머신러닝으로, 양자 데이터는 양자 머신러닝으로 분석하는 것이 적어도 속도측면에서는 바람직한 접근법이다. 하지만 머신러닝에서는 항상 속도만이 중요한 것은 아니다. 아무리 계산(또는 학습)을 오래해도 성능이 개선되지 않는 문제들이 있다. 따라서 고전 데이터에 양자 머신러닝 알고리즘을 적용하는 시도는, 만약 성능이 개선 될 수 있다면, 충분히 의미 있는 접근이 될 수 있다.

이론과 현실

만약 데이터가 양자 상태로 주어진다고 해도 앞서 언급한 양자머신러닝 알고리즘들은 여전히 극복해야할 문제가 있다. 이는 양자 회로의 깊이 및 게이트 연산 비용이 큐비트 개수 대비 다항적(polynomially)으로 증가한다는 것인데, 이러한 양자 회로를 높은 신뢰도로 구현하기 위해서는 양자오류정정 및 결함허용[3] 양자컴퓨팅이 필요하다. 양자오류정정 및 결함허용 양자컴퓨팅의 탄탄한 이론은 양자컴퓨터의 범용성과 확장성을 보장해 주기는 하지만, 이를 실제로 구현하는 양자컴퓨터 하드웨어 개발은 매우 어려운 숙제로 남아 있다. 근본적으로는 문제가 없어 보이지만 양자컴퓨터는 반도체 기반의 디지털 컴퓨터보다 훨씬 만들기 어려우며 기술력이 언제 이론을 따라잡을지는 예측하기가 매우 어렵다. 이러한 배경에서 현재 양자컴퓨팅 연구의 방향성은 크게 두 갈래로 나뉘게 되는데 첫째는 양자오류정정 이론을 기반으로 확장성과 범용성을 모두 구비한 양자컴퓨팅 시스템을 개발하는 것이며 둘째는 가까운 미래에 상용화가 가능한 제한된 양자 하드웨어를 이용하여 양자 이득[4]을 달성할 수 있는 양자컴퓨팅 응용 알고리즘을 개발하는 것이다. 이 제한적 양자 하드웨어를 Noisy Intermediate-scale Quantum(NISQ)[5] 컴퓨터라고도 부른다. 말 그대로 결함은 있지만, 큐비트의 개수가 고전컴퓨터로는 모사하기 어려울 정도의 중규모 수준인 양자컴퓨터라는 뜻이다. 양자오류정정을 하지 않고도 유의미한 계산 결과를 얻어내려면 양자 회로의 깊이가 얕아야 하는데, 보통 양자 회로의 깊이가 큐비트 개수 대비 대수적(logarithmic)으로 증가하거나 또는 큐비트 개수에 따라 증가하지 않는 상수여야 한다. NISQ 컴퓨터에서 구현 가능하고, 고전 알고리즘 대비 증명 가능한 양자 이득을 달성할 수 있는 상업적 문제는 아직 알려져 있지 않다.

가까운 미래의 양자머신러닝

NISQ 컴퓨터로 머신러닝 분야에서 실용적이며 고전 알고리즘 대비 증명 가능한 양자 이득을 달성할 수 있을지는 아직 모르지만, 그럼에도 불구하고 NISQ 컴퓨팅 기반의 머신러닝 알고리즘들이 계속해서 새롭게 개발 되고 있다. NISQ 컴퓨터로 접근할 수 있는 머신러닝 문제들은 크게 세 가지로 분류될 수 있는데, 첫째는 커널 기반 머신러닝이다. 머신러닝에서 커널을 계산하는 것은 데이터를 고차원으로 매핑한 후 데이터 간의 내적을 계산하는 것과 동일한 효과를 갖기 때문에 비선형적 데이터 분석에 매우 유용한 것으로 알려져 있다. 재미있는 것은 양자컴퓨터가 출력하는 결과 값은 커널 함수 값으로 나타낼 수 있다. 따라서 양자알고리즘을 잘 디자인 하여 고전컴퓨터가 계산하기 어려운 커널 함수를 만들어 계산할 수 있다. 물론 계산하기 어려운 커널이 과연 실제 데이터 분석에 있어서 얼마나 유용한지는 불명확하지만, 양자컴퓨터가 커널 기법과 자연스럽게 연결되는 것은 매우 흥미로우며 앞으로 활용도가 기대된다. 두번째는 연속 최적화이다. 양자컴퓨터는 특정한 함수 값을 계산하는 것 뿐 아니라 이에 대한 기울기(gradient)도 쉽게 계산할 수 있다. 이러한 특징을 활용하면 모든 경사하강법(gradient descent) 기반의 최적화 문제에 양자컴퓨터를 사용할 수 있다. 또한, 앞서 언급한 커널 기법과 연계하여 데이터에 맞게 커널을 최적화 하는 일도 해볼 수 있다. 머신 러닝 분야에서도 경사하강법을 사용하는 모든 알고리즘에 양자컴퓨팅 기술을 도입해 볼 수 있다. 필자의 연구실에서는 이를 기반으로 양자 합성곱 신경망(Convolutional Neural Network), 양자 오토인코더,

[3] https://horizon.kias.re.kr/15547/

[4] 본 글에서 양자 이득이란 성능, 속도 등 하나 또는 그 이상의 지표에서 양자 컴퓨터가 고전 컴퓨터에 비해 이점을 제공하는 것을 의미한다.

[5] NISQ 를 한글로 번역하자면, 노이즈가 있는 중간 규모의 양자컴퓨터라고 할 수 있겠다. NISQ 에 대한 자세한 내용은 다음 링크에 잘 설명이 되어있다: https://horizon.kias.re.kr/16769/.

양자 서포트 벡터 데이터 묘사(Support Vector Data Description), 고전-양자 하이브리드 딥러닝 등 다양한 알고리즘을 개발하고 있다. 이때 학습 효율성 향상, 메모리 비용 절감, 일반화 오차(generalization error) 감소 등의 효과를 기대해 볼 수 있다. 마지막으로 조합 최적화에도 양자알고리즘을 적용할 수 있다. N 개의 큐비트로 이루어진 양자컴퓨터는 N 비트로 표현 가능한 2 의 N 제곱 가지수의 모든 비트 스트링들을 양자 중첩 상태로 동시에 처리할 수 있는데, 연산 이 후에는 이 중 하나의 비트 스트링만 확률적으로 출력한다. 이러한 성질을 잘 활용하면, 양자컴퓨터는 N 차원 변수의 조합 최적화 문제에서 모든 가능한 경우의 수를 동시에 담고 있는 상태로부터 출발하여 최적값이 가장 높은 확률로 뽑히도록 상태를 바꿀 수 있고, 이를 통해 최적화 문제를 풀 수 있다. 조합 최적화에는 외판원 순회 문제(travelling salesman problem), 그래프 max k-cut 문제 등 NP-hard 문제들이 많은데, 안타깝게도 양자컴퓨터가 이러한 조합 최적화 문제들을 다항 시간 안에 풀 수 있지는 않아 보인다. 일반적으로 전역 최적해를 찾기 위해서는 실행 시간이 큐비트 개수 대비 지수함수적으로 증가하기 때문이다. 한편 어려운 조합 최적화 문제들의 국소 최적해를 다항 시간 안에 찾는 무작위 알고리즘들 대비 양자 알고리즘이 이점이 있을 수도 있지만, 이에 대해서는 더 연구가 필요하다. 필자의 연구실에서는 비지도 학습 데이터 클러스터링 문제를 조합 최적화 문제로 해석하여 양자컴퓨터로 해결하는 알고리즘 개발 연구도 진행 중이다.

맺는말

양자컴퓨팅 기술은 기존 기술의 연장선상에서 컴퓨터의 성능을 향상시키는 것이 아니라, 전통적인 방식과는 완전히 다른 양자역학의 원리를 활용하여 연산을 수행하는 새로운 개념의 컴퓨팅 기술이다. 양자머신러닝은 이러한 양자컴퓨터를 활용하여 기존 머신러닝 기술의 한계를 극복하고자 도전하는 새로운 학문이다. 그러나 양자컴퓨터 하드웨어는 엄청난 기술적 난이도를 요구하기 때문에 아직은 실용적이지 않다. 하지만 양자컴퓨터의 성능과 안정성은 지속적으로, 그리고 빠르게 발전하고 있다. 가까운 미래에 수십 개의 큐비트를 안정적으로 제어할 수 있는 양자컴퓨터 하드웨어가 상용화 되면, 커널 기법, 연속 최적화, 조합 최적화를 사용하는 다양한 머신러닝과 데이터 분석 문제에 양자머신러닝을 적용해 볼 수 있을 것이다. 만약 양자오류정정 및 결함허용양자컴퓨팅이 가능하고, 고전 데이터를 양자 데이터로 변환하는 효율적인 방법을 발견하게 된다면, 다양한 머신러닝 문제에서 지수함수적 또는 이차항적 속도 향상을 달성할 수도 있을 것이다. 또한 양자컴퓨터 하드웨어의 발전을 위해서, 그리고 NISQ 컴퓨터 활용의 극대화를 위해서는 양자컴퓨터가 만들어 내는 잡음이 섞인 데이터로부터 유의미한 정보를 얻어내는 것이 매우 중요하다. 따라서 고급 머신러닝 및 데이터 분석 기법들이 양자컴퓨팅 기술 발전에 기여할 수 있을 것이다. 양자머신러닝은 수학, 물리학, 컴퓨터과학, 통계학 등 다양한 학문간의 융합적 연구가 매우 중요다. 다양한 연구자들 간의 활발한 교류와 협업은 분명 양자 데이터사이언스 시대를 앞당길 수 있을 것이다. 또한 현재 빅데이터라고 하면 방대한 양의 고전데이터를 의미하지만, 언젠가 양자 빅데이터의 시대가 열린다면 분명 양자 머신러닝에 대한 수요도 증가할 것이며 양자머신러닝은 현재는 상상할 수 없을 정도로 급격한 발전을 경험하게 될 지도 모르겠다.