

양자컴퓨팅을 이용한 양자 인공지능 기술 동향

김 현 지*, 임 세 진*, 김 덕 영*, 서 화 정**

요 약

최근 양자 역학의 원리를 기반으로 하는 양자 컴퓨팅 기술이 발달하면서 양자 컴퓨터가 고전컴퓨터에 비해 이점을 가질 수 있는 작업 중 하나인 양자 인공지능에 대한 연구들이 관심을 받고 있다. 최근에는 실제로 작은 규모의 문제에서는 양자 인공지능이 기존 인공지능 기술에 비해 이점을 얻을 수 있음이 여러 연구 사례들을 통해 확인되었다. 하지만 현재의 양자 컴퓨터는 많은 자원을 사용할 수 없는 오류가 있는 중간 규모의 양자 컴퓨터 (Noisy Intermediate-Scale Quantum, NISQ) 이므로 아직까지는 고전 인공지능을 능가한다고 정의하기는 어렵다. 따라서 현재의 양자 인공지능 기술은 고전 컴퓨팅과 양자 컴퓨팅을 결합한 하이브리드 방식이 보다 활발히 사용되고 있는 상황이며, 제약적인 환경에서 동작하는 신경망 구조와 학습 기술들이 주가 되고 있다. 본 고에서는 NISQ 상에서의 양자 인공지능 기술들에 대해 자세히 알아본다.

I. 서 론

양자 컴퓨팅은 양자 역학의 원리를 활용하여 기존 컴퓨터로 수행하기 어려웠던 난제를 해결하는 기술이다. 양자 컴퓨터에서는 0과 1의 상태를 동시에 가지는 큐비트를 기본 연산단위로 사용하기 때문에 큰 규모의 경우의 수를 탐색하면서 연산하고 비교하는 작업에서 강점을 가진다. 이러한 작업의 대표적인 예로 암호분야에 있어 큰 이슈로 다가오고 있는 소인수분해 그리고 대규모 데이터 셋을 기반으로 하는 인공지능 학습이 있다. 기존에 높은 연산 부하와 메모리 사용량 한계가 있던 대규모 인공지능 학습에서 이점을 얻고자 양자 컴퓨팅 기술을 기반으로 하는 양자 인공지능이 활발히 연구되고 있다. 본 고에서는 양자컴퓨팅을 활용한 양자 인공지능 기술에 대해 확인해 보도록 한다.

II. 관련 연구

2.1. 양자 컴퓨터

2.1.1. 개발 현황

IBM, Google 등 세계적인 IT 기업들은 양자 컴퓨팅 분야에 큰 관심을 가지고 투자하고 있다. 양자 컴퓨터 구축을 위해 가장 활발히 기술 개발을 수행하고 있는 IBM은 [표 1]의 개발 로드맵[1]을 따라 매년 양자 프로세서를 발표하고 있으며, 최근 2022년 11월에는 433 큐비트의 양자 컴퓨터 Osprey를 공개하였다[2]. 지난 몇 년 간 하나의 칩에서 지원할 수 있는 큐비트의 수를 늘리는 것에 집중했다면, 올해 선보일 프로세서 중 하나인 Heron부터는 지원하는 큐비트 수가 크게 줄어들었지만 고품질의 큐비트를 가지며, 각각의 칩을 다른 Heron 프로세서에 직접 연결하는 기술도 적용된다. 이는 IBM이 큐비트 수 규모를 확장하기 위해 기존의 단일 칩 프로세서를 넘어서서 다수의 프로세서가 연결된 모듈형 양자 컴퓨터로 개발 방향을 전환한다는 것을 의미한다. 또한, IBM은 실행 가능한 회

본 연구는 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (<Q|Crypton>, No.2019-0-00033, 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발, 50%) 그리고 본 연구는 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구, 50%).

* 한성대학교 IT융합공학과 (대학원생, khj1594012@gmail.com, dlatpws834@gmail.com, dudejrdl123@gmail.com)

** 한성대학교 융합보안학과 (부교수, hwajcong84@gmail.com)

[표 1] IBM 양자 컴퓨터 개발 로드맵

Year	Processor	Qubit
2019	Falcon	27
2020	Humming bird	65
2021	Eagle	127
2022	Osprey	433
2023	Condor	1,121
	Heron	133
2024	Flamingo	1,386+
	Crossbill	408
2025	Kookaburra	4,158+
2026	-	10K ~ 100K

로의 깊이를 늘려가는 것을 목표로 하고 있다. 이처럼 지금까지는 양자 프로세서가 지원하는 큐비트의 수를 강조하는 추세였지만 앞으로는 단순히 큐비트 수를 확장하는 것이 아니라 양자 컴퓨터가 실질적으로 활용될 수 있도록 하기 위한 요소들에 초점을 맞추어 개발이 진행되고 있다.

이러한 양자 컴퓨터의 개발과 더불어 세계적인 IT 기업들에서는 양자 컴퓨팅을 위한 플랫폼들을 개발하고 있다. 대표적인 플랫폼으로는 IBM Qiskit, Amazon Braket, Microsoft Q#, Google Cirq, Xanadu PennyLane이 있다. 해당 플랫폼들에서는 시뮬레이터 및 하드웨어를 제공하고, 화학 시뮬레이션, 양자 인공지능 등과 같이 양자 컴퓨터가 해결할 수 있을 것으로 기대되는 분야들에 대한 다양한 라이브러리를 활발히 개발하고 있다.

[표 2] 대표적인 양자 게이트에 대한 연산 내용

Gate	Matrix	Operation
X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$X 0\rangle = 1\rangle$ $X 1\rangle = 0\rangle$
H	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$H 0\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$ $H 1\rangle = \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$
$R_x(\theta)$	$\begin{pmatrix} \cos(\frac{\theta}{2}) & -i \cdot \sin(\frac{\theta}{2}) \\ -i \cdot \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$	$R_x(\theta) 0\rangle = \cos\frac{\theta}{2} 0\rangle - i \cdot \sin\frac{\theta}{2} 1\rangle$ $R_x(\theta) 1\rangle = -i \cdot \sin\frac{\theta}{2} 0\rangle + \cos\frac{\theta}{2} 1\rangle$
$R_y(\theta)$	$\begin{pmatrix} \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$	$R_y(\theta) 0\rangle = \cos\frac{\theta}{2} 0\rangle + \sin\frac{\theta}{2} 1\rangle$ $R_y(\theta) 1\rangle = -\sin\frac{\theta}{2} 0\rangle + \cos\frac{\theta}{2} 1\rangle$

그러나 이러한 노력들에도 불구하고 현재의 양자 컴퓨터는 오류가 있는 중간 규모의 양자 컴퓨터(Noisy Intermediate-Scale Quantum, NISQ)이기 때문에 실제로는 대규모 양자 계산이 불가능하며, 고전 컴퓨터의 성능을 뛰어넘는 양자 이점을 달성하기 쉽지 않다. 이로 인해 고전과 양자 컴퓨터를 함께 활용하는 하이브리드 방식이 많이 사용되고 있으며, 이는 앞서 언급한 PennyLane은 하이브리드 양자 컴퓨팅을 위한 플랫폼이다.

2.1.2. 양자 컴퓨팅 기술

양자 컴퓨터를 활용한 프로그램을 개발하기 위해서는 양자회로를 설계해야하며, 양자회로는 큐비트와 양자 게이트로 구성된다.

큐비트는 고전 컴퓨터의 비트와 같이 양자 컴퓨터에서의 연산의 기본 단위이며, 양자 현상인 중첩과 얽힘 성질을 가진다. 중첩 성질로 인해, 고전 비트가 0과 1의 값 중 하나만을 표현할 수 있는 것과 달리 큐비트는 큐비트의 구면(블로흐 구면) 위의 값을 표현할 수 있으므로 0과 1의 상태를 확률로써 가질 수 있다. 이러한 중첩 성질로 인해 n 개의 큐비트로 2^n 개의 값을 동시에 표현할 수 있게 된다. 또한, 여러 큐비트들 간의 얽힘 관계를 통해 어떤 큐비트의 상태가 다른 큐비트의 상태에도 영향을 줄 수 있게 된다. 이와 같은 양자적 특성으로 인해 모든 경우의 수에 대해 동시에 연산이 가능해지고, 고전 컴퓨터에 비해 매우 빠른 연산 속도를 얻을 수 있다는 이점이 있다.

양자 게이트는 큐비트의 상태를 변경하고 제어할 수 있으며 고전 컴퓨터의 논리 게이트와 유사한 역할을 한다. 양자 게이트는 행렬 형태로 표현할 수 있으며, 큐비트의 상태 벡터와의 행렬 곱을 통해 큐비트의 상태를 변경한다. [표 2]는 양자 게이트의 일부이며, 각 게이트가 수행하는 연산을 보여준다. X 게이트는 단일 큐비트에 대해 상태를 반전시키는 연산을 수행한다. 상태가 1인 큐비트에 적용하면 0이 되고, 상태가 0인 큐비트에 적용하면 큐비트의 상태가 1로 변경된다. H 게이트는 Hadamard 게이트이며, 대상 큐비트가 0과 1의 상태를 동일한 확률로 가지는 중첩 상태로 변환한다. 회전 게이트 (R_x, R_y)의 경우 매개변수 (θ)를 가진다. 해당 매개변수를 회전각으로 사용하여 x 축 또는 y 축을 기저로 한 회전 연산이 수행된다.

2.2. 고전 신경망

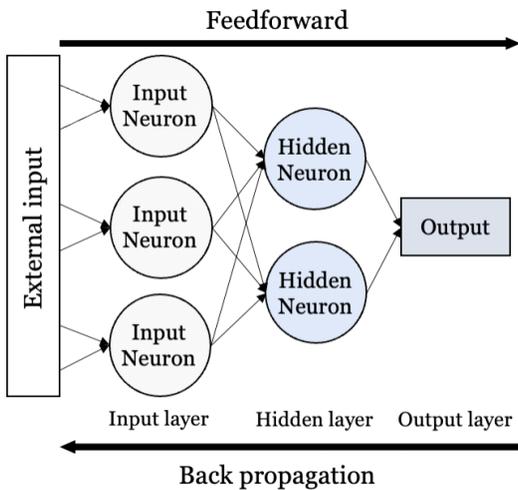
신경망의 기본 개념은 뉴런이라는 개체 무리가 결합하여 네트워크를 형성한 것이다. [그림 1]은 전체적인 신경망 프로세스이다. 각 뉴런은 내부 계산에 따라 하나 이상의 입력과 출력 값을 가지며, 여러 개의 뉴런들이 하나의 레이어를 이룬다. 레이어는 입력, 은닉, 그리고 출력 레이어로 나뉜다. 이때 입력 레이어의 뉴런들은 최초 외부 입력을 수신하여 연산하고 은닉 레이어는 입력 레이어의 출력을 입력 받아 수정하여 다음 레이어로 전송한다. 마지막 은닉 레이어는 자신의 연산 결과를 출력 레이어에 보내고 최종적으로 신경망

의 결과를 출력한다 [3].

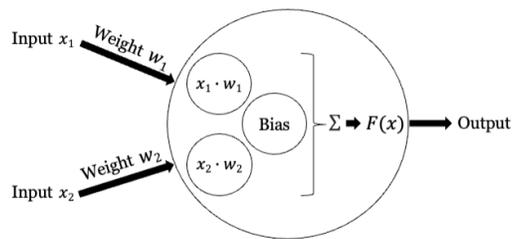
네트워크가 데이터를 입력 받아 순방향 (Feed forward) 으로 여러 뉴런을 거쳐 얻은 최종 출력과 해당 데이터의 실제 정답을 비교하고 그에 대한 손실 값을 계산하여 출력 레이어로부터 역방향으로 계산을 수행하면서 기울기를 구하는 방식을 역전파 (Back propagation)라고 하며, 일반적으로 경사하강법을 사용한다.

[그림 2]는 입력 뉴런의 구조를 세부적으로 표현한 것이며, 해당 그림과 같이 하나의 뉴런은 여러 입력을 가질 수 있고 서로 연결되어 네트워크를 형성하는 방식도 다양하다. 뉴런의 동작 방식은 다음과 같다. 입력 (Input)이 들어오면 해당 입력에 가중치 (Weight)을 곱한 후 가중치가 적용된 입력에 편향 (Bias) 값을 더하는 것이 기본 프로세스이다. 가중치란 뉴런의 동적 다이를 의미하며 이 값은 학습 과정에서 계속 변경되어 네트워크의 출력을 개선할 수 있도록 한다. 해당 과정 후에는 활성화 함수를 거쳐 뉴런의 출력을 결정한다. 즉, 가중치와 입력, 편향을 계산한 값이 활성화 함수에 입력되고, 활성화 함수에 따라 해당 결과 값이 노드의 최종 값으로 결정된다. 활성화 함수에는 일반적으로 Relu, Sigmoid, 그리고 Softmax 등의 함수가 사용된다.

신경망 학습에 필요한 요소에는 손실 함수와 경사하강법이 있다. 손실 함수란 학습 과정에서 알고리즘이 잘못된 예측을 하는지 확인하기 위한 함수이며, 신경망의 성능 지표인 손실을 계산한다. 손실 값이 크다면 학습이 부적절하게 진행되고 있는 것이며, 손실이 적을수록 학습이 잘 이루어지고 있다고 볼 수 있다. 따라서 손실을 최소화하여야 하며, 이를 통해 데이터에 대한 올바른 예측을 수행하는 것이 신경망의 목표이다. 손실을 최소화하기 위해서는 손실 함수의 최솟값을 찾아야하며, 이를 위해 기울기를 이용하여 함수의



(그림 1) 인공신경망 프로세스



(그림 2) 뉴런의 상세 구조

최솟값을 찾는 경사하강법이 사용된다. 경사하강법은 손실 함수의 최솟값을 찾기 위해 기울기를 낮은 쪽으로 조금씩 움직여 가면서 최적의 파라미터를 찾는 방식이다.

인공 신경망 모델은 여러 종류가 있으며, 대표적인 예로 MLP (Multi Layer Perceptron)[4], CNN (Convolutional Neural Network)[5], GAN (Generative Adversarial Networks)[6] 등이 있다.

MLP는 인공 신경망의 가장 기본적인 구조로, 일반적으로 모든 뉴런이 서로 연결된 Fully-connected 구조를 갖는다. CNN은 주로 이미지나 영상 인식 처리에 쓰인다. Convolution 과정과 Pooling 과정을 진행하는데, Convolution에서 커널(필터) 행렬을 입력 데이터에 적용하여 연산함으로써 데이터 특징을 추출하여 패턴을 파악한 뒤, Pooling 과정을 통해 사이즈를 줄이는 방식으로 학습한다. GAN은 실제에 가까운 가짜 데이터를 생성하는 모델로, 적대적 생성 신경망이라는 단어에서 알 수 있듯이 서로 다른 두 개의 네트워크를 적대적으로 학습시켜 실제 데이터와 유사한 데이터를 생성하는 모델이다. 두 네트워크는 생성자(Generator)와 판별자(Discriminator)이고, 생성자는 랜덤 분포로부터 실제 데이터와 유사한 확률 분포를 가지는 데이터를 생성해내고, 판별자는 실제 데이터와 생성자가 생성한 데이터를 입력받아 판별하는 역할을 수행한다. 이 과정에서 생성자는 판별자가 구별할 수 있는지의 여부를 확인하고 구별할 수 없는 데이터를 만들기 위해 학습됨으로써 실제와 유사한 데이터를 생성할 수

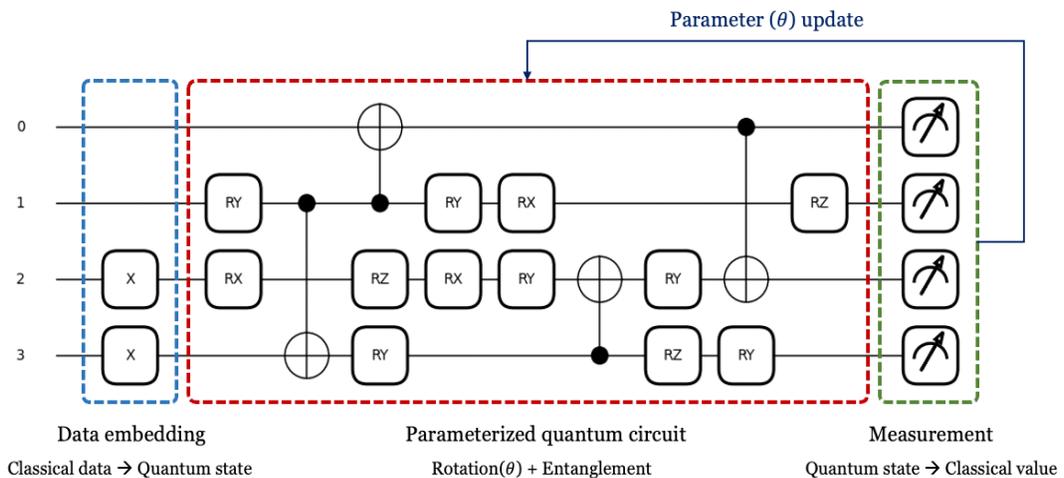
있게 된다.

III. 양자 인공지능 기술 동향

본 장에서는 양자 신경망의 동작 원리와 현재 개발된 다양한 양자 인공지능 기술들을 살펴본다.

3.1. 양자 신경망

양자 신경망은 양자 컴퓨팅을 통해 학습을 수행하는 신경망이며, 고전 신경망과 동일하게 데이터의 특징을 학습하여 학습되지 않은 데이터에 대해서도 올바른 추론을 수행할 수 있도록 일반화 성능을 확보하는 것을 주목적으로 한다. 그러나 고전 신경망과 다르게 모델이 양자 회로로 구성되어 있으므로 양자 컴퓨터 상에서 동작한다. 또한, 양자 회로로 구성되었으므로 각 큐비트에 대해 양자 게이트가 적용된 구조를 가진다. 양자 게이트는 앞서 살펴보았듯이 매개변수를 갖는 행렬로 표현되기 때문에 큐비트의 상태를 변환시킬 수 있는 선형함수이고, 연속함수들로 구성되어 있으므로 미분이 가능하다. 이러한 성질로 인해 고전 신경망과 같이 경사 하강법을 통해 매개변수를 반복적으로 갱신하여 학습할 수 있는 구조를 갖는다. 정리하면, 양자 계산은 매개변수에 대한 연속 함수이므로 미분 가능한 프로그램이라는 것을 기반으로 양자 신경망이 동작할 수 있는 것이며, 고전 신경망의 아이디어가 양자 회로에 적용된 것이다.



[그림 3] 양자 신경망의 학습 구조

양자 신경망이 고전 신경망과 같이 성공하기 위해서는 양자 하드웨어의 발전과 고전 신경망의 알고리즘과 같이 다양한 양자 알고리즘이 필요하며, 이러한 작업들을 수행할 수 있도록 하는 라이브러리들이 개발되어야 한다. 특히, 고전 신경망이 GPU를 통해 속도 향상을 달성하였듯이 양자 신경망을 통한 속도 향상의 이점을 얻기 위해서는 양자 신경망을 동작 시킬 수 있는 수준의 QPU가 반드시 필요하다. 그러나 현재 일반인들에게 공개된 양자 하드웨어는 7~12 큐비트 정도를 지원하므로 아주 작은 규모의 양자신경망에 대한 작업만 실행 가능하다.

또한, 현재 다양한 종류의 양자 신경망 알고리즘들이 개발되어 있다. 대표적으로 QSVC (Quantum Support Vector Classifier), QGAN (Quantum Generative Adversarial Network), QCNN (Quantum Convolutional Neural Network), QRL (Quantum Reinforcement Learning)이 있으며, 학습 기법으로는 전이 학습 (Transfer learning), 앙상블 (Ensemble) 등의 방식이 있다. 이러한 기술들은 Qiskit, PennyLane 등의 플랫폼에서 간단한 예제를 제공하거나 라이브러리를 통해 호출하여 사용할 수 있도록 지원하고 있는 상황이다.

3.2. 양자 신경망의 동작 과정

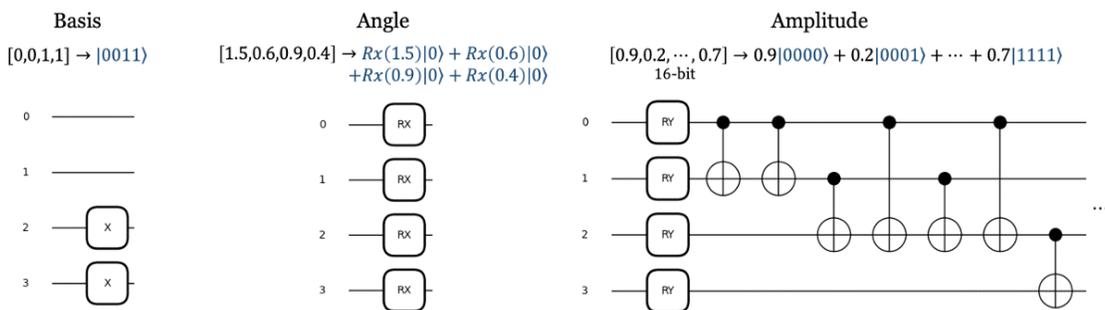
양자 신경망의 학습 과정은 [그림 3]과 같다. 먼저, 학습에 사용할 데이터를 준비해야 하는데, 현재의 학습 데이터는 고전 컴퓨터에서 연산 가능한 데이터이므로 양자 신경망에서 사용하기 위해서는 양자 상태로 변환해야 한다. 이러한 과정을 데이터 임베딩 (Data embedding)이라고 한다. 데이터 임베딩 과정을 거치

면 큐비트에 학습 데이터가 반영된 상태가 된다. 이후, 매개변수화된 양자 회로 (Parameterized quantum circuit, PQC)에 입력된다. 이 과정에서 중첩과 얽힘을 생성하는 양자 게이트들이 적용된다. 회전 게이트의 회전 각(θ)에 따라 큐비트의 상태가 변화하며, *CNOT* 게이트들에 의해 여러 큐비트들이 서로 얽힘 상태를 갖게 된다. *CNOT* 게이트는 그 자체로는 가역적이지 않지만 보조 큐비트를 추가하고 회로 전체에 단일 게이트들을 적절히 배치하여 변환을 줌으로써 비선형성을 확보할 수 있다. 회로의 마지막에서는 측정을 통해 큐비트들의 상태가 하나의 고전 값으로 결정되며, 해당 값을 기반으로 손실을 계산한다. 계산된 손실 값을 기반으로 최적화 함수를 통한 매개변수 갱신이 이루어지고 새로운 매개변수가 적용된 회로를 다시 실행함으로써 새로운 예측 값을 얻는다. 전체 과정을 반복하면서 올바른 예측이 가능하도록 학습한다.

위와 같이 양자 신경망의 학습에는 크게 데이터 임베딩, 매개변수화 된 회로, 매개변수 갱신 기법이 필요하다. 3.2.1 절부터는 각 기술에 대해 자세히 살펴본다.

3.2.1. 데이터 임베딩

데이터 임베딩은 고전 컴퓨터에서 처리할 수 있는 형식의 데이터를 양자 상태로 변환하는 과정이다. 이를 위한 다양한 방식이 존재하며, 대표적으로 기저 임베딩 (Basis embedding), 각도 임베딩 (Angle embedding), 그리고 진폭 임베딩 (Amplitude embedding)이 있다[7]. 데이터의 유형에 따라 적절한 임베딩 기법을 사용하는 것이 권장된다. [그림 4]는 기저 임베딩, 각도 임베딩, 진폭 임베딩을 위한 양자 회로를 보여준다. 기저 임베딩은 이진 데이터에 적합하



(그림 4) 데이터 임베딩을 위한 양자 회로

며, 길이가 4인 이진 데이터 $[0,0,1,1]$ 를 4개의 큐비트에 임베딩하여 $|0011\rangle$ 의 상태로 나타낼 수 있다. 즉, 모든 큐비트의 상태를 $|0\rangle$ 으로 초기화 한 후, 입력되는 데이터가 1일 경우 X 게이트를 통해 상태를 반전시켜주어 이진 데이터를 큐비트에 그대로 반영할 수 있다.

다음으로 각도 임베딩은 부동 소수점으로 표현할 수 있는 연속 데이터에 적합하다. 해당 임베딩 기법은 입력되는 데이터를 회전 게이트 (R_x, R_y, R_z)의 회전 각도로 사용한다. 예를 들어 $[1.5, 0.6, 0.9, 0.4]$ 라는 길이가 4인 데이터가 있다면 R_x 게이트를 사용할 경우, $R_x(1.5)|0\rangle + R_x(0.6)|0\rangle + R_x(0.9)|0\rangle + R_x(0.4)|0\rangle$ 의 상태로 임베딩 된다.

진폭 임베딩은 입력 데이터를 큐비트의 진폭 벡터로 표현하는 방식이며, 이 방식 또한 연속 데이터에 적합하다. 앞서 설명한 두 방식에 비해 같은 수의 큐비트를 사용할 경우 더 많은 데이터를 임베딩 할 수 있으나, 회로의 길이가 더 깊으며 복잡하다. $[0.9, 0.2, \dots, 0.7]$ 이라는 길이가 16 ($=2^4$)인 벡터는 4개의 큐비트에 임베딩할 수 있으며, $0.9|0000\rangle + 0.2|0001\rangle + \dots + 0.7|1111\rangle$ 으로 표현된다.

기저 임베딩 또는 각도 임베딩과 같이 하나의 데이터 포인트를 단일 큐비트 회전 및 반전을 사용하여 임베딩 하는 방식은 현재 많이 사용되는 일반적인 기술이지만, 매우 간단하기 때문에 효과적인 방법이라고 하기 어렵다. 그러나, 회로의 길이가 깊고 복잡한 임베딩 방식이 반드시 효과적인 것은 아니며 데이터의 특성과 수행하고자 하는 작업에 적합한 방식을 사용해야 한다. 위의 방식들 이외에도 다양한 데이터 임베딩 방식들이 있으며, 최적 또는 합리적인 임베딩 기술을 찾기 위해 많은 연구가 필요할 것으로 생각된다.

3.2.2. 매개변수화 된 양자 회로

데이터 임베딩 이후에 수행되는 매개변수화 된 양자 회로가 수행된다. 매개변수화 된 양자 회로는 자유 매개변수를 가지며, 회로의 구성은 동일하여도 매개변수들이 갱신됨에 따라 회로의 결과 값이 달라진다[8]. 따라서 고전 신경망과 같이 손실 값을 최소화하여 올바른 추론을 수행할 수 있도록 학습된다. 매개변수화 된 회로는 PQC (Parameterized quantum circuit) 또는 변이 회로 (Variational circuit)로 불린다. PQC는 양자

신경망에서 중요한 요소이며, 해당 회로를 구성할 수 있는 많은 방법이 존재한다. 해결하고자 하는 문제에 대한 수학적, 물리적 근거에 의해 결정될 수도 있고, 임의의 회로일 수도 있다. 이처럼 어떤 회로가 최적인지에 대해 정해진 바는 없으며 특정 구조를 반드시 사용해야 할 필요가 없다. 양자-고전 하이브리드 컴퓨팅을 위한 플랫폼인 PennyLane에서는 기본적인 얽힘과 회전을 갖는 회로, 얽힘과 회전이 임의로 배치되는 회로, 모든 큐비트들이 규칙적으로 강하게 얽혀있는 형태의 회로 등을 템플릿 형태로 제공하고 있다. 해당 회로들은 큐비트 수와 레이어의 개수를 설정할 수 있으므로 이러한 요소들을 조정함으로써 성능을 향상시킬 수 있다.

매개변수화 된 양자 회로는 표현력과 연결성이라는 요소를 가지며 해당 요소들은 성능 (정확도)에 영향을 미친다[9]. 표현력은 데이터의 상관관계나 특성을 포착하고 학습할 수 있는 능력을 말한다. 일반적으로 축이 다른 회전 게이트를 쓸수록 큐비트 구면 위에서 가질 수 있는 값의 범위가 늘어나므로 표현력이 높아진다. 또한, 회로의 얽힘과 회전 게이트들이 늘어날수록 높아지기도 하며, 회로의 구성에 따라 다르다. 그러나, 회로의 길이가 깊어지거나, 사용한 큐비트의 수에 비해 과도한 파라미터를 가질 경우 복잡도가 증가하고 성능이 저하되기도 한다. 특히, 복잡도가 증가할 경우 NISQ 장치에서 사용하기에 부적합하다. 따라서 적은 길이를 갖는 회로에서 적절한 얽힘과 회전 연산을 수행하는 매개변수화 된 양자 회로를 설계해야 할 필요가 있다.

3.2.3. 매개변수 갱신

앞서 살펴본 바와 같이 양자 신경망은 미분 가능한 연산인 양자 회로를 기반으로 동작하므로 경사 하강법을 통해 훈련할 수 있다. 따라서 양자 신경망의 학습을 위해서는 고전 신경망과 같이 기울기를 계산하면 되는 것이므로 양자 회로에 대해 기울기를 계산할 수 있는 방법이 필요하며, 이것이 가능해지면 고전 딥러닝과 같이 학습에 관한 여러 방법론들을 적용할 수 있게 된다. 그러나 양자 계산은 매우 고차원의 공간에서 큐비트의 진폭을 다루어야 하므로 어려운 작업이다. 또한, 고전 신경망에서 정방향 연산에서 생기는 노드들의 값을 저장한 후 역전과 과정에서 저장된 중간 단계의 정

보들을 사용하는 것과 같이 양자 하드웨어에서는 양자 회로의 연산 중간 값을 저장하여 사용할 수 없다. 따라서 고전 신경망의 역전파 과정을 그대로 적용할 수 없으며, 양자 회로에서의 기울기 계산을 위해 사용된 기술이 파라미터 이동 (Parameter shift) 이다.

사인 (sine) 함수의 도함수는 코사인 (cosine) 함수이며, 서로 다른 함수이지만 $\pi/2$ 만큼 위상 편이가 있는 관계이다. 따라서 사인 함수의 도함수인 코사인 함수는 사인 함수만으로 표현할 수 있다. 즉, 어떠한 함수를 평행 이동 시켜서 도함수를 얻을 수 있으며, 이러한 개념이 양자 신경망의 기울기 계산에 적용되었다. 양자 신경망은 삼각함수 속성을 많이 사용하기 때문에 일반적으로 파라미터 이동 규칙이 적용될 수 있다. 매개변수 θ 를 가지는 양자 회로의 결과 값을 $f(\theta)$ 로 표현하면, $f'(\theta) = c[f(\theta+s) - f(\theta-s)]$ 와 같이 양자 신경망의 매개변수 갱신에 필요한 기울기를 계산할 수 있다 (c 는 상수). 즉, 양자 회로는 매개변수를 가지고 있고, 양자 회로의 특성 상 매개변수 이동 규칙을 적용하여 미분할 수 있으며, 해당 규칙은 양자 신경망 소프트웨어에 의해 자동으로 계산될 수 있다. 따라서 경사 하강법을 통한 양자 회로 훈련이 가능해지는 것이다.

3.3. 현재 개발된 양자 신경망 모델 및 학습 기술

현재까지 QSVC, QGAN, QCNN, QRL 등과 같은 다양한 양자 신경망 모델들이 개발되었으며, 전이학습, 앙상블 등과 같은 구조의 학습 기법들도 연구되었다.

3.3.1. 양자 서포트 벡터 머신 분류기 (QSVC) [10]

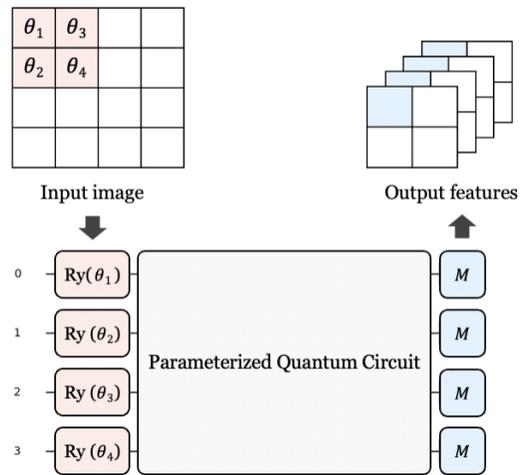
QSVC는 고전 머신러닝 기술 중 하나인 서포트 벡터 머신을 양자 회로를 통해 구현한 것이다. 고전 서포트 벡터 머신은 $n - 1$ 차원의 초평면을 통해 n 차원의 데이터를 분리할 수 있는 최적 경계를 찾는 머신러닝 알고리즘이다. 초평면을 잘 배치하여 데이터 포인트 간의 경계를 최대화하여 효율적으로 분리하기 위해 커널 함수를 사용하며, 이러한 초평면을 찾기 위해서는 데이터에 비선형 함수를 적용해야 한다.

QSVC는 서포트 벡터 머신의 커널 연산을 양자 회로로 구현한 것이며 양자 컴퓨터가 고차원의 데이터 작업에 유리하므로 기존의 서포트 벡터 머신이 처리하기 어려웠던 커널 최적화에서의 이점이 존재한다.

QSVC도 양자 신경망의 기본 요소인 데이터 임베딩과 매개변수화 된 회로로 구성되고, 기존 서포트 벡터 머신에서 사용되는 비선형 함수를 매개변수화 된 회로의 회전 각으로 사용한다. 이러한 회전 게이트들과 얽힘을 여러 큐비트들에 반복적으로 적용함으로써 양자 서포트 벡터 머신을 구성할 수 있다.

3.3.2. 양자 컨볼루션 신경망 (QCNN) [11]

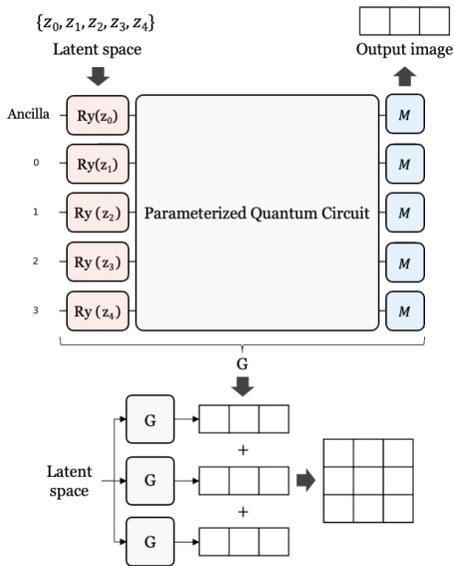
양자 컨볼루션 신경망은 [그림 5]와 같은 구조를 갖는다. 고전 컨볼루션 신경망에서는 입력 이미지의 일부분과 커널 (필터) 간의 연산을 수행하였는데 해당 부분에 양자 신경망이 적용된 것이다. 이때 주로 2×2 또는 3×3 크기의 커널이 사용되며, 이를 위해서는 4 큐비트 또는 9 큐비트를 갖는 회로가 필요하다, 만약 2×2 크기의 커널이 사용된다면 학습에 사용할 이미지 데이터 중 2×2 픽셀 영역만을 양자 신경망에 입력한다. 입력된 데이터는 양자 회로를 거쳐 측정되며 큐비트 수만큼의 픽셀 값이 출력된다. 각 픽셀은 자기 다른 채널의 단일 픽셀로 매핑된다. 이러한 과정을 전체 이미지 영역에 대해 반복하여 학습을 진행한다.



(그림 5) QCNN의 구조

3.3.3. 양자 생성형 적대적 신경망 (QGAN) [12]

QGAN은 생성형 신경망이며, 고전 신경망의 종류 중 하나인 생성형 적대적 신경망 (GAN)을 양자 신경망으로 구현한 것이다. QGAN의 동작 과정은 [그림 6]



(그림 6) QGAN의 생성자의 구조

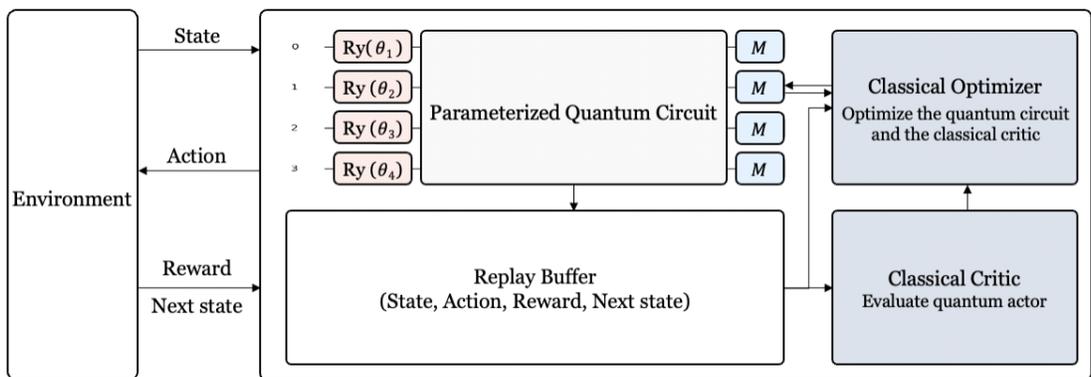
과 같다. 고전 GAN과 같이 생성자는 랜덤 벡터로부터 특정 데이터의 확률 분포를 만들어내고, 판별자는 생성자가 생성한 데이터와 실제 데이터를 구별한다. 이후, 판별자의 구별 결과를 기반으로 생성자는 구별 불가능한 데이터를 생성하기 위해 학습한다. 생성자와 판별자는 모두 신경망 모델이며, 생성자와 판별자 모두 양자 신경망으로 구성될 수 있다. 판별자는 양자 신경망 기반의 분류기로 구성되며 앞서 설명한 모델들과 같이 학습 데이터를 입력으로 받는다. 그러나 생성자는 판별자와 다르게 생성형 신경망이며, 잠재 벡터를 입력 받은 후 실제 데이터가 갖는 분포와 비슷하게 변형해야 한다. 생성 작업을 위해서는 분류 모델에 비해

복잡한 비선형 변환이 필요하며 이를 위해 보조 큐비트 (Ancilla qubit)가 사용된다. 보조 큐비트는 회로의 중간 연산 결과를 저장하는 데에 주로 사용되며, 3.2절에서 설명한 바와 같이 CNOT 게이트를 사용하여 다른 큐비트들과 얽히도록 함으로써 비선형성을 더욱 효율적으로 사용할 수 있도록 한다. 이러한 이유로 인해 QGAN에서는 더욱 효율적인 비선형을 위해 보조 큐비트를 사용하였다. 이러한 방식으로 양자 신경망을 통해 복잡한 비선형 변환을 수행하는 생성자를 구성할 수 있다.

데이터 생성을 위해서는 [그림 6]과 같은 양자 신경망 기반의 생성자를 여러 개 결합해야 한다. 즉, 생성할 데이터의 일부를 각각의 서브 생성자가 생성하고 그 결과를 모두 통합하면 하나의 이미지를 생성할 수 있는 구조이다. 생성형 신경망은 데이터를 분류하는 작업보다 훨씬 복잡하고 정교한 작업이므로 분류기에 비해 더 많은 자원을 필요로 하지만 현재의 양자 컴퓨팅 환경에서는 많은 큐비트를 사용하기 어렵다. 그러나 QGAN의 구조는 NISQ 환경에서 실행하기에 적합하도록 구성되었으며, 현재는 이러한 패치 단위의 학습이 주로 사용되고 있다.

3.3.4. 양자 강화학습 [13]

양자-고전 강화학습은 고전 강화 학습과 전체적인 프로세스는 동일하며, 에이전트가 행동을 결정하기 위해 학습하는 과정의 일부에 양자 신경망을 적용한 기술이다. 고전 강화학습은 해결하고자 하는 문제에 대해 최적의 선택을 행하도록 하는 학습법이고, 이를 위해 어떠한 행동에 대한 보상 (Reward)를 활용한다. 따



(그림 7) 양자 강화학습의 구조

라서 강화학습 모델은 최대 보상을 받기 위해 올바른 선택을 하게 된다. [그림 7]은 양자-고전 강화학습의 구성도이다. 매개변수화 된 양자 회로는 현재 상태 (State)를 입력으로 받아 동작하고 측정되며, 회로의 출력 값을 사용하여 현재 상태에서 어떠한 행동 (Action)을 할 것인지에 대한 확률 값을 계산한다. 이러한 정보는 Replay Buffer에 저장되고, 해당 정보들을 기반으로 매개변수화 된 회로 자체의 매개변수와 회로가 생성한 행동을 평가하는 Classical Critic 모델의 매개변수가 최적화된다. 이와 같이 강화학습을 위한 정책에 의해서 최적의 행동을 도출하는 과정에 양자 신경망이 적용될 수 있다.

3.3.5. 양자 인코더 [14]

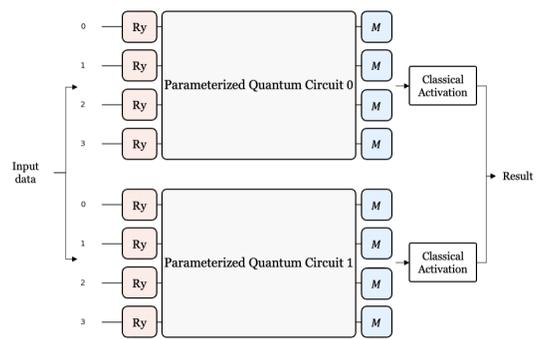
오토 인코더는 입력 데이터에 대한 특징을 효율적으로 압축하고 (인코딩), 압축된 주요 특징 정보를 기반으로 데이터에 대한 복원을 수행 (디코딩)하는 신경망 구조이다. 그 중, 인코딩 과정은 데이터의 주요 특징을 남겨두고 차원을 축소하는 기능을 한다. 양자 신경망의 특성 상 고차원의 복잡한 데이터에 대한 학습을 수행하기 적절하므로 고전 신경망보다 상위 레이어로 사용하여 특징 추출을 위한 인코더 형식으로도 많이 사용된다.

3.3.6. 양자 전이학습 [15]

전이학습은 사전 훈련된 모델을 기반으로 추가 학습을 통해 해결하고자 하는 문제에 맞게 조정할 수 있는 학습 기법이다. 전이학습을 구현하기 위해서는 사전 훈련된 네트워크 뒤에 새로운 레이어를 추가해야한다. 즉, 두 개의 네트워크 (사전 학습된 모델과 새로운 레이어)를 순차적으로 결합하는 구조이다. 이러한 구조는 양자-고전 하이브리드 신경망과 동일한 구조이며, 학습된 고전 신경망 뒤에 양자 신경망을 추가하여 구현할 수 있다.

3.3.7. 양자 앙상블 [16]

앙상블은 여러 개의 네트워크를 개별적으로 학습시킨 후 그 결과를 결합함으로써 일반화 성능을 향상시키는 학습 기법이다. 결합 기법으로는 각 모델의 평균

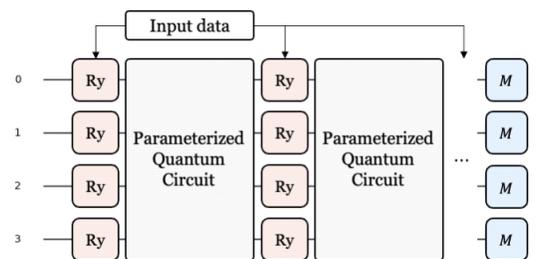


(그림 8) 양자 앙상블 학습

이나, 다수의 모델이 선택한 결과로 선택하는 방식 등이 있다. 양자 앙상블 기법은 [그림 8]과 같으며, 사용되는 신경망들이 양자 신경망으로 구성된다는 점을 제외하면 전체 구조는 동일하다. 각 모델은 다른 구조를 가지도록 설계하여야 하고, 서로 다른 QPU에서 병렬 처리될 수 있다. 일반적으로 앙상블 방식은 단일 모델에 비해 성능이 좋으며, 이는 양자 신경망에서도 동일하다. 이것은 각 QPU의 성능과 관련 없이 서로 다른 매개변수를 갖는 회로이므로 발생하는 결과이다.

3.3.8. 데이터 재업로딩[17]

데이터 재업로딩은 [그림 9]과 같이 동일한 데이터를 양자 신경망에 여러 번 임베딩하는 기술이다. 즉, 단일 회전만으로 데이터를 반영하는 것이 아니라 반복적인 회전 게이트를 통해 여러 번 업로드 하는 것이고, 각 임베딩 사이에서 매개변수를 갖는 회로가 동작한다. 이는 같은 데이터에 대해 또 다른 가중치를 적용할 수 있도록 하며, 데이터를 한 번 임베딩해서 단일 회전을 수행할 때보다 더 복잡한 기능을 수행할 수 있게 된다. 이는 고전 신경망의 입력층의 각 뉴런들마다 입력 데이터를 처리하는 것과 같은 역할을 한다. 다시 말



(그림 9) 데이터 재업로딩

해서, 데이터 업로딩이 반복될수록 하나의 고전 레이어가 갖는 뉴런의 수가 증가하는 것과 유사한 구조를 갖는다.

IV. 결 론

양자 컴퓨터는 양자 역학의 원리를 기반으로 기존의 컴퓨터가 해결할 수 없었던 난제들을 푸는데 활용될 수 있으며, 특히 암호 분석, 화학 시뮬레이션, 대규모 데이터 셋 기반의 인공지능 등에 관한 연구들이 지속적으로 수행되고 있다. 그 중, 양자컴퓨터를 활용한 인공지능 기술은 양자컴퓨터의 특성을 고전 신경망 기술에 적용한 것이며, 예측 정확도와 학습 속도, 메모리 관점에서 양자적 이점을 얻을 수 있을 것으로 기대되고 있다. 그러나 현재의 양자컴퓨터는 많은 큐비트와 깊은 회로 깊이를 사용할 수 없으므로 아직까지는 고전 컴퓨터를 능가하기 어렵다. 따라서 현재는 양자와 고전 컴퓨팅 기술을 결합한 하이브리드 방식을 활용하는 연구들이 많이 수행되고 있다. 3장에서 살펴보았듯이 양자 신경망 모델과 학습 기술들이 많이 개발되었으나 현재는 제약적인 NISQ 환경에서 활용 가능한 양자 신경망에 관한 연구들이 수행되는 추세이다. 또한, 소개된 기술들 외에도 소규모 양자컴퓨터에서 대규모 시뮬레이션을 하기 위한 회로 절단 기술[18] 등의 새로운 기술들이 연구되고 있으며, 이와 같이 더 효율적인 학습이 가능하도록 하기 위한 기술들 또한 개발되고 있는 상황이다. 이러한 사례들에서 알 수 있듯이, 현재 상황에서 활용할 수 있는 양자 인공지능 기술들이 활발히 연구되고 있으며 앞으로도 이러한 관심이 지속될 것으로 보인다. 향후 더 큰 규모의 양자컴퓨터가 사용 가능해지고 그에 맞는 학습 기술들이 개발된다면 학습 속도나 정확도 측면에서 양자 우위에 더욱 가까워질 수 있을 것으로 예상된다.

참 고 문 헌

- [1] The IBM Quantum Development Roadmap [Website]. (2023, Mar 23). <https://www.ibm.com/quantum/roadmap>.
- [2] IBM's Osprey is a Quantum Bomb: The World's Most Powerful Quantum Computer[Website]. (2023, Mar 23). <https://techcasm.com/ibms-osprey-is-a-quantum-bomb-the-worlds-most-powerful-quantum-computer-2023/>
- [3] Haykin, Simon. "Neural networks and learning machines, 3/E," Pearson Education, Inc., Upper Saddle River, New Jersey 07458, pp. 1-906, 2009.
- [4] Gardner, Matt W., and S. R. Dorling. "Artificial neural networks (the multilayer perceptron)—a review of applications in the atmospheric sciences," *Atmospheric environment*, Vol. 32, no. 14 - 15: pp. 2627-2636, Aug. 1998.
- [5] Albawi, Saad, Tareq Abed Mohammed, and Saad Al-Zawi. "Understanding of a convolutional neural network," 2017 international conference on engineering and technology (ICET). pp. 1-6, Aug. 2017.
- [6] Goodfellow, Ian, et al. "Generative adversarial networks," *Communications of the ACM* Vol. 63, no. 11: pp. 139-144, 2020.
- [7] How to embed data into a quantum state[Website]. (2023, Mar 23). <https://pennylane.ai/blog/2022/08/how-to-embed-data-into-a-quantum-state/>
- [8] Variational circuit[Website]. (2023, Mar 23). https://pennylane.ai/qml/glossary/variational_circuit.html
- [9] Sukin, Sim, et al. "Expressibility and Entangling Capability of Parameterized Quantum Circuits for Hybrid Quantum-Classical Algorithms," *Advanced Quantum Technologies*, 2(12), Dec. 2019.
- [10] Havlíček, Vojtěch, et al. "Supervised learning with quantum-enhanced feature spaces," *Nature*, 567, pp. 209-212, Mar. 2019.
- [11] Henderson, Maxwell, et al. "Quantum neural networks: powering image recognition with quantum circuits," *Quantum Machine Intelligence*, 2(1), pp. 2, Feb. 2020.
- [12] Huang, He-Liang, et al. "Experimental quantum generative adversarial networks for image generation," *Physical Review Applied*, 16(2), pp. 024051, Aug. 2021.
- [13] Kwak, Yunseok, et al. "Introduction to quantum reinforcement learning: Theory and pennylane-based implementation," 2021 *Inter-*

national Conference on Information and Communication Technology Convergence (ICTC). IEEE, pp. 416-420, Dec. 2021.

- [14] Mangini, Stefano, et al. "Quantum neural network autoencoder and classifier applied to an industrial case study," *Quantum Machine Intelligence*, 4(2), pp. 13, Jun. 2022.
- [15] Mari, Andrea, et al. "Transfer learning in hybrid classical-quantum neural networks," *Quantum*, 4, pp. 340, Oct. 2020.
- [16] Schuld, Maria, and Francesco Petruccione. "Quantum ensembles of quantum classifiers," *Scientific reports*, 8(1), pp. 2772, Feb. 2018.
- [17] Pérez-Salinas, Adrián, et al. "Data re-uploading for a universal quantum classifier," *Quantum*, 4, pp. 226, Feb. 2020.
- [18] Peng, Tianyi, et al. "Simulating large quantum circuits on a small quantum computer," *Physical review letters*, 125(15), 150504, Oct. 2020.

〈저자 소개〉



김 현 지 (Hyun-ji Kim)

학생회원

2020년 2월 : 한성대학교 IT응용시스템공학과 졸업

2020년 3월~2022년 2월 : 한성대학교 IT융합공학과 석사 졸업

2022년 3월~현재 : 한성대학교 정보컴퓨터공학과 박사과정

<관심분야> 정보보안, 인공지능, 양자 컴퓨팅



임 세 진 (Se-jin Lim)

학생회원

2022년 2월 : 한성대학교 컴퓨터공학부 졸업

2022년 3월~현재 : 한성대학교 IT융합공학과 석사과정

<관심분야> 양자 컴퓨터, 인공지능보안, 정보보안



김 덕 영 (Duk-young Kim)

2019년 2월 : 한성대학교 디자인 아트평생교육원 인테리어디자인과 졸업

2023년 3월~현재 : 한성대학교 융합보안학과 석사과정

<관심분야> 정보보안, 인공지능



서 화 정 (Hwa-jeong Seo)

종신회원

2010년 2월 : 부산대학교 컴퓨터공학과 졸업

2012년 2월 : 부산대학교 컴퓨터공학과 석사

2016년 1월 : 부산대학교 컴퓨터공학과 박사

2016년 1월~2017년 3월 : 싱가포르 과학기술청

2017년 4월~2023년 2월 : 한성대학교 IT융합공학부 조교수

2023년 2월~현재 : 한성대학교 융합보안학과 부교수

<관심분야> 정보보안, 암호구현