One Control Qubit 양자 위상 추정 알고리즘의 성능 분석

하진영(고려대학교), 허준(고려대학교)*
ksuwer@korea.ac.kr, *junheo@korea.ac.kr

Performance Analysis of One Control Qubit Quantum Phase Estimation Algorithm

요 약

본 논문에서는 One Control Qubit 를 사용하는 양자 위상 추정 알고리즘의 시뮬레이션을 수행한다. One Control Qubit 양자 위상 추정 알고리즘의 오류율을 기존 양자 위상 추정 알고리즘의 오류율을 비교한다. QISKit 을 사용해 시뮬레이션을 수행하여 One Control Qubit 양자 위상 추정 알고리즘이 기존 양자 위상 추정 알고리즘에 비하여 약 5.3%의 정확도 향상을 가지는 것을 확인하였다.

Ⅰ. 서 론

1994 년에 Copper Smith 는 양자 정보를 bit domain 에서 phase domain 으로 변환하는 양자 푸리에 변환(QFT)을 개발하였다[1]. 또한 1994 년에 Peter Shor 는 소인수 분해를 효율적으로 수행하는 Shor Algorithm 을 구현하는 과정에서 양자 위상을 추정할 수 있는 양자 위상 추정 알고리즘(QPE)을 개발하였다[2]. 1998 년에 Artur Ekert 는 One Control Qubit 양자 위상 추정 알고리즘(OQPE)을 개발하였다[3]. 본 논문에서는 QISKit 을 사용하여 OQPE 와 QPE 시뮬레이션을 수행하여 두 알고리즘의 성능을 비교한다[4].

Ⅱ. 본 론

본 논문에서는 QPE 의 근간이 되는 QFT 에 대해서 설명을 하고, 이를 기반으로 QPE 에 대해서 설명을 한다. 또한 OQPE 에 대해 설명을 하고, 일반적으로 OQPE 가 가지는 장점인 적은 큐비트를 사용하는 것 이외에 정확도 측면에서도 QPE 에 비하여 OQPE 가 더 높은 정확도를 보임을 시뮬레이션을 통해 보인다.

A. 양자 푸리에 변환 (QFT)

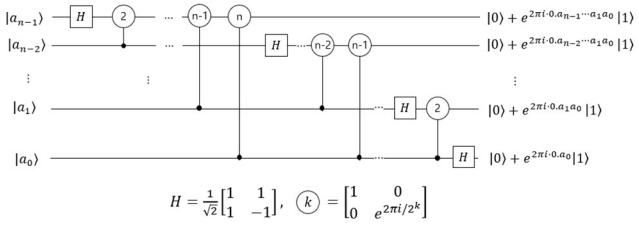

그림 1. QFT 수행 양자회로의 구조

그림 1 은 n 큐비트 QFT 를 수행하는 양자회로의 구조를 나타낸다. QFT 의 n비트 입력 $|a\rangle$는 다음과 같이 표현된다.

$$|a\rangle = |a_{n-1}a_{n-2}\cdots a_1 a_0\rangle \quad (1)$$

위 식에서 $a_{n-1}a_{n-2}\cdots a_1 a_0$ 는 a 를 2 진수로 나타낸 값이다. QFT 이후의 양자 상태는 다음과 같이 표현된다.

$$|a\rangle \xrightarrow{QFT} \sum_{k=0}^{2^n-1} e^{2\pi i \cdot ka/2^n}|k\rangle \quad (2)$$

따라서 QFT 는 bit domain 의 a 값을 양자 상태의 phase domain 으로 변환하는 것을 확인할 수 있다.

B. 양자 위상 추정 알고리즘 (QPE)

양자 위상 추정 알고리즘은 유니터리 연산자 U 와 해당연산자의 고유벡터 $|u\rangle$ 가 주어져 있을 때 고유값 $e^{2\pi i\phi}$을 추정한다. 알고리즘의 구조는 그림 2 와 같다.

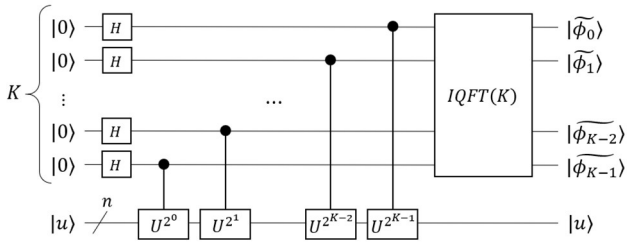

그림 2. 양자 위상 추정 알고리즘의 구조

K는 위상 추정에 사용되는 레지스터 큐비트의 개수로, 위상 추정의 해상도와 관련이 된다. n은 데이터 큐비트의 개수로, U와 $|u\rangle$의 dimension 이다. $IQFT(K)$는 K 큐비트 Inverse QFT 이다. QPE 수행 후 양자상태는 다음과 같이 표현된다.

$$|0\rangle^{\otimes K}|u\rangle \xrightarrow{QPE} \frac{1}{N}\sum_{j=0}^{N}\left\{\frac{1-e^{2\pi i\left(\phi-\frac{j}{N}\right)N}}{1-e^{2\pi i\left(\phi-\frac{j}{N}\right)}}\right\}|j\rangle|u\rangle \quad (3)$$

위 식에서 $N = 2^K$ 이다. 알고리즘 수행 이후 $|\tilde{\phi}\rangle = |\widetilde{\phi_0}\rangle \otimes \cdots \otimes |\widetilde{\phi_{K-1}}\rangle$ 를 측정하여 t 를 얻을 확률 $p(t)$ 는 다음과 같다.

$$p(t) = \frac{1}{N^2}\cdot\frac{\sin^2\left[\pi\left(\phi-\frac{t}{N}\right)N\right]}{\sin^2\left[\pi\left(\phi-\frac{t}{N}\right)\right]} \quad (4)$$

이 때 ϕ의 추정 값 $\tilde{\phi}$는 $\tilde{\phi} = \frac{t}{N}$이다. 식(4)에서 $\delta = \phi - \tilde{\phi}$가 작을수록 $p(t)$가 급격하게 증가하므로, 측정은 높은 확률로 ϕ를 추정할 수 있음을 확인할 수 있다.

QPE 가 적어도 $1-\epsilon$ 이상의 확률로 성공함을 보장하고자 할 때 필요한 K는 다음과 같다.

$$K = L + \left\lceil \log_2\left[2+\frac{1}{2\epsilon}\right]\right\rceil \quad (5)$$

따라서 높은 확률로 올바른 측정 결과를 얻기 위해서는 추가로 필요한 큐비트의 개수K가 커지는 것을 확인할 수 있다.

C. 단일 큐비트 양자 위상 추정 알고리즘 (OQPE)

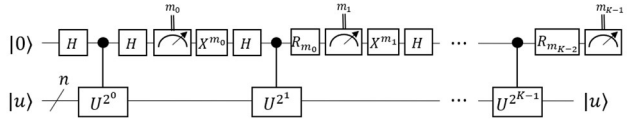

그림 3. 단일 큐비트 위상 추정 알고리즘의 구조

그림 3 은 OQPE 의 구조를 나타낸다. R_{m_i}는 다음과 같은 연산을 수행한다.

$$R_{m_i} = \begin{bmatrix}1 & 0\\ 0 & e^{-2\pi i\cdot 0.0m_i m_{i-1}\cdot m_{0(2)}}\end{bmatrix} \quad (6)$$

OQPE 알고리즘은 QPE 의 과정에서 해상도를 위한 큐비트를 K 개 사용하지 않고 한 개의 큐비트를 K 번

재사용하는 방식을 사용한다. 측정 이후 큐비트의 상태는 $|0\rangle$ 또는 $|1\rangle$ 상태로 붕괴되는데, 이를 $|0\rangle$ 상태로 반환하기 위해 X^{m_i} 연산이 사용된다. OQPE 를 QPE 와 비교하였을 때, QPE 에서 레지스터 큐비트에서 각 큐비트에 수행되는 연산을 모두 한 후 해당 큐비트를 측정하고, 그 측정결과에 따라 레지스터의 다음 큐비트에 연산을 수행한다.

일반적으로 QPE 에 비해서 OQPE 의 장점으로 이야기하는 것은 상대적으로 적은 큐비트 수를 사용한다는 것이다. 본 논문에서는 실제로 양자 프로세서 상에서 OQPE 를 구동할 때 OQPE 는 첫번째로 IQFT 과정에서 오류율이 높은 2 큐비트 연산을 사용하는 QPE 에 비교하여 1 큐비트 연산을 사용하고, 두번째로 QPE 는 알고리즘 전체 수행 이후 측정을 하는 반면 OQPE 는 알고리즘 중간중간에 측정을 하는 식으로 수행을 하기 때문에 레지스터 큐비트의 상태를 오래 지속할 필요가 없어 전체적으로 OQPE 방식이 QPE 보다 낮은 오류율을 가질 것으로 가정하였다. 본 논문에서는 시뮬레이션을 통해 이러한 가정이 실제로 성립하는지 확인한다.

D. 시뮬레이션을 통한 OQPE 와 QPE 의 성능 비교

고유값 $e^{2\pi i \cdot 1011_{(2)}}$ 를 추정하는 QPE 와 OQPE 양자 회로를 설계하고 시뮬레이션을 통해 두 알고리즘의 성능을 비교한다. QPE와 OQPE의 양자 회로는 그림 4와 같다.

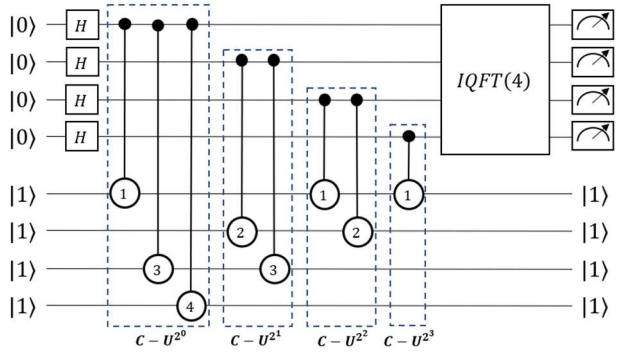

그림 4. (a) QPE 양자회로

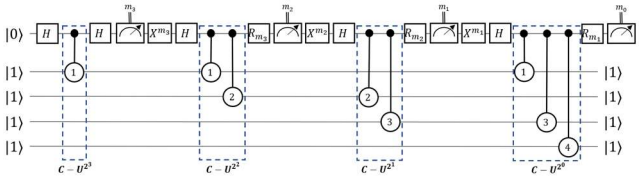

그림 4. (b) OQPE 양자회로

그림 4 에서 U^{2^k}연산을 U를 2^k번 수행하지 않고 효율적으로 구현을 할 수 있음을 확인할 수 있다. QPE 양자 회로는 8 개의 큐비트를, OQPE 양자 회로는 5 개의 큐비트를 사용한다. 예시로 든 고유값은 2 진수로 유한하게 표현될 수 있기 때문에 레지스터 큐비트에 4 개의 큐비트만을 사용해도 100%의 확률로 고유값을 찾을 수 있다. 2 진수로 유한하게 표현되지 않는 고유값의 경우에는 레지스터 큐비트에 추가로 큐비트를 사용하여야 한다.

양자 회로 시뮬레이션 툴인 QISKit 을 사용하여 시뮬레이션을 수행하였으며, IBM 의 16 큐비트 양자 프로세서 Melbourne 을 모사하여 시뮬레이션을 수행하였다. 그림 4 의 양자 회로를 총 10,00,000 회 시뮬레이션을 수행하였다. 16 큐비트 양자 프로세서 Melbourne 의 스펙은 그림 5 와 같다[4].

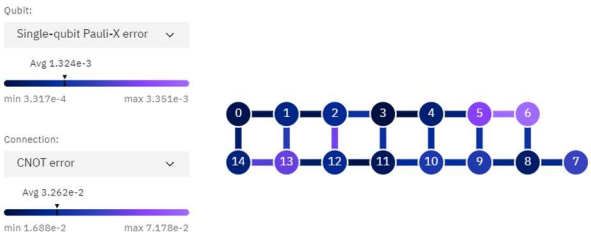

그림 5. ibmq_16_melbourne 의 스펙

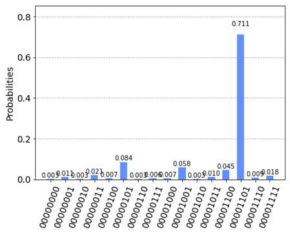

그림 6. (a) QPE

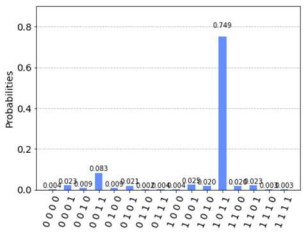

그림 6. (b) OQPE

그림 6 은 QPE 와 OQPE 양자회로의 시뮬레이션 결과이다. QPE 양자회로의 시뮬레이션 결과 약 71.1%의 정확도를 보이는 반면 OQPE 양자회로의 시뮬레이션 결과는 약 74.9%의 정확도를 보이는 것을 확인할 수 있다. 따라서 해당 시뮬레이션에 대하여 OQPE 의 방식이 QPE 에 비하여 약 5.3%의 성능 우위를 보이며, 가정한 대로 OQPE 방식이 QPE 방식에 비하여 더 좋은 성능을 보이는 것을 확인할 수 있다.

Ⅲ. 결론

본 논문에서는 QPE 알고리즘과 OQPE 알고리즘을 실제 양자 회로로 구현할 때 OQPE 방식이 QPE 방식보다 더 좋은 성능을 보임을 QISKit 시뮬레이션을 통해 보였다. 이는 OQPE 방식이 비교적 오류율이 낮은 1 큐비트 연산을 QPE 방식에 비하여 많이 사용하고, OQPE 방식은 양자오류정정 방식과 비슷하게 알고리즘 중간중간에 측정을 수행하기 때문으로 추정되며, 따라서 레지스터 큐비트 개수가 많을수록, 양자 프로세서의 연산 오류율, 큐비트 상태 유지시간 등의 성능이 낮을 수록 OQPE 방식이 QPE 방식에 비하여 더 높은 성능을 보일것으로 예측할 수 있다.

ACKNOWLEDGMENT

이 논문은 2021 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.2019R1A2C2010061)

참 고 문 헌

[1] Coppersmith, D. (1994), "An approximate Fourier transform useful in quantum factoring", Technical Report RC19642, IBM.

[2] Shor, Peter W. (1994), "Algorithms for quantum computation: discrete logarithms and factoring", Proceedings 35th annual symposium on foundations of computer science. Ieee.

[3] Mosca, Michele, and Artur Ekert. (1998), "The hidden subgroup problem and eigenvalue estimation on a quantum computer." NASA International Conference on Quantum Computing and Quantum Communications. Springer, Berlin, Heidelberg.

[4] IBM Quantum Experience, http://www.research.ibm.com/quantum.