

비-허미시안 행렬에 대한 저 복잡도 양자 역행렬 알고리즘

정현우, 하정석

한국과학기술원

destinylz@kaist.ac.kr, jsha@kaist.edu

Low Complexity Quantum Matrix Inversion Algorithm
for non-Hermitian Matrices

Hyunwoo Jung, Jeongseok Ha

Korea Advanced Institute of Science and Technology

요약

양자 알고리즘은 양자 컴퓨터가 주어진 문제를 해결하기 위해 사용하는 절차이며 다양한 알고리즘이 제안되어왔다. 양자 알고리즘 중 Harrow-Hassidim-Lloyd (HHL) 알고리즘은 행렬 \mathbf{A} 와 벡터 \mathbf{b} 가 주어졌을 때 선형 방정식 $\mathbf{Ax}=\mathbf{b}$ 의 답을 찾는 알고리즘이다. HHL 알고리즘은 행렬 \mathbf{A} 가 에르미트 행렬일 때를 가정하며, 비-에르미트 행렬의 경우에는 차원을 확장하고 새로운 선형 방정식을 만들면서 문제를 해결한다. 본 논문에서는 비-에르미트 행렬일 때 HHL 알고리즘의 동작 과정을 설명하고, 새로운 선형 방정식의 특징을 이용하여 계산 복잡도를 줄이기 위한 방법을 제안한다.

I. 서론

양자 컴퓨터 (quantum computer)는 기존의 컴퓨터가 계산하는 데 많은 시간이 걸리는 문제를 양자의 중첩을 이용하여 지수적인 속도 향상을 하면서 해결할 수 있다. 양자 알고리즘 (quantum algorithm)은 양자 컴퓨터가 주어진 문제를 해결하기 위해 사용하는 절차이며 다양한 알고리즘 [1]이 제안되어왔다. 행렬의 고유값 (eigenvalue)을 추출하는 양자 위상 추정 (quantum phase estimation, QPE), 기존의 컴퓨터에서 수행하는 푸리에 변환 (Fourier transform)을 큐비트에서 수행하는 양자 푸리에 변환과 같은 기본적인 알고리즘을 바탕으로 주어진 문제의 답의 개수를 세는 양자 카운팅 알고리즘 (quantum counting algorithm, QCA), 답의 리스트를 찾는 Grover 알고리즘, 소인수 분해를 위한 Shor 알고리즘 등이 존재한다. 최근에는 양자 컴퓨터를 이용하여 기계학습 (machine learning)을 수행하기 위하여 양자 특이값 분해 (quantum singular value decomposition, QSVD) 알고리즘이나 선형 방정식 $\mathbf{Ax}=\mathbf{b}$ 의 해를 구하는 양자 역행렬 (quantum matrix inversion) 알고리즘 [2]이 주목받고 있다.

양자 역행렬 알고리즘은 Harrow-Hassidim-Lloyd (HHL) 알고리즘으로 알려졌으며 행렬 \mathbf{A} 가 허미시안 행렬일 때 스펙트럼 분해 (spectral decomposition)를 이용한다. 행렬 \mathbf{A} 가 비-허미시안 행렬일 때는 차원을 확장하여 새로운 허미시안 행렬 \mathbf{H} 를 만든 후에 스펙트럼 분해를 이용하여 선형 방정식의 해를 구한다. 본 논문에서는 비-허미시안 행렬일 때 HHL 알고리즘의 동작 과정에 대하여 설명한다. 또한, 새롭게 만들어진 선형 방정식의 특징을 이용하여 모든 큐비트를 측정하는 기존의 방식에서 불필요한 큐비트의 측정을 줄이는 방식으로 계산 복잡도를 줄이는 방법을 제안한다.

본 논문은 총 5장으로 구성된다. 2장에서는 HHL 알고리즘의 수학적 배경에 대하여 간단히 설명한다. 3장에서는 HHL 알고리즘의 회로를 설명한다. 4장에서는 비-허미시안 행렬일 때 허미시안 행렬을 생성하는 방법과 그 특징을 설명하고 계산 복잡도를 줄이는 방법을 제안한다. 마지막으로 5장에서는 결론과 함께 논문을 마친다.

II. HHL 알고리즘의 수학적 배경

$N \times N$ 행렬 \mathbf{A} 가 허미시안 행렬일 때 선형 방정식 $\mathbf{Ax}=\mathbf{b}$ 를 살펴보자. 양자 상태로 치환하기 위하여 벡터 \mathbf{x} 와 \mathbf{b} 는 크기를 정규화하고 각각 양자 상태 $|x\rangle$ 와 $|b\rangle$ 로 매핑한다. 행렬 \mathbf{A} 는 스펙트럼 분해를 이용하면 다음 식과 같다.

$$\mathbf{A} = \sum_{j=0}^{N-1} \lambda_j |e_j\rangle \langle e_j|$$

이때 λ_j 와 $|e_j\rangle$ 는 행렬 \mathbf{A} 의 고유값과 고유벡터이다. \mathbf{A} 의 역행렬의 고유벡터는 행렬 \mathbf{A} 와 같으며 고유값만 반전되므로 \mathbf{A} 의 역행렬은 다음 식과 같다.

$$\mathbf{A}^{-1} = \sum_{j=0}^{N-1} \lambda_j^{-1} |e_j\rangle \langle e_j|$$

또한 $|b\rangle$ 는 행렬 \mathbf{A} 의 고유 기저 $\{|e_i\rangle\}$ 의 선형 결합으로 나타낼 수 있다.

$$|b\rangle = \sum_{j=0}^{N-1} b_j |e_j\rangle$$

그러므로 선형 방정식의 해는 아래와 같다.

$$|x\rangle = \mathbf{A}^{-1} |b\rangle = \sum_{j=0}^{N-1} \lambda_j^{-1} b_j |e_j\rangle$$

III. HHL 알고리즘의 회로

HHL 알고리즘의 회로는 그림 1과 같다. 크게 4개의 과정으로 나뉘며 각각의 과정은 초기값 준비, 양자 위상 추정, 고유값 전도, 복원 및 측정을 수행한다.

첫 번째 과정은 유니터리 게이트를 사용하여 양자 상태 $|b\rangle$ 를 만든다. 두 번째 과정은 양자 위상 추정 알고리즘을 사용하여 행렬 \mathbf{A} 의 고유값을 추출한다. 이때 제어 연산자 (controlled operator)에 사용하는 연산자 U 는 다음 식과 같다.

$$U = e^{i\mathbf{A}(2\pi)} := \sum_{j=0}^{N-1} e^{i\lambda_j(2\pi)} |e_j\rangle\langle e_j|$$

양자 위상 추정 알고리즘을 수행한 이후 양자 상태는 아래와 같다.

$$\sum_{j=0}^{N-1} b_j |\tilde{\lambda}_j\rangle_{n_q} |e_j\rangle_{n_b}$$

이때 $\tilde{\lambda}_j$ 는 λ_j 의 n_q 비트 이진 표현 (bit binary representation)이다. 세 번째 과정인 고유값 전도는 양자 상태의 진폭에 고유값의 정보를 전도하기 위한 과정으로 추가적인 큐비트를 사용하여 제어 회전 변환을 취하며 이후 양자 상태는 다음 식과 같다.

$$\sum_{j=0}^{N-1} b_j |\tilde{\lambda}_j\rangle_{n_q} |e_j\rangle_{n_b} \left(\sqrt{1 - \left(\frac{c}{\tilde{\lambda}_j}\right)^2} |0\rangle + \frac{c}{\tilde{\lambda}_j} |1\rangle \right)$$

이때 c 는 회전 변환 상수이다. 마지막으로 양자 위상 추정의 역변환을 사용하여 고유값을 추출하였던 큐비트를 원래의 상태로 변환시킨 이후 나머지 큐비트를 측정한다. 만약 세 번째 과정에서 사용한 추가적인 큐비트의 측정값이 1이라면 나머지 큐비트의 상태는 다음식과 같다.

$$\sum_{j=0}^{N-1} \frac{b_j}{\tilde{\lambda}_j} |0\rangle_{n_q} |e_j\rangle_{n_b}$$

추가적으로 n_b 개의 큐비트의 측정을 통해 진폭 값을 추정하고 최종적으로 선형 방정식의 해 \mathbf{x} 를 구한다.

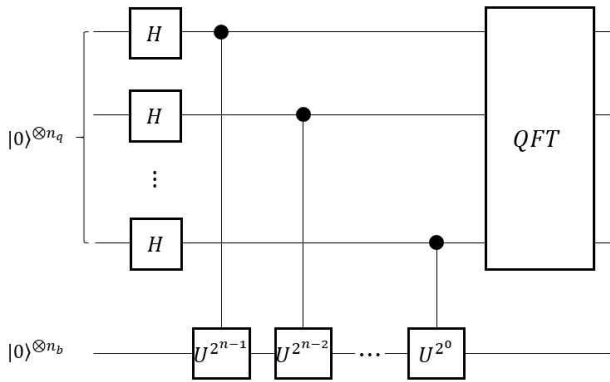


그림 1. 양자 위상 추정의 회로도

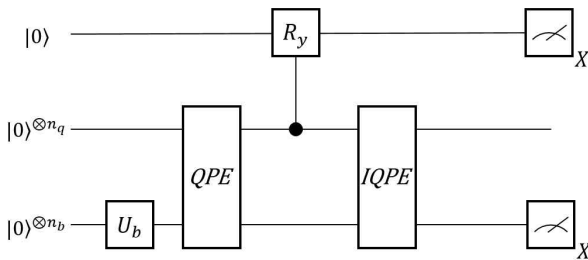


그림 2. 양자 역행렬 알고리즘의 회로도

IV. 비-허미시안 행렬을 위한 HHL 알고리즘

$N \times N$ 행렬 \mathbf{A} 가 비-허미시안 행렬일 때는 행렬 \mathbf{A} 를 사용하여 $2N \times 2N$ 허미시안 행렬 \mathbf{H} 를 구성하고 벡터 \mathbf{x} 와 \mathbf{b} 를 사용하여 \mathbf{y} 와 \mathbf{c} 를 구성한다.

$$\mathbf{H} = \begin{pmatrix} \mathbf{0}_{N \times N} & \mathbf{A}_{N \times N} \\ \mathbf{A}_{N \times N}^\dagger & \mathbf{0}_{N \times N} \end{pmatrix}$$

$$\mathbf{y} = \begin{pmatrix} \mathbf{0}_{N \times 1} \\ \mathbf{x}_{N \times 1} \end{pmatrix}, \quad \mathbf{c} = \begin{pmatrix} \mathbf{b}_{N \times 1} \\ \mathbf{0}_{N \times 1} \end{pmatrix}$$

새로운 선형 방정식 $\mathbf{H}\mathbf{y} = \mathbf{c}$ 가 형성되고 해 \mathbf{y} 를 구하면 우리는 해 \mathbf{x} 를 구할 수 있다.

예를 들어 선형 방정식 $\begin{pmatrix} 2 & -1 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ 를 생각해보자. 주어진 행렬은 비-허미시안 행렬이므로 위의 방식을 사용하여 새로운 선형 방정식

$$\begin{pmatrix} 0 & 0 & 2 & -1 \\ 0 & 0 & 1 & 4 \\ 2 & 1 & 0 & 0 \\ -1 & 4 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ 0 \\ 0 \end{pmatrix}$$

으로 변경할 수 있다. 3장에서 설명한 HHL 알고리즘을 수행한 이후 추가적인 큐비트의 측정값이 1일 때 큐비트의 상태는 다음과 같다.

$$\frac{\alpha}{8\sqrt{5}} \cdot \frac{8-\sqrt{10}}{9} |0\rangle(-|e_1\rangle + |e_2\rangle) + \frac{\beta}{8\sqrt{5}} \cdot \frac{8+\sqrt{10}}{9} |0\rangle(-|e_3\rangle + |e_4\rangle)$$

이때 α 와 β 는 각각 $\sqrt{40+12\sqrt{10}}$ 과 $\sqrt{40-12\sqrt{10}}$ 이며, $|e_j\rangle_{j=1}^4$ 는 행렬의 고유벡터이다. 마지막으로 표준 기저 $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ 로 큐비트의 상태를 정리하면 다음과 같이 나타낼 수 있다.

$$\frac{5}{\sqrt{26}} |10\rangle + \frac{1}{\sqrt{26}} |11\rangle$$

그러므로 우리는 선형 방정식의 해를 $k \cdot (0,0,5,1)$ 로 결정하고 선형 방정식에 대입하여 $k = \frac{1}{9}$ 을 찾으면서 알고리즘을 종료한다.

HHL 알고리즘은 1개의 추가적인 큐비트의 측정과 n_b 개의 큐비트의 측정으로 한 번의 결과를 얻기 위하여 총 $1+n_b$ 번의 측정을 한다. 하지만 비-허미시안 행렬을 위한 HHL 알고리즘은 n_b 개의 큐비트 중 첫 번째 큐비트의 상태는 항상 $|0\rangle$ 임을 확인할 수 있다. 우리는 이 사실을 이용하여 항상 모든 큐비트를 측정할 필요가 없다. 첫 번째 큐비트를 먼저 측정하여 0이 측정되면 오류가 발생했다고 판단할 수 있고 나머지 n_b 번의 측정을 추가로 할 필요가 없다. 즉 $1+n_b$ 번의 측정이 아닌 오직 1번의 측정만으로 오류를 판단할 수 있다. 이러한 방식을 반복하여 결과를 분석한다면 계산 복잡도를 줄일 수 있다.

V. 결론

본 논문은 비-허미시안 행렬을 위한 HHL 알고리즘을 분석하였고 선형 방정식의 구조를 이용하여 측정하는 큐비트의 개수를 줄이면서 계산 복잡도를 줄이는 방법을 제안하였다.

HHL 알고리즘의 계산 복잡도는 측정 횟수뿐만 아니라 양자 위상 추정 알고리즘에 사용하는 큐비트의 개수에도 영향을 받는다. 그러므로 두 값의 적절한 선택으로 계산 복잡도를 줄이는 방법도 생각할 수 있다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음 (IITP-2020-2018-0-01402).

참고 문헌

- [1] R. Cleve, A. Ekert, C. Macchiavello and M. Mosca, "Quantum Algorithms revisited," The Royal Society, Jan. 1998
- [2] A. W. Harrow, A. Hassidim and S. Lloyd, "Quantum Algorithm for Solving Linear Systems of Equations," Quantum Physics, Sep. 2009