Grover algorithm을 이용한 최솟값 찾기 분석 및 회로 구현

김정민(고려대학교), 허준(고려대학교)*
jmcaptain@korea.ac.kr, *junheo@korea.ac.kr

Designing a Minimum Searching circuit using Grover algorithm

Kim Jung Min, *Heo Jun(Korea Univ.)

요 약

본 논문에서는 기존의 Grover algorithm을 이용하여 Christopher Dürr과 Peter Høyer가 고안해낸 최소값 찾기 알고리즘을 분석하고 IBM Q를 이용하여 실제적인 회로 모델을 구상하였다. 양자 게이트들을 활용하여 3-qubit Grover algorithm을 구상하여 더 작은 state를 도출하는 데에 성공했다.

Ⅰ. 서 론

양자통신기술이 기존 디지털 기술을 이을 차세대 기술로 각광받고 있다. 디지털 컴퓨터에 사용되는 알고리즘의 단점을 보완한 양자 알고리즘이 개발되고 있고 그 중 하나가 검색 알고리즘인 Grover algorithm 이다. 1996 년 Christopher Dürr 과 Peter Høyer 이 Grover algorithm 을 이용하여 N 개의 데이터 값 중 최소값을 찾는 알고리즘을 구상하였다.[1] 본 논문에서는 위 알고리즘을 실제로 설계하여 시뮬레이션을 수행하였다.

Ⅱ. 본 론

Grover algorithm에 대해서 알아본 후 이를 이용하여 최솟값 알고리즘을 수행하는 양자 회로를 설계하고, 시뮬레이션을 수행하여 설계한 회로를 분석한다.

A. Grover Algorithm

Grover algorithm은 $N=2^n$ (n은 qubit의 수)개의 임의의 데이터 값 중 원하는 값을 도출해낼 수 있는 양자 알고리즘이다.[2] 작동원리는 모든 qubit을 중첩시켜준 후, Oracle function을 이용하여 원하는 state의 위상을 반전시켜준다. 반전시킨 state의 크기를 증폭시켜주기 위해서 모든 state의 평균에 대하여 반전시킨다. 앞서 설명한 과정을 $\sqrt{N}$번 반복하면 원하는 값의 크기를 극대화시키고 오차율을 줄임으로써 원하는 값을 도출할 수 있다.

위 설명은 그림 1과 같이 표현된다.

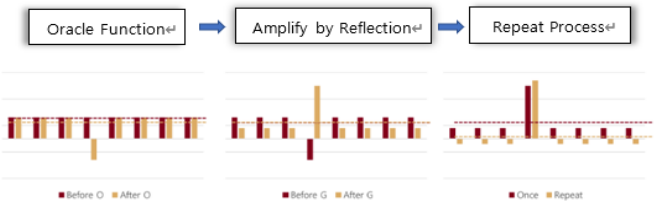

그림 1. Grover Algorithm 개요도

B. 최소값 찾기 알고리즘

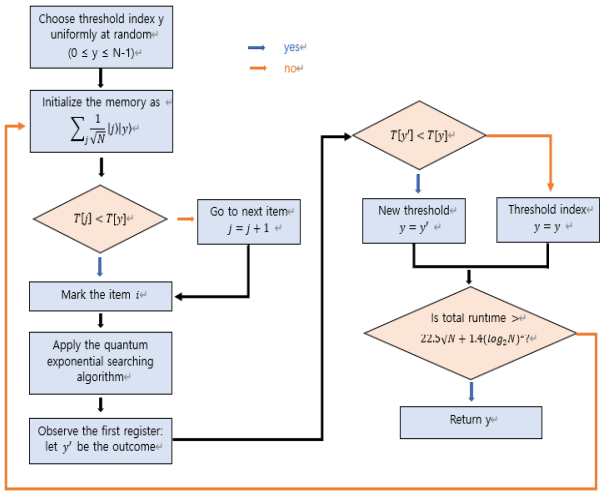

그림 2. 최소값 찾기 알고리즘의 블럭다이어그램

1996년 C.Dürr이 고안한 최소값 찾기 알고리즘은 그림 2와 같이 $T(y)$(threshold)에 초기값보다 더 작은 y의 값을 넣어주는 과정을 반복하며 최소값을 찾는 알고리즘이다.

Classical algorithm을 이용한다면 O(N)번의 시도로 최소값을 구해야하지만 위의 알고리즘을 이용한다면 $22.5\sqrt{N}+1.4(log_2N)^2$ 번만으로 최소값을 도출해낼 수 있다[3].

C. 최소값 찾기 알고리즘 회로 설계 with IBM Q

Threshold를 $|011\rangle$로 설정하여 $|010\rangle, |001\rangle, |000\rangle$의 state를 분별하는 Grover algorithm을 적용 후 threshold를 $|010\rangle, |001\rangle$로 바꾸어 위 과정을 한번 더 반복하는 회로를 설계하였다. 여기서 c bit는 6 qubit으로 구성되는 레지스터이다.

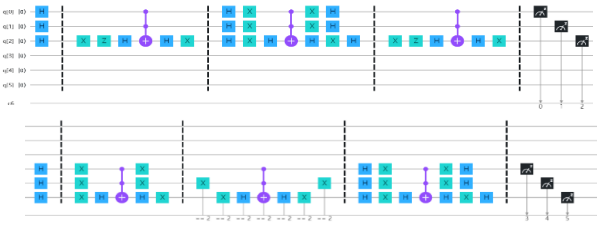

그림 3. IBM Q를 이용하여 설계한 알고리즘

길이상 둘로 나누었지만 두 회로는 연결되어 있다. 그림 3의 회로 앞부분은 6 qubit 중 오른쪽의 상위(회로상) 3 qubit에 Grover algorithm을 적용한다. $|010\rangle, |001\rangle, |000\rangle$를 분별해내고 이 중 하나의 값을 다음 threshold로 설정한다. 나온 state 결과를 c 비트에 저장 후 다음 세 qubit을 이용하여 6 qubit중 왼쪽에 해당하는 하위 세 비트에 대하여 Grover algorithm을 적용한다. 최종 $|000\rangle$을 얻는 것이 목표이기 때문에 그에 맞는 oracle 함수를 적용하고 두번째 threshold가 $|010\rangle$일 때 $|001\rangle$을 찾아내는 oracle 함수를 추가하였다.

D. 결과 분석 및 고찰

IBM Q를 이용하여 1024 shot을 수행한 결과, 하위비트가 000이 나오는 결과값의 확률을 합하면 70.898%이다. $|001010\rangle$의 확률은 13.867%로 아주 크게 나왔다. 최종결과가 001이 나오는 확률이 아주 크게 나왔다는 것이기 때문에 추가로 3 qubit을 넣어 이 세 qubit에 $|000\rangle$ 을 도출하는 Grover algorithm을 넣는 방법을 시도해보았다.

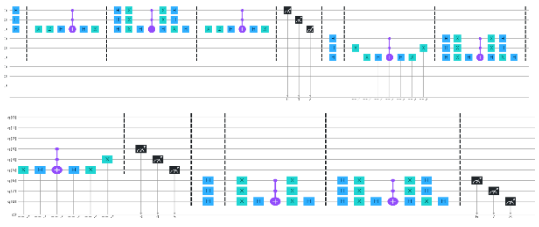

그림 4. 회로에 세 qubit을 추가하여 설계한 알고리즘

세 qubit q[6], q[7], q[8]를 추가하여 설계한 알고리즘이다. C bit를 9 qubit으로 설정 후 q[3], q[4], q[5]에 Grover algorithm을 적용하는 과정에서 마지막에 oracle function을 넣어주고 회로상 하위 세 qubit에 $|000\rangle$을 도출하는 Grover algorithm을 적용하였다.

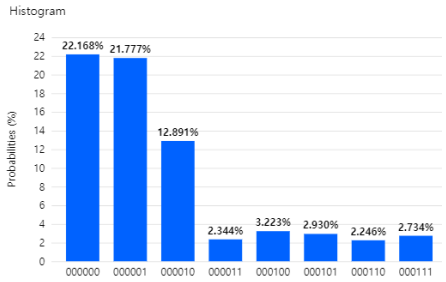

그림 5. 그림 3 회로의 1024 shots 시뮬레이션 결과

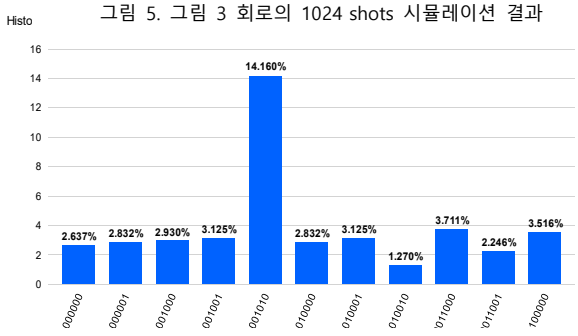

그림 6. 그림 4 회로의 1024 shots 시뮬레이션 결과

두 시뮬레이션을 비교해본 결과, 그림 5에서는 70.898%, 그림 6에서는 77.055%의 성공률을 보였다. 최소값 알고리즘에서 요구하는 총 시도횟수는 $22.5\sqrt{N}+1.4(log_2N)^2$번, 즉 3 qubit일 때 76번이다. 이 이론적 숫자에 근접할수록 높은 성공률을 보임을 알 수 있다.

Ⅲ. 결론

본 논문에서는 양자 최솟값 찾기 알고리즘을 설계하고 시뮬레이션을 수행해 77.055% 성공률을 보이는 것을 확인하였다. 또한, 시도횟수가 $22.5\sqrt{N}+1.4(log_2N)^2$번에 가까워질수록 최소값이 성공적으로 나올 확률이 증가한다는 것을 확인하였다.

ACKNOWLEDGEMENT

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 한국 연구재단의 지원을 받아 수행된 연구임 (No. 2019R1A2C2010061)

참 고 문 헌

[1] Christopher Dürr & Peter Hoyer"A quantum algorithm for finding the minimum", arXiv:quant-ph/9607014, 1996

[2] L.K.Grover, "A fast quantum mechanical algorithm for database search", Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, 1996

[3] Binam Bajracharya "Quantum Advantages Quantum Algorithm for Finding the Minimum",Lake Forest College, 2019