IBM Q를 이용한 논리 게이트 기반 양자 곱셈기 구현

조윤호(고려대학교) 허준(고려대학교)
chyn7@naver.com junheo@korea.ac.kr

Realization of Quantum Multiplier based on Logic Gate

Cho Yoon Ho(Korea Univ.)

요 약

본 논문에서는 IBM Q 를 이용한 양자 곱셈기를 구현하였다. 기존의 디지털 논리 게이트 기반 곱셈기 회로에 사용되는 게이트를 양자 게이트로 표현하여 곱셈기를 구현하였다. 곱셈기를 구성하는데 있어서 필요한 큐비트의 개수는 $2N^2+10N$개이고 필요한 logic gate 의 수는 $18N^2-27N$개이다.

Ⅰ. 서 론

양자 컴퓨터는 고전 컴퓨터처럼 0 과 1 이 각 실행 때마다 구분되는 비트를 사용하는 것이 아니라 0 과 1 이 동시에 공존 할 수 있는 큐비트를 사용한다는 점에서 강점을 갖는다. 양자 컴퓨터는 이처럼 양자 얽힘, 중첩 현상 등 양자적 특성을 이용하여 암호해독 또는 300 자리 정수 소인수분해 같이 기존의 컴퓨터로서는 해결이 불가능해 보였던 일들을 해결할 수 있는 가능성을 보였기에 큰 관심을 끌었다.[1] 본 논문에서는 IBM Q를 이용한 양자 곱셈기를 구현해보았다.

Ⅱ. 본 론

N x N bit 곱셈기는 여러 개의 가산기의 합으로 이루어진다. 가산기란 덧셈 연산을 수행하는 회로로서 산술 논리 장치와 더불어 아니라 주소 값, 테이블 색인 등을 더하는 프로세서의 한 부분으로 사용되고 있다. 이때 N x N bit 곱셈기를 이루는 가산기에는 전가산기(N≥3)와 반가산기가 있다.[2]

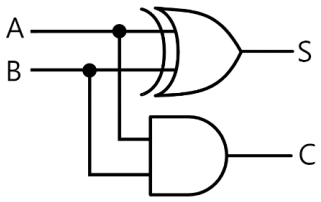


그림 1. 반가산기 회로도

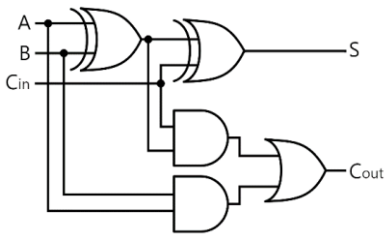


그림 2. 전가산기 회로도

그림 1 은 반가산기로 이진수의 한 자리수를 연산하고, 자리 올림수는 자리 올림수 출력에 따라 출력하는 회로로서 AND, OR 그리고 NOT 게이트로 구성 가능한 회로이다. 더 간단히 표현하면, 반가산기는 1 개의 XOR 게이트와 1 개의 AND 게이트로 이루어진다. 또, 그림 2 는 전가산기로 반가산기와 달리 이진수의 한 자릿수를 연산하고, 하위의 자리 올림수 입력을 포함하여 출력한다. 하위의 자리 올림수 출력을 상위의 자리 올림수 입력에 연결함으로서 임의의 자릿수의 이진수 덧셈이 가능해진다. 또한, 하나의 전가산기는 두 개의 반가산기와 하나의 OR 게이트로 이루어진다.

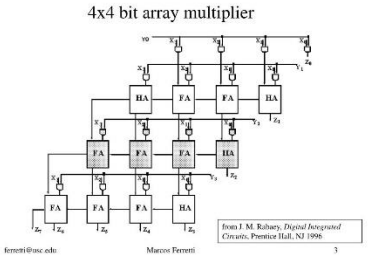


그림 3. 4x4 곱셈기 구성도

그림 3 은 4x4 곱셈기의 구성도이다. 곱셈기는 디지털 회로에서 두 이진값을 곱하는 목적의 하드웨어 회로이다. 다양한 컴퓨터 산술 기술은 디지털 곱셈을 수행하는 데 사용할 수 있으며 대부분의 기술은 계산된 "부분적 곱"의 집합을 포함하고, 그러면 부분적 곱은 동시에 합계된다.[3]

A. 양자 게이트의 표현

디지털 회로에서 bit 를 이용한 논리 게이트가 이용되는 것과 같이, 양자회로에서는 qubit 을 이용한 양자 게이트가 이용된다. 아래의 양자 게이트들은 곱셈기를 구현하는데 있어서 사용되는 양자 게이트들이다.

① X 게이트

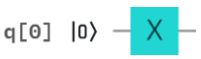


그림 4. X 게이트

X 게이트는 디지털 회로에서 NOT 게이트와 같은 역할을 한다. 즉, |0⟩은 |1⟩로 |1⟩은 |0⟩으로 bit flip 을 하는 게이트이다

② CX 게이트

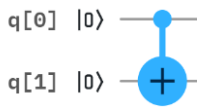


그림 5. CX 게이트

CX 게이트에는 입력이 control qubit 와 target qubit 있다. Control qubit 이 |1⟩일 경우에만 target qubit 이 반전된다.

③ CCX 게이트

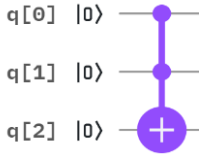


그림 6. CCX 게이트

CCX 게이트는 q[0]와 q[1]이 모두 |1⟩일 때만 q[2]가 반전되는 게이트이다.

B. 논리 게이트의 양자 게이트화

곱셈기는 full adder 와 half adder 로 이루어져 있고, full adder 와 half adder 는 AND, OR 그리고 NOT 게이트 또는 XOR 게이트와 AND 게이트로 구성이 가능하다. 앞에서 살펴본 양자 게이트로 AND, OR 그리고 XOR 게이트를 구현하였다.

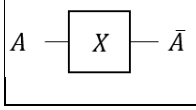
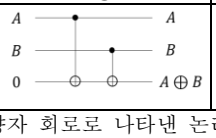
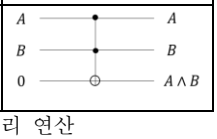
$\bar{A}$	$A \oplus B$	$A \wedge B$
		

표 1. 양자 회로로 나타낸 논리 연산

또한, OR gate 는 다음과 같이 구현할 수 있다.

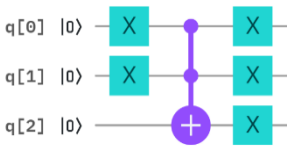


그림 7. OR 양자 gate

OR 게이트는 위의 그림과 같이 CCX 게이트와 X 게이트의 조합으로 만들 수 있다.

C. 양자 곱셈기의 구현

본 논문에서는 두 가지 방식으로 양자 곱셈기를 구현해보았다. 첫 번째 방식은 임시 저장 장소로 사용되는 temp qubit 을 재사용하지 않은 방식이고 두번째 방식은 필요로 하는 qubit 의 수를 최소화 하기 위하여 temp qubit 을 재사용한 방식이다. 두 가지 방식 중 2 번 째 방식으로 IBM Q 를 이용하여 시뮬레이션을 수행하였다.

구현방식 1. 양자 곱셈기를 구현하면서 temp qubit 을 재사용하지 않고 필요할 때마다 새로운 temp qubit 을 지정하여 회로를 구현하였다. 이 방식은 temp qubit 을 재사용하기 위하여 초기화 하는 과정이 필요 없기 때문에 필요한 게이트 수가 줄어든다는 장점이 있다. <그림 8.> 에서 볼 수 있는 바와 같이 3x3 bit 곱셈기를 구현하는데 24 개의 temp qubit 이 사용되었다. 그러나 양자 알고리즘을 구현하는데 있어서 큐비트는 무한히 사용할 수 있는 자원이 아닌 귀한 자원이기 때문에 두 번째 방식에서는 사용되는 qubit 의 수를 최소화할 수 있는 방식으로 회로를 구현해보았다.

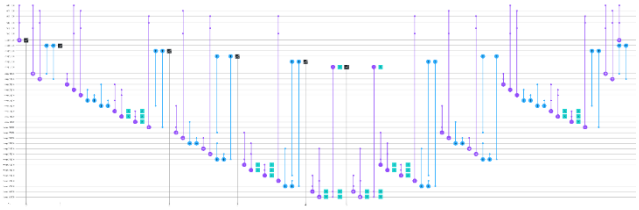


그림 8. temp qubit 을 재사용하지 않은 곱셈기

구현 방식 2. 두번째 방식에서는 <그림 3.>에 나와있는 회로를 바탕으로 논리 게이트의 위치에 같은 역할을 하는 양자 게이트를 넣어서 구현하였고 시뮬레이션까지 수행하였다..

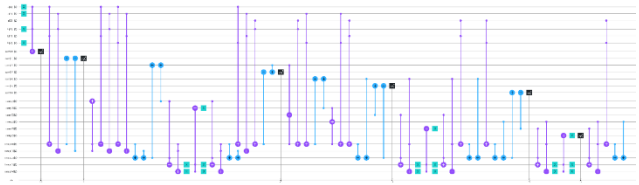


그림 8. 3x3 unsigned binary multiplier(011 x 101) 회로도

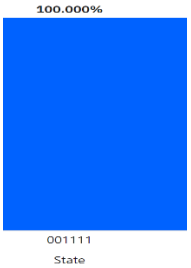


그림 9. 011 x101 에 대한 시뮬레이션 결과

Ⅲ. 결론

본 논문에서는 기본적인 논리 게이트들을 양자 게이트로 구현해보았다. 기본적인 양자 게이트를 사용하여 Multiplier 를 구현하고 IBM Q 를 통해 시뮬레이션을 수행하였다. 본 논문에서 구현한 곱셈기는 N 의 값이 커질수록 필요한 qubit 의 수와 gate 의 수가 급격히 증가하므로 실제 양자 컴퓨터에서 사용되기 위해서는 회로 개선이 필요하다.

ACKNOWLEDGMENT

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

참 고 문 헌

[1] 양자 컴퓨터. [Online]. Available: https://ko.wikipedia.org/wiki/%EC%96%91%EC%9E%90_%EC%BB%B4%ED%93%A8%ED%84%B0

[2] Adder. [Online]. Available: https://ko.wikipedia.org/wiki/%EA%B0%80%EC%82%B0%EA%B8%B0

[3] Multiplier [Online]. Available: https://ko.wikipedia.org/wiki/%EA%B3%B1%EC%85%88%EA%B8%B0

[4] The Classical and Quantum Information Theory An

Introduction for the Telecom Scientist