

# Quantum Computing Performance Analysis of the Ground-State Estimation Problem

Byung-Soo Choi<sup>†</sup>

*Electronics and Telecommunication Research Institute, 218, Gajeong-ro, Yuseong-gu, Daejeon 34129, Korea*

(Received February 18, 2018; Revised April 1, 2018; Accepted April 2, 2018)

As the quantum volume increases, we are about to use quantum computers for real applications. Therefore, it is necessary to investigate how much quantum-computational gain is achievable in the near future. In this work, we analyze a fault-tolerant quantum computing method for near-term applications such as the ground-state estimation problem. Based on quantitative analysis, we find that it is still necessary to improve the current fault-tolerant quantum computing. This work also discusses which parts should be improved to improve quantum computing performance.

Keywords: Quantum computer, Quantum simulation, Chemistry, Fault-tolerant quantum computation

OCIS codes: (270.5585) Quantum information and processing; (270.0270) Quantum optics; (270.5565) Quantum communications

## 기저상태계산 문제에 대한 양자컴퓨팅의 성능 분석

최병수<sup>†</sup>

한국전자통신연구원 초연결통신연구소 초연결원천연구본부 양자창의연구실  
Ⓣ 34129 대전광역시 유성구 가정로 218

(2018년 2월 18일 받음, 2018년 4월 1일 수정본 받음, 2018년 4월 2일 게재 확정)

최근 양자프로세서와 관련한 연구개발이 본격화되면서 실제 수행가능 한 양자계산량도 계속 증가하고 있다. 이에 양자컴퓨팅은 본격적으로 활용화단계로 진입하고 있다고 볼 수 있다. 다만 아직은 큰 규모의 양자컴퓨팅이 가능하지 않기 때문에 작은 규모의 문제이지만 고전컴퓨팅으로는 해결하기 힘들고, 양자컴퓨팅으로는 효과적으로 계산할 수 있는 문제를 대상으로 하고 있다. 본 연구에서는 이와 관련하여 양자컴퓨터를 이용한 작은 크기의 양자시뮬레이션분야의 실질적인 계산성능에 대한 정량적인 분석 결과를 보고한다. 분석결과 현재까지의 결합허용 기반 양자컴퓨팅은 양자계산성능의 측면에서 다양한 문제점을 갖고 있음을 확인하였다. 본 연구에서는 이와 관련하여 향후 수행해야 할 연구개발 내용을 정리하였다.

Keywords: 양자컴퓨터, 양자시뮬레이션, 화학, 결합허용양자컴퓨팅

OCIS codes: (270.5585) Quantum information and processing; (270.0270) Quantum optics; (270.5565) Quantum communications

### I. 서 론

양자컴퓨팅은 양자역학적 특성을 이용하여 기존의 비트기반 컴퓨팅이 수행하지 못하는 연산을 효율적으로 수행할 수 있다. 이는 양자정보가 갖는 중첩성, 간섭성, 얽힘성 등을 이용하여 연산과정에서 요구되는 정보표현공간과 연산량을 매우 효율적으로 처리하기 때문이다. 예를 들어서, 중첩성을 사용하게 되면, 하나의 큐비트를 이용하여 두 가지 비트 상태를 동시에 표현하는 강점을 가지며, 이를 통해서 연산에서 다루는 상태공간을 지수적으로 압축하여 표현할 수 있다(양자정보의 메모리 압축효과). 또한, 간섭성을 이용하여 기저상태 값들 사이에서의 연산기능을 구현할 수 있다(양자연산기능.

연산의 선형성). 마지막으로, 얽힘성을 이용하여 큐비트들이 연산과정에서의 상태공간을 모두 표현할 수 있도록 해준다(압축된 정보공간에서 양자연산기능, 따라서 통신량 감소 효과). 이에 따라서 양자컴퓨팅은 기존 비트기반 컴퓨팅이 메모리, 연산노드, 통신량 등을 많이 써야 하는 상황에서 매우 효율적인 연산이 가능하도록 한다. 그러므로 양자컴퓨팅은 연산 과정에서 다루어야 하는 상태공간 혹은 경우의 수가 많은 상황에서 전역적인 특성을 분석하거나 전역적 상황에서의 특정값을 찾아내는 문제에 적합하다고 볼 수 있다. 이에 따라서 조합최적화나 주어진 함수의 전역적 특성을 분석하는데 효과적이다.

<sup>†</sup>E-mail: bschoi3@etri.re.kr, ORCID: 0000-0002-4989-9622

Color versions of one or more of the figures in this paper are available online.

이러한 양자컴퓨팅을 구현하기 위해서 요구되는 양자프로세서에서는 최근 구현되는 큐비트수가 매우 빠르게 증가하고 있다. 어닐링 머신을 제외하고도 범용적 양자프로세서에서 구현되는 큐비트수는 매년 가파르게 증가하고 있다. IBM(실제 양자프로세서 및 가상머신 기반), Rigetti(양자프로세서 및 가상머신 기반), Microsoft(가상머신 기반)등은 이와 관련하여 양자컴퓨팅을 체험 혹은 실제 구동할 수 있는 클라우드를 제공하여 다양한 연구개발을 촉발하고 있다. 최근에는 Intel이 양자프로세서를 본격적으로 구현하기 시작하였다. 더불어 Google에서는 최근 72개의 큐비트를 갖는 양자프로세서를 통해서 양자적 계산의 우수성을 입증하는 단계의 실험을 진행하고 있다.

이에 따라서 현재 시점에서 가장 중요한 질문은 양자컴퓨팅이 어떠한 문제, 특히 실용적으로 활용가치가 높으면서 고전적으로 해결하기 힘들지만 양자적으로는 쉽게 해결하는 문제를 찾고, 그것을 실제로 구현하는 것이라 할 수 있다. 이러한 기준으로 볼 때 현재 가장 주목받는 것은 양자컴퓨터를 이용한 양자역학적 동역학의 시뮬레이션(전산모사) 분야이다. 본 연구에서는 양자컴퓨터를 이용한 양자역학적 동역학의 전산모사를 양자시뮬레이션으로 정의하고 있다. 참고로, 호스트 양자시스템을 이용하여 게이트 양자시스템을 모사하는 것은 양자에뮬레이션으로 구분되지만, 본 연구에서는 다루지 않는다. 양자시뮬레이션은 양자상태의 동역학적 변화를 계산하는 과정의 복잡도가 중요한데, 일반적으로 고전적으로는 지수적 복잡도를 갖기 때문에 제한된 크기의 시스템만 계산 가능하다. 반면에, 양자시뮬레이션은 다항적 복잡도를 가질 수 있기 때문에 지금까지 분석하지 못하였던 더 큰 양자시스템을 시뮬레이션 할 수 있다. 다만, 모든 양자역학적 동역학이 다항적으로 양자계산되는 것은 아님을 주지해야 한다. 양자시뮬레이션의 대상이 되는 양자역학적 현상들 중에는 현재 중요하게 연구되고 있는 고온초전도 현상 등과 같은 과학적, 산업적으로 중요한 대상의 문제들을 포함하고 있다. 그리고, 이러한 수준의 문제는 상대적으로 작은 수의 큐비트수를 요구하기 때문에, 현재 및 가까운 시일내에 구현될 것으로 보이는 양자컴퓨터 시스템의 실질적인 활용분야로 적합하다<sup>1)</sup>.

본 연구에서는 이러한 양자시뮬레이션과 관련하여 현재까지 제안된 결함허용 기반 양자컴퓨팅 구현 방법론의 계산성능 분석결과를 소개한다. 분석과정은 1단계로 어셈블리 코드 수준에서의 이상적 성능을 분석한다. 이는 수학적 표현을 양자컴퓨터가 구현 가능한 게이트 단위로 분해하는 이론적 수준으로써, 다양한 양자시뮬레이션 알고리즘 분야에서 고려되는 복잡도이다. 이후 2단계로 오류보정-결함허용이 적용된 후의 성능을 분석한다. 이는 양자하드웨어의 제공 신뢰도와 양자시뮬레이션 알고리즘의 요구 신뢰도 사이에서의 간극을 오류보정과 이에 따른 결함허용적 구현방법으로 제거하기 위한 과정이다. 전반적으로 이 과정에서 추가적 비용이 크게 발생한다. 마지막으로 실제 하드웨어 수준에서의 합성에 따른 계산성능을 분석한다. 이는 실제 구현될 양자프로세서에서 양자회로가 어떻게 동작하는지에 따라서 큐비트동 과정

에서의 시간지연과 양자회로의 동작 순서 변화 현상이 발생한다. 이러한 변화는 양자컴퓨팅의 동작시간에도 영향을 끼친다. 이와 유사한 선행연구로는 참고문헌 [9]에서 언급한 과정이다. 다만, 본 연구는 참고문헌 [9]에 비해서 조금 더 다양한 상황 및 자세한 기술적 내용을 고려하는데, 컴파일 과정에서의 최신 분해과정의 적용, 오류보정코드, 양자알고리즘부터 양자회로 수준까지의 오버헤드 증가 과정, 논리적 수준에서의 스케줄링 등이 추가되었다. 대상문제의 상황을 토대로 분석한 결과, 현재의 양자하드웨어 기술의 낮은 성능과 오류보정-결함허용방식에서의 오버헤드 문제로 인하여 양자컴퓨팅의 계산성능이 이론적 수준에 비해서 크게 감소하는 것을 확인하였다. 양자컴퓨팅의 기본적인 목적이 높은 계산성능을 확보하는 것인 만큼, 이러한 분석을 통해서 드러난 다양한 문제점을 지속적으로 해결하는 것이 매우 중요함을 확인하였다.

본 논문은 다음과 같이 구성되었다. 2장에서는 양자시뮬레이션 문제를 설명한다. 3장에서는 본 연구의 대상 양자동역학 해밀토니언, 기저상태 예측 알고리즘을 소개한다. 4장에서는 결함허용 양자컴퓨팅의 적용에 따른 양자컴퓨팅의 기대성능 분석결과를 제시한다. 5장에서는 고성능 양자컴퓨팅을 위한 향후 해결해야 할 문제 등을 설명한다. 6장에서는 본 논문을 마무리한다.

## II. 양자시뮬레이션 개요

양자시뮬레이션은 주어진 초기 양자상태  $|\psi_0\rangle$ 를 대상으로 하여, 그 양자상태에 적용될 양자동역학적인(시간 독립적) 연산자  $H$ 를 특정한 시간  $t$ 만큼 적용한 후의 양자상태  $|\psi_t\rangle$ 를 찾아내는 것이다. 이때 양자동역학을 표현하는 슈뢰딩거 방정식은 다음과 같은 형식을 갖는다<sup>2)</sup>.

$$i\hbar \frac{\partial |\psi\rangle}{\partial t} = H |\psi\rangle \quad (1)$$

이러한 슈뢰딩거 방정식에 대한 미분방정식을 풀면, 다음과 같은 행렬지수식이 유도된다.

$$|\psi_t\rangle = e^{-iHt/\hbar} |\psi_0\rangle = U |\psi_0\rangle \quad (2)$$

이제, 이렇게 구해진 행렬지수식을 대상으로 하여 주어진 초기 양자상태를 대상으로 하여 연산을 수행하면 시간  $t$ 만큼 지난 후의 최종 양자상태  $|\psi_t\rangle$ 를 계산할 수 있다. 이때, 사용되는 해밀토니언은 대상 양자시스템의 특성에 따라서 다르다. 슈뢰딩거 방정식의 해를 표현하는 식 (2)는 다음과 같이 Taylor시리즈를 이용하여 계산할 수 있다.

$$e^{-iHt/\hbar} \equiv I - i \frac{Ht}{\hbar} - \frac{1}{2i} \left( \frac{Ht}{\hbar} \right)^2 + \frac{1}{3i} \left( \frac{Ht}{\hbar} \right)^3 + \frac{1}{4i} \left( \frac{Ht}{\hbar} \right)^4 \dots \quad (3)$$

문제가 되는 것은 이때 사용되는  $H$ 가 앞서 언급한 것과 같이 양자수  $n$ 에 따라서  $2^n \times 2^n$ 로 증가하기 때문에 고전적 계산에서는 지수적 상태 표현 및 행렬이 요구된다. 이에 따라서 고전적 방법을 이용하여 계산할 수 있는 대상 양자시스템의 크기가 매우 제한된다. 반면에, 양자컴퓨팅을 이용한 전산모사(양자시뮬레이션)에서는 특정한  $H$ 의 경우, 이러한 양자수  $n$ 에 비례하는 수준에서의 큐비트를 사용하고,  $H$ 는 양자게이트 수준에서 분해하여 적용하면 상대적으로 쉽게 시뮬레이션을 수행할 수 있다. 참고로, 모든  $H$ 에 대하여 효과적으로 양자시뮬레이션이 되는 것은 아님을 주의하여야 한다. 이는 대상  $H$ 를 양자게이트로 분해한 후의 복잡도가 항상 다항적이지는 않기 때문이다.

본 연구에서 대상으로 하는 양자분자는 Iron-Sulfur이며, 이에 해당하는 해밀토니언은 다음과 같다. 이 분자는 전자를 전달하는데 주로 사용되며, 특히 광합성 등과 같은 과정에서 사용된다.

$$H = \sum_{p,q} h_{p,q} a_p^\dagger a_q + \frac{1}{2} \sum_{p,q,r,s} h_{p,q,r,s} a_p^\dagger a_q^\dagger a_r a_s \quad (4)$$

### III. 기저상태 찾기 알고리즘

양자시스템의 기저상태를 찾는 알고리즘은 특정한 초기값, 해당 양자시스템의 행렬지수에 해당하는  $U$ 의 지수곱, 그리고 위상추출부분으로 구성되어 있다. 기본적인 아이디어는 특정한 초기값을 대상으로 하고, 그것에 대하여 행렬지수에 해당하는  $U$ 의 모든 지수곱을 인가하도록 한다. 그런 다음에, 그 값이 갖는 위상의 주기값을 관측하고, 그 주기값으로부터 최소에너지의 값을 유추하는 방식이다. 관련한 양자회로의 개념도는 그림 1과 같다<sup>[3]</sup>. 그림에서  $M$ 은 대상 양자시스템의 크기(#Orbital의 2배)를 의미하며,  $b$ 는 기저상태의 정보에 대한 정확도를 의미한다. 또한, 그림에서  $H$ 는 중첩상태를 만드는 양자게이트를 의미하며,  $FT$ 는 양자푸리에 변환게이트를 의미한다.

$U$ 와  $|u\rangle$ 를 각각 유니터리와 그것의 고유벡터라고 하자. 이에 따라  $U|u\rangle = e^{2\pi i\theta} |u\rangle$ 이고, 이때  $\theta$ 는 위상값이다. 이제 그림 1을 그대로 적용하면, 관측된  $m$ 은  $8/\pi^2$ 의 확률로 다음과 같은 조건을 만족한다.

$$|\theta - m2^{-b}| \leq 2^{-b} \quad (5)$$

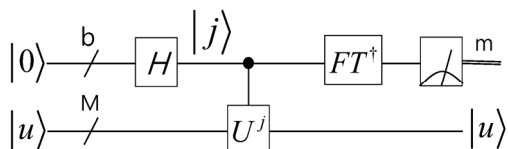


Fig. 1. Concept of quantum algorithm for ground-state estimation problem

이제 이렇게 관측된  $m$ 으로부터 기저상태를 유추하는 과정을 살펴본다.  $E_0 \in [E_{\min}, E_{\max}]$ 이 기저에너지로 가정하자. 이제  $\tau = 2\pi/\Delta E$ ,  $\Delta E = E_{\max} - E_{\min}$ , 그리고  $H$ 는 대상 양자시스템의 2차 양자화 해밀토니언이라고 하고,  $U = e^{iE_{\max}\tau} e^{-iH\tau}$ 를 정의할 수 있다. 이제 다음을 만족하는 기저상태의 파동함수  $|\Psi_0\rangle$ 가 있다고 가정한다.

$$e^{-iH\tau/h} |\Psi_0\rangle = e^{-iE_0\tau} |\Psi_0\rangle \quad (6)$$

이러한 기저상태는 다음을 만족한다.

$$U|\Psi_0\rangle = e^{2\pi i\theta} |\Psi_0\rangle, \quad \theta = \frac{\tau(E_{\max} - E_0)}{2\pi} = \frac{E_{\max} - E_0}{\Delta E} \in [0,1) \quad (7)$$

위 식으로부터 기저상태는  $E_0 = E_{\max} - \theta\Delta E$ 이다. 이제 남은 것은  $\theta$ 를 계산하는 것인데, 이는 앞선 알고리즘 수행을 통해서 관측된  $m$ 으로부터  $\theta = m/2^b$ 로 계산된 값을 사용하면,  $E_0$  근사값을 찾을 수 있다. 특히 이 과정에서  $U^j$ 를 계산하는 행렬지수과정은 Trotter분해방법을 이용하여 효과적으로 양자회로로 분해할 수 있다<sup>[2]</sup>. 이 과정에서의 모든 회로 복잡도는 다항적이다. 대상이 되는 양자시스템의 양자수 및 사용자의 요구정확도에 맞추어서 다항적 복잡도를 갖는다.

### IV. 성능 분석 결과

#### 4.1. 알고리즘의 양자회로 분해 수준 분석

일차적으로 양자알고리즘은 프로그래밍 형태로 기술되어야 하고, 이를 기계어 수준으로 변환하는 과정을 거친다. 이때 사용되는 것이 양자컴파일러이다. 양자컴파일 과정에서는 양자컴퓨터 혹은 양자프로세서가 실제로 구현하는 양자게이트의 집합으로 알고리즘이 분해된다. 본 연구에서는 결합허용 양자컴퓨팅 방식을 고려하기 때문에, 양자컴파일 과정에서 사용되는 게이트는 결합허용 양자컴퓨팅에서 주로 사용되는  $H$ ,  $T$ ,  $CNOT$ ,  $S$  게이트 등을 사용한다. 특히, 결합허용이 적용되지 않는 경우에는 단일큐비트에 대한 게이트를 직접 구현할 수 있기 때문에,  $H$ ,  $T$ ,  $S$ 등으로 분해하지 않아도 된다. 컴파일 과정 후 생성되는 회로는 양자어셈블리코드 수준이며, 일반적으로 고전컴퓨터에서 사용되는 어셈블리코드와 유사하다. 특히 양자어셈블리코드는 양자회로 수준을 의미하기 때문에, 어셈블리코드 수준에서의 해석을 통해서 양자회로 수준의 분석이 가능하다. 본 연구에서는 이를 위하여 현재 사용 가능한 양자컴파일러인 Scaffold<sup>[4]</sup>와 Quipper<sup>[5]</sup> 등을 사용하였다. 또한, 참고문헌 [9]번 이후 추가적으로 개발된 개선된 분해알고리즘등이 반영되었는데, grid-synthesis등의 방법이 적용되었다<sup>[10]</sup>. 이에 따라서 단일큐비트 게이트의 최적 분해기술이 적용되었다.

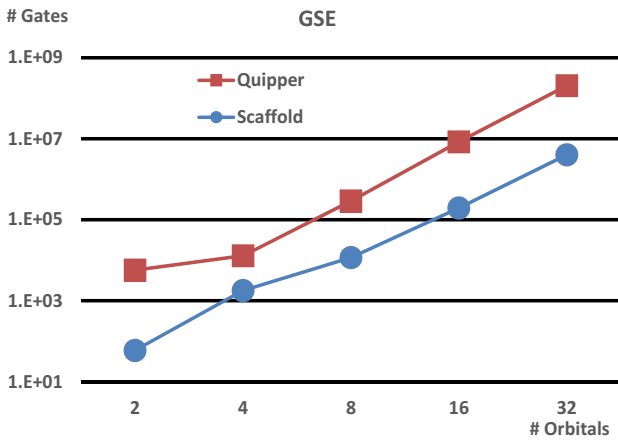


Fig. 2. Total number of gates

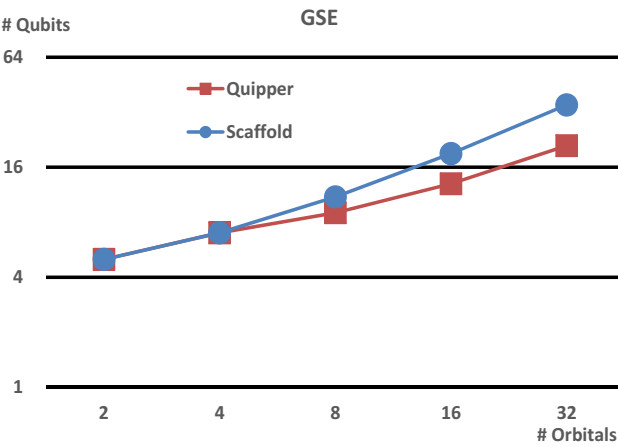


Fig. 3. Total number of qubits

컴파일 실행 후 GSE 알고리즘의 예상 성능은 다음과 같다 (그림 2, 3)<sup>[6]</sup>. 이때, 알고리즘 수준에서의 위상정확도 값  $b=10$  을 가정하였다. 문제의 크기에 해당하는 #Orbital이 2배씩 증가함에 따라서 게이트와 큐비트의 숫자 모두 2배씩 증가하는 것을 할 수 있다. 즉, #Orbital에 따라서 선형적인 복잡도 증가가 가능함을 확인할 수 있다. 이 과정에서 Scaffold의 경우 단일큐비트게이트에 대한 최적분해 알고리즘이 적용된 관계로, 게이트수가 Quipper에 비해서 작은 것을 확인할 수 있다.

#### 4.2. 오류보정-결합허용 적용 수준 분석

양자컴퓨터는 기본적으로 물리적 수준의 큐비트와 게이트를 이용하여 알고리즘수준에서의 큐비트와 게이트를 구현하는 과정이다. 이때, 알고리즘 수준에서는 큐비트와 게이트가 모두 완벽하다고 가정한다. 그러나, 양자프로세서의 큐비트와 게이트는 완벽하지 않기 때문에, 알고리즘의 연산결과는 매우 부정확할 수 있다. 이러한 문제점을 해결하기 위해서 알고리즘 수준(정확히는 어셈블리 코드 수준 혹은 양자회로수준)의 큐비트와 게이트에 대하여 오류보정코드 및 결합허용방식을 적용하여 사용자가 원하는 임의의 정확도 수준으로 높이는 작

업을 진행한다<sup>[7]</sup>. 이는 물리적 수준에서의 큐비트와 게이트가 갖는 정확도의 한계와 어셈블리 수준에서 요구하는 정확도의 수준 사이에서의 차이를 보정하는 작업이라 할 수 있다. 이러한 과정은 연산결과의 신뢰도와 양자컴퓨팅의 확장성 및 신뢰성에는 도움이 되지만, 양자컴퓨팅의 계산성 측면에서는 문제점을 야기한다. 오류보정 및 결합허용과정은 기본적으로 다수의 물리적 큐비트와 게이트를 사용하여 오류에 대한 민감도를 낮추는 과정인 만큼, 필요한 물리적 큐비트수, 게이트수와 동작시간 측면에서 필연적으로 오버헤드를 발생시킨다. 이에 따라서 오류보정-결합허용 과정에서 수반되는 오버헤드를 고려해야만 양자컴퓨팅의 실질적인 성능을 계산할 수 있다.

본 연구에서는 이와 관련하여 현재 많이 연구되고 있는 Steane코드와 Bacon-Shor코드를 사용하는 경우에서의 성능 저하현상을 분석하였다<sup>[8]</sup>. 또한, 각 코드별로 요구되는 결합허용 프로토콜을 모두 적용하는데, 논리적 큐비트를 인코딩하는 과정, 오류보정과정, 관측과정, 단순논리적 게이트구현 (transversal gate), 복잡논리적 게이트 구현(non-transversal) 프로토콜, 그리고 이 과정에서 요구되는 몇 가지 주요한 프로토콜들(magic state, CAT state distillation protocols) 등이 모두 적용되었다. 본 연구에서는 사용되는 물리적 큐비트에서의 게이트의 정확도를  $10^{-6}$ 으로 간주하였다. 한편, 양자회로 수준에서 요구하는 알고리즘 수준 게이트의 허용 오류율은  $1/(\text{#gate steps} * \text{#qubits})$ 로 할 수 있다. 또한, 오류보정코드를 반복적으로 적용하면, 논리적 게이트의 오류율은 지수적으로 작아진다. 따라서 양자회로 수준에서 요구되는 최대허용 오류율보다 작은 오류율을 갖기 위하여 오류보정과정을 반복적으로 적용해야 한다. 이렇게 반복적으로 적용하는 경우, 표 1에서와 같이 오류보정코드에 따라서 필요한 concatenation의 레벨은 달라진다. 일반적으로 Bacon-Shor코드가 효율성이 높기 때문에 상대적으로 필요한 레벨수가 낮은 편이다. 표 2에서는 이와 관련하여 필요한 큐비트수의 증가를 의미한다. 전반적으로, Bacon-Shor코드의 효율성이 높은 편이지만, 그럼에도 필요한 오버헤드가 매우 크다는 것을 알 수 있다. 이에 따라서 오류보정-결합허용 과정이 적용됨에 따른 양자컴퓨팅의 예상 연산시간은 그림 4와 같이 추가적으로 증가한다. 전반적인 시간은 대략 10~100배 이상 증가하는 것을 확인할

Table 1. Necessary level of QEC concatenation

M	2	4	8	16	32
Steane	2	2	2	2	3
Bacon-Shor	2	2	2	2	2

Table 2. Increase of total number of qubits with input size

M	2	4	8	16	32
Steane	539	637	833	1,225	14,063
Bacon-Shor	891	1,053	1,377	2,025	3,321

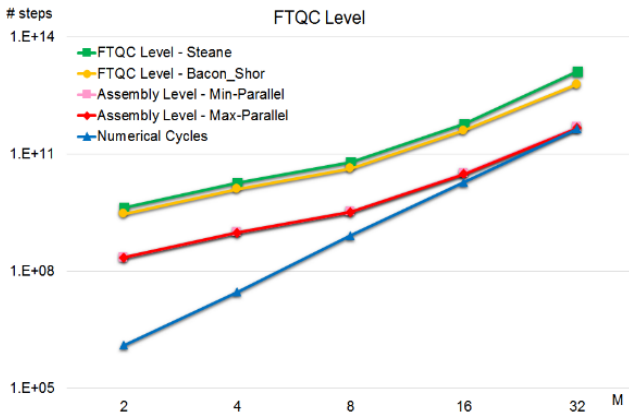


Fig. 4. Quantum computation time with fault-tolerant quantum computation methods

였다. 특히, 이 단계까지는 모두 양자게이트의 단계수를 기준으로 하고 있다.

### 4.3. 하드웨어 정보 반영 및 시스템 합성 적용 수준 분석

마지막 단계로 결함허용이 적용된 양자회로를 실제의 양자 프로세서에서 구현하는 경우에 대한 성능분석을 진행한다. 이 과정에서는, 물리적 큐비트의 물리적 제한요건에 맞추어서 추가적인 오버헤드가 발생한다. 특히, 물리적으로 떨어져 있는 큐비트들 사이에서의 CNOT게이트 구현이 요구되기 때문에, 이 과정에서 큐비트의 이동시간 및 필요한 버스 공간 등과 같은 물리적 오버헤드가 추가된다. 결과적으로, 이러한 오버헤드는 양자알고리즘의 연산시간을 증가시킨다. 특히 본 연구에서는 다양한 큐비트 기술을 대상으로 하고 있으며, 큐비트들 간의 이동과정에서의 스케줄링 등이 반영되었다는 측면에서 기존의 참고문헌 [9]에서의 특정 하드웨어, 특정 구조에 한정된 것의 한계를 벗어난다. 본 연구에서는 이러한 현상을 정량적으로 분석하기 위해서 현재까지 공개된 주요 큐비트 기술 및 그들의 성능을 토대로 물리적 배치에 따른 성능변화를 분석하였다. 특히 이 과정에서는 필요한 시스템 크기 정보까지 파악할 수 있다. 사용된 큐비트 기술은 양자점, 초전도, 이온 큐비트 기술이다. 본 연구에서는 각 기술별로 물리적 주요 기능들(초기화, 게이트 동작시간, 관측 동작시간, 정확도 등)의 값은 관련 실험결과들을 참고하였다. 다만, 특정한 한가지 시스템에서 모든 값이 최적이지 않기 때문에, 대부분인 큐비트기술에서 세부적으로 달라지는 구현방법상의 차이는 고려하지 않았다. 본 연구에서는 따라서 각 대분류 기술별로 가장 좋은 물리적 성능값을 반영하였다고 볼 수 있다.

이러한 상황을 고려하여 실제 시스템 수준에서의 실행시간 분석결과를 살펴보면, M = 80인 경우 Bacon-Shor코드를 사용하는 경우 대략적으로  $10^{16}$  초 정도가 요구된다(그림 5). 사실, 이정도 수준이면 상당히 오랜 시간이 걸리는 것으로 분석될 수 있다. 물리적 큐비트의 수도  $10^{13}$  정도로 매우 크다는 것을 알 수 있다(그림 6). 마찬가지로 양자컴퓨터 시스템의 크기도 상당히 크다는 것을 알 수 있다(그림 7).

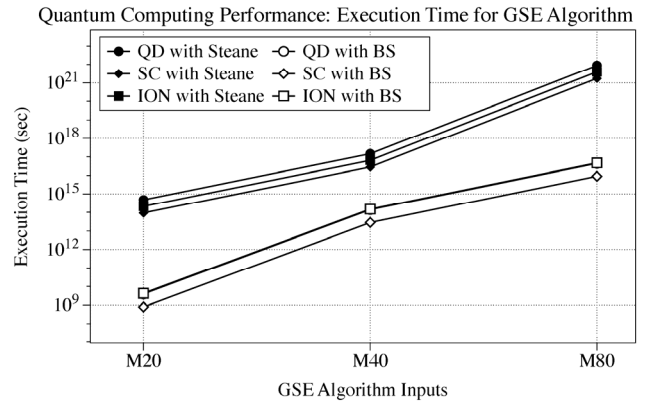


Fig. 5. Quantum computation time with considering system architecture

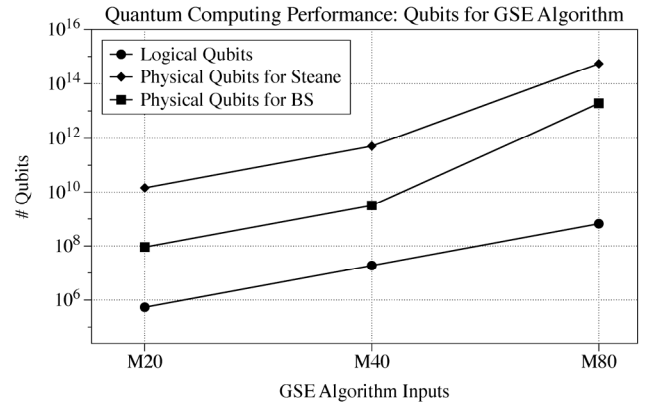


Fig. 6. Total number of physical qubits with considering system architecture

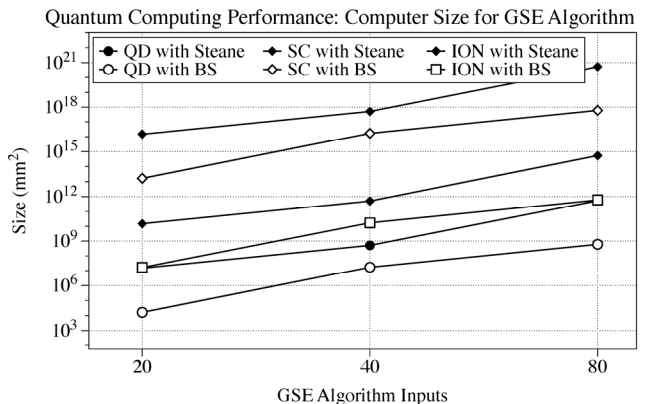


Fig. 7. Quantum computing system size

## V. 향후 진행해야 할 연구개발들

본 연구에서의 핵심 목표는 상대적으로 작은 크기의 양자 컴퓨팅에서 이론적으로 기대하는 높은 계산성능 확보를 위한 고려사항에 대해서 논하고자 하였다. 또한, 양자컴퓨팅 모델의 측면에서는 연산결과 신뢰도를 확보하기 위해서는 오류보정-결함허용방식이 적용되는 상황을 고려하였다. 분석

과정에서는 현재까지 제안된 다양한 방법들이 주로 사용되었으며, 최신의 기법과 데이터 등을 주로 사용하였다. 이를 통해서 전반적으로는 상대적으로 작은 크기 혹은 복잡도를 갖는 경우에도 현재의 양자컴퓨팅 구현 방법론 및 기술 등은 이론적으로 기대하는 양자계산성능을 확보하기 어렵다는 것을 확인하였다.

이러한 결과를 통해서 몇가지 중요한 내용을 다음과 같이 정리할 수 있다.

첫 번째로는 현재 시점 및 당분간의 양자컴퓨팅 실험은 오류보정-결함허용 방식보다는 아날로그 방식(알고리즘을 물리적 큐비트 수준에서 직접 구현하는 방식)이 합리적일 것이다. 양자알고리즘을 양자회로로 분해하는 과정에서 아날로그 양자컴퓨팅을 고려하는 경우에는 상대적으로 간단한 수준이 될 것으로 예상된다. 이에 따라서 필요한 단계수와 큐비트수의 요구량은 상대적으로 작을 것으로 기대된다.

두 번째로는 논리적 큐비트의 구현만을 목적으로 한 요구수준과 양자시뮬레이션을 목적으로 한 요구수준 사이의 비교 분석이 필요하다. 논리적 큐비트는 당장 시점에서는 구현되기 어렵지만, 높은 신뢰도를 갖는 양자컴퓨팅을 구현하기 위해서는 반드시 필요한 기술이다. 따라서 논리적 큐비트를 검증하는 것이 매우 중요한데, 이 과정에서의 기술적 요구수준이 양자시뮬레이션의 요구수준과 어떻게 상이한지 확인하는 것이 중요하다.

세 번째로 본 연구결과에서 구체적으로 제시하는 성능값은 모두 현재 상황을 반영한 것이긴 하지만, 빠르게 발전하는 양자하드웨어 기술과 양자컴퓨팅 구현 이론들을 고려하면 구체적인 값보다는 경향성을 활용하는 것이 의미있다.

네 번째로 이미 학계에서 확인된 것이지만, 오류보정-결함허용 과정에서의 오버헤드가 가장 크다는 것을 다시 한 번 더 확인하였다. 이는 대상 문제의 크기가 커짐에 따라라도 계속 증가하기 때문에 향후에도 매우 중요한 문제점으로 인식될 것이다. 따라서 오버헤드가 적은 오류보정-결함허용 방식을 개발하는 것은 매우 중요하다.

## VI. 결 론

본 연구에서는 현재까지 개발된 결함허용 양자컴퓨팅의 계산성능 측면에서의 정량적 분석을 진행하였다. 현재까지 개발된 양자프로세서의 기술 수준을 고려하여, 단기적으로 활용가치가 높은 양자시뮬레이션 분야를 대상으로 하여 결함허용기반 양자컴퓨팅 구현 방법론의 계산성능을 양자회로, 양자시스템구조, 오류보정-결함허용 적용 단계별로 분석하였다. 최종적으로는 우리가 기대하는 수준만큼의 계산성능을 확보하기는 어려워 보인다. 다만, 본 연구를 통해서 결함허용 양자컴퓨팅을 구성하는 주요 요소들의 계산성 측면에서

의 영향을 정교하게 분석할 수 있었으며, 이를 통해서 향후 우리가 개발 혹은 개선해야 하는 부분이 무엇인지를 정확히 알 수 있었다.

중요한 메시지중 하나는 양자하드웨어의 성능 못지않게 시스템수준에서의 영향, 즉, 컴파일, 오류보정-결함허용, 시스템구조 등의 영향도 매우 중요하다는 것이다. 이에 따라서 향후 양자컴퓨팅의 연구개발에서는 알고리즘수준, 시스템수준, 프로세서 수준 모두에서 계산성이 향상되어야 한다.

## 감사의 글

본 연구는 한국전자통신연구원 연구운영비지원사업의 일환으로 수행되었음[18ZH1400, 양자컴퓨팅 플랫폼 및 비용효율성 향상에 대한 연구개발].

## References

1. A. Trabesinger, "Quantum simulation," *Nat. Phys.* **8**, 263 (2012).
2. M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," Cambridge Press (2011).
3. J. D. Whitfield, J. Biamonte, and A. Aspuru-Guzik, "Simulation of electronic structure hamiltonians using quantum computers," *Mol. Phys.* **109**, 735-750 (2011).
4. A. J. Abhari, S. Patil, D. Kudrow, J. Heckey, A. Lvov, F. T. Chong, and M. Martonosi, "ScaffCC: Scalable compilation and analysis of quantum programs," *Parallel Comput.* **45**, 2-17 (2015).
5. A. S. Green, P. L. Lumsdaine, N. J. Ross, P. Selinger, and B. Valiron, "Quipper: A scalable quantum programming language," in *Proc. 34th ACM SIGPLAN Conference on Programming Language Design and Implementation (USA, Jun. 2013)*, pp. 333-342.
6. J.-K. Kim, A.-R. Jang, and B.-S. Choi, "Quantitative analysis of quantum computing power," in *Proc. KIPS Spring Conference (Dongguk Univ., Korea, Apr. 2016)*, pp. 84-86.
7. J. Preskill, "Fault-tolerant quantum computation," arxiv: 9712048 (1997).
8. A.-R. Jang and B.-S. Choi, "Performance analysis of ground state estimation algorithm on the fault-tolerant quantum computer system," in *Proc. IEIE Summer Conference (Korea, Jun. 2016)*, pp. 91-94.
9. C. R. Clark, T. S. Metodi, S. D. Gassner, and K. R. Brown, "Resource requirements for fault-tolerant simulation: The ground state of the transverse ising model," *Phys. Rev. A* **79**, 062314 (2009).
10. N. J. Ross and P. Selinger, "Optimal ancilla-free Clifford+T approximation of z-rotations," <https://arxiv.org/abs/1403.2975>