연차 보고서 (2차)

사업명	KAIST Grand Challenge 30 Project		
과제명	(국문) 양자컴퓨터 가능한가?		
	(영문) Is Quantum Computer Possible?		
연구책임자	한상근	소 속	수리과학과
총수행기간 (1단계)	2017.05.01. ~ 2022.12.31. (5 년)		
당해연도 협약기간	2018.01.01. ~ 2018.12.31. (1 년)		
당해년도 사업비(원)	20,000,000		

자체연구협약서(KAIST Grand Challenge 30 Project)제5조에 의거하여
연차보고서 2부를 제출합니다.

2019년 1월 15일

연구책임자: 한 상 근 (인)

한국과학기술원 총장 귀하

Ⅰ. 2차년도 추진 현황

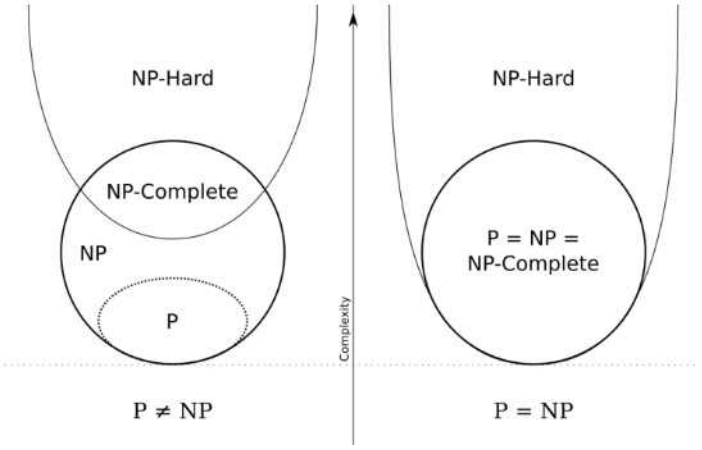
1. 연구의 배경

양자컴퓨터의 존재성과 현실적인 구현 가능성에 대한 연구들은 물리학, 전산학 분야에서 많이 이루어지고 있다. 하지만 이러한 양자컴퓨터의 가능성에 대한 연구는 계산 복잡도 이론 (Computational Complexity Theory)을 통해서 수학적으로도 접근해볼 수 있다. 복잡도 이론에서 BQP (Bounded-error Quantum Probabilistic Algorithms) class에 속하는 알고리즘은 양자 컴퓨터가 다항식 번의 연산으로 주어진 문제를 풀 수 있는 문제로서, BQP class가 기존의 P (Polynomial-time reduction algorithm) class와 다르면 양자컴퓨터의 존재 가치를 보여주는 것이다. 따라서 복잡도 이론을 통해 수학적으로 양자컴퓨터를 접근하게 된다면, 양자컴퓨터를 개발하려는데 투입되는 막대한 연구비에 비해 상당히 적은 양의 연구비로도 양자컴퓨터의 존재 가능성을 접근해볼 수 있다. 또한 이러한 연구 주제와 방향은 기존의 유명한 P vs NP 문제를 해결하는 것에도 기여를 할 수 있을 것으로 보인다.

2. 연구의 내용

위에서 언급했던 것처럼 양자컴퓨터의 존재 가능성은 복잡도 이론에서 BQP class와 P class를 연구하는 것으로 보일 수 있다. 만약 BQP = P 라면, 양자컴퓨터가 할 수 있는 모든 작업들은 기존의 컴퓨터로도 수행할 수 있다는 것을 의미하며, 실제로 양자컴퓨터가 개발되더라도 이론적으로 “새로운 것”이 없다는 것을 의미한다. 하지만 대부분의 연구자들은 BQP ≠ P라고 믿고 있었으며, 기존의 컴퓨터와는 다른 양자컴퓨터가 존재한다면 연구할 가치가 있다고 생각하고 있다.

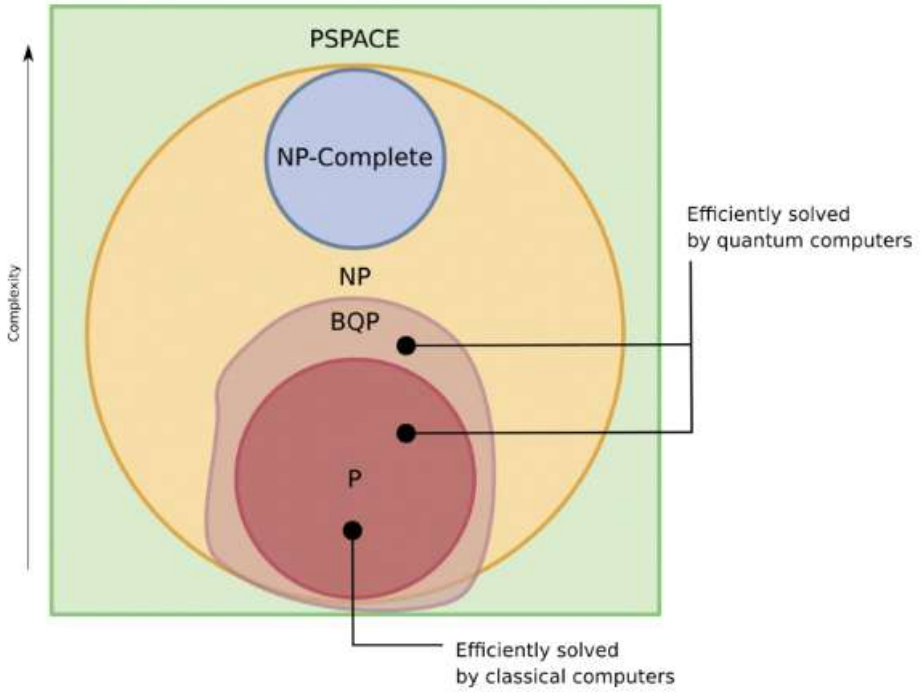
그러나 BQP vs P를 증명하는 것은 양자컴퓨터를 가정하지 않았던 고전적인 복잡도 분류 (Classical Complexity Classes, [그림 1])에서는 다루어지지 않았었다. 따라서 양자컴퓨터를 가정하고 새로운 문제들을 정의하여, 양자 복잡도 분류 (Quantum Complexity Classes)로 확장시키고자 하였다.



[그림 1] 고전적인 계산 복잡도 분류

BQP Class

BQP class는 1993년 Bernstein과 Vazirani가 정의한 양자 복잡도 문제로서, 양자 컴퓨터가 다항시간 내에 “예” 혹은 “아니오”로 대답할 수 있는 모든 결정(decision) 문제들을 포함한다. 따라서 기존의 컴퓨터로 다항식 시간내에 풀 수 있는 문제인 P class는 BQP class에 속하게 된다. 또한 1994년에 발표된 Shor의 알고리즘을 통해 소인수분해, 이산대수 문제가 설령 P class에 속하지 않더라도 BQP class에는 속하게 된다는 사실이 밝혀져 P ⊆ BQP라는 사실이 잘 알려져 있었다 [그림 2]. 더욱이 BQP는 [그림 2]의 아랫부분과 같이 NP class의 밖으로 돌출된 모양일 것으로 추측되고 있었다. 이는 기존의 컴퓨터로 문제의 답이 맞는지 검증하는 과정보다 양자컴퓨터로 문제를 푸는 시간이 더 빠른 어떤 문제가 존재할 것이라는 의미를 가지고 있지만, 저 영역에 해당하는 문제는 아직 발련되지 않은 상태이다. 이렇듯 정확한 BQP의 경계는 아무도 알고 있지 못한 상태이고, BQP 영역에 대하여 대부분의 연구자들이 [그림 2]와 같이 추측하고 있을 뿐이었다.



[그림 2] BQP class의 영역

Polynomial Hierarchy

계산 복잡도 이론을 더 자세히 분류해 보면 PH(Polynomial Hierarchy) class라는 개념이 있다. PH는 NP를 일반화한 것으로 NP 문제의 “there exists”, “for all”과 같은 수량사 (quantifier)들을 변경하거나 추가함으로써 문제를 더욱 복잡하게 만들어낸 class를 의미한다. 따라서 PH는 고전적인 복잡도 이론에서 잘 알려진 복

잡도 종류들을 대부분 포함하고 있으며, 여기에는 P, NP, co-NP 뿐만아니라 확률적 복잡도인 BPP(Bounded-error Probabilistic Polynomial time), RP(Randomized Polynomial time) 등이 있다.

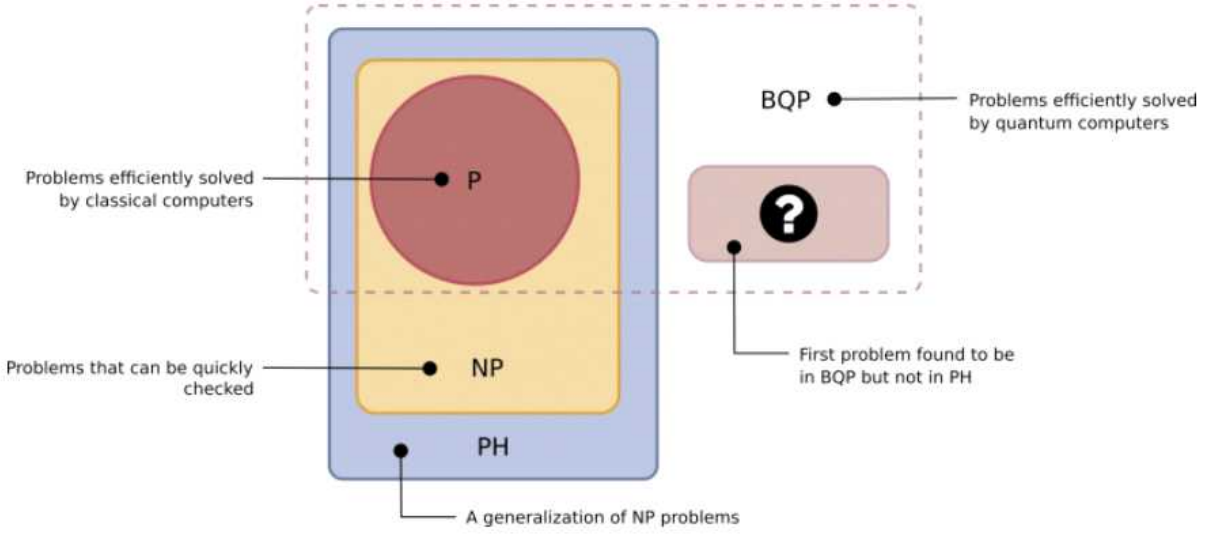
따라서 일반적으로는 P ⊆ PH 이지만, 정확한 P class와 PH class의 관계는 밝혀져 있지 않다. P vs PH 문제는 P vs NP 문제와 동치인데, 만약 P = NP 라면, P = PH이기 때문이다. 즉, 대부분의 연구자들이 믿고 있는 P ≠ NP를 가정한다면, 기존의 컴퓨터로는 PH class 문제를 풀 수 없다는 것이 중론이다.

BQP vs PH

위에서 살펴본 바와 같이 BQP class와 PH class를 비교하는 것은 기존의 컴퓨터가 지금보다 더 많은 문제를 풀 수 있다고 하더라도, 양자컴퓨터가 존재한다면 기존의 컴퓨터보다 본질적으로 더 나아질 수 있는지 답을 주기 때문이다. 즉, 대부분의 복잡도 종류들처럼 BQP가 PH에 속하게 된다면, 양자컴퓨터만의 장점이 사라져 존재 의의가 불분명해지기 때문이다.

대부분의 연구자들은 기존의 컴퓨터와는 다른 양자컴퓨터가 존재할 것으로 믿고 있으며, BQP ≠ PH라 생각하고 있다. 이 문제를 증명하는 방법은 한 class에 속하면서, 다른 class에는 속하지 않는 problem을 찾아내는 것이다.

FORRELATION은 f, g 가 두 개의 random Boolean function일 때에, g의 푸리에 변환 (Fourier transform)과 f의 corelation의 크기에 대한 decision 문제에 얼마나 빨리 대답할 수 있는지 묻는 문제이다. 2010년, Scott Aaronson은 generalized FORRELATION이 BQP-complete에 속한다는 것을 밝혀냈다. 이제 BQP ≠ PH임을 증명하기 위해서는 FORRELATION이 PH에 속하지 않다는 것만이 남아 있는데, 이는 2018년 6월, Ran Raz와 Avishay Tal에 의해 증명되었다.



[그림 3] BQP와 PH의 영역

BQP class와 PH class의 복잡도를 비교하기 위해서는 계산 시간 (computation time)을 측정해 보면 된다. 하지만 그 누구도 실제로 계산 시간을 측정하는 방법을 명확하게 알고 있지 못하기 때문에 이 방법은 사용할 수가 없다. 따라서 Raz와 Tal은 “oracle” (혹은 “black box”) 라는 것을 사용하여 문제를 해결하였다. 여기에서의 oracle은 $\{0,1\}$로 대답할 수 있는 결정 문제 (decision problem)를 풀기위해 사용되는 것으로서, 모든 복잡도 종류들을 풀 수 있다. 그렇기 때문에 주어진 문제를 풀기 위해서 몇 개의 힌트를 사용했는지를 통해 계산 복잡도를 짐작할 수 있다. 이에 Raz와 Tal은 FORRELATION 문제를 풀기 위하여 BQP 에서는 단 하나의 힌트가 필요했던 것에 비하여, PH에서는 무제한적으로 힌트가 주어지더라도 문제를 풀 수 없었다고 밝혀냈다.

결과적으로 FORRELATION이 BQP에는 속하지만, PH에는 속하지 않는 문제로 밝혀지게 되면서 [그림 3]과 같이 BQP $\neq$ PH 임이 증명되었다. 또한 자연스럽게 BQP $\neq$ P임이 밝혀져 양자컴퓨터의 (존재한다면) 가치가 복잡도 이론을 통해 힘을 얻었다.

Ⅱ. 결론 및 3차년도 계획

양자컴퓨터를 복잡도 이론으로 접근하는 연구는 BQP vs P 라는 open problem으로 오랫동안 연구되어 왔다. 그러다 올해 (2018년 6월), Raz와 Tal에 의해 BQP $\neq$ PH임이 증명되면서 양자컴퓨터의 존재 가치가 복잡도 이론을 통해 증명되었고, 이 분야에서 가장 굵직한 문제가 해결되었다. 그에 따라 [그림 3]과 같이 양자컴퓨터와 기존의 컴퓨터는 서로 다른 계산 복잡도의 영역을 차지하고 있음을 확인할 수 있어서, 양자컴퓨터가 존재한다면 기존의 컴퓨터에 비해 계산적인 우위를 가진다는 것이 확연하게 밝혀졌다.

그러나 세부적으로는 아직 풀지 못한 open problem들이 많이 남아 있다. 첫 번째로는 복잡도 이론의 관점에서는 NP-complete와 같이 표현되는 BQP-complete가 존재하는데, 아직까지는 그 범위가 불분명 하다고 볼 수 있다. 따라서 BQP-complete 방식으로 표현할 수 있는 문제를 찾을 수 있으면, BQP에서 BQP-complete로 확장시켜 더 넓은 범위의 양자 복잡도 분류를 넓혀나갈 수 있다. 두 번째로는 BQP class와 sub-EXPTIME의 차이가 알려져 있지 않으며, 실제로 BQP에 속하는 소인수분해와 이산로그 문제는 모두 sub-EXPTIME임이 잘 알려져 있다. 따라서 BQP class를 연구하는 것과 sub-EXPTIME을 연구하는 것은 동일한 문제로 여겨질 수 있는데, 문제점은 sub-EXPTIME이 수학적으로 엄밀하게 정의되어있지 않기 때문에 연구자들 사이에서도 논란이 있다. 따라서 애매하게 정의된

sub-EXPTIME에 대한 정의를 통해 BQP class를 세분화하여 분류할 수 있을 것으로 보인다.

격자(Lattice)를 사용하는 양자 내성(Quatum Resistant, Post-Quantum) 암호는 암호화에 걸리는 연산 복잡도를 줄이기 위해 순환(Circular) 행렬을 사용한다. 그런 특수한 행렬을 사용하는 것에 대해 암호학자들은 안전하다고 말하고 있으나, 양자계산을 연구하는 Fang Song등은 순환(Circular) 행렬을 사용하는 암호에는 Dihedral Group에 대한 generalized Fourier 변환으로 양자계산 공격이 가능할 것으로 추측하고 있어 연구가 필요하다.