논문 20-45-12-03 The Journal of Korean Institute of Communications and Information Sciences '20-12 Vol.45 No.12
https://doi.org/10.7840/kics.2020.45.12.2046

자원 할당을 위한 낮은 복잡도의 양자 Grover 알고리즘 설계

민 건 식•, 허 준°

Design of Low-Complexity Quantum Grover Algorithm for Resource Allocation

Gun-sik Min•, Jun Heo°

요 약

본 논문은 채널 할당 문제(Channel allocation)와 대응되는 문제인 그래프 색칠 문제를 낮은 복잡도의 양자 Grover 알고리즘으로 해결하는 기법을 제안다. NP 문제를 해결하기 위한 양자 알고리즘인 Grover 알고리즘은 N 개의 데이터베이스에서 해답을 찾을 때 디지털 알고리즘 대비 quadratic speed up 효과를 가져 연구가 활발히 진행됐다. 일반적으로 최적 경로 탐색 기반 최적화, 소인수분해, 대량 데이터 탐색 등에 있어 강점을 가진 것으로 평가되고 있다. 디지털 알고리즘을 이용한 다색 색칠 문제에 관한 연구는 그래프를 간단한 그래프로 치환하여 알고리즘을 적용하거나 노드 수를 줄여 색칠 문제를 해결해왔다. 그러나 이러한 노력에도 불구하고, 현재까지 연구된 색칠 문제를 해결하는 디지털 알고리즘은 몇 가지 한계점들에 의하여 만족스러운 성능을 얻어내지 못하였다. 따라서 본 논문에서는 이러한 한계점을 극복하기 위하여 Grover Search Algorithm의 input state dimension을 줄여 다색 색칠 문제 해결을 위한 복잡도를 줄인다.

Key Words : Quantum computing, Quantum algorithm, Graph coloring, Channel allocation

ABSTRACT

In this paper we propose a technique to solve the problem of graph coloring, which is a problem corresponding to channel allocation problem, with a low complexity quantum Grover algorithm. The Grover algorithm, a quantum algorithm for solving NP problems, has a quadratic speed up effect compared to digital algorithm when finding answers in N databases so research has been actively carried out. In general, it is evaluated to have strengths in optimizing the base of optimal path exploration, small factor resolution, and mass data exploration. The study on multi-coloring problem using digital algorithm has solved the problem of coloring by replacing the graph with simple graph to applying the algorithm or reducing the number of nodes. Despite these efforts, however, the digital algorithm that solves the coloring problem studied so far has not achieved satisfactory performance by some limitations. Therefore, in order to overcome these limitations, this paper shows the result of reducing complexity in solving multi-coloring problem by reducing input state dimension of Grover Search Algorithm.

※ 이 논문은 2020년도 정부(교육과학기술부)의 재원으로 한국 연구재단의 지원을 받아 수행된 연구임 (No.2019R1A2C2010061)
• First Author : Korea University, mgs3351@korea.ac.kr, 학생(석사), 학생회원
° Corresponding Author : Korea University, junheo@korea.ac.kr, 정교수, 종신회원
논문번호 : 202008-200-A-RN, Received August 19, 2020; Revised September 17, 2020; Accepted September 24, 2020

Ⅰ. 서 론

Grover Search Algorithm(GSA)은 높은 확률로 함수에 대한 답을 생성하는 양자 알고리즘이다. GSA는 1996년 Lov Grover에 의해 처음으로 제안된 데이터베이스 검색 양자 알고리즘이다.[1] Data base 크기가 N일 경우 기존 디지털 방식의 알고리즘은 답을 생성하는데 $O(N)$의 복잡도로 연산하는 데 비해 Grover Search 알고리즘은 $O(\sqrt{N})$의 복잡도로 연산을 수행한다. GSA는 선형 함수에 대한 해답을 찾는 것뿐만 아니라 비선형 문제에 대한 해답을 생성하는 것 또한 가능하다. 즉, 비선형 문제인 K-SAT (satisfiability) 문제를 해결하는 것에 용이한 양자 알고리즘이다.

SAT 문제란 충족 가능성 문제로 여러 개의 불리언(Boolean) 변수들로 이루어진 불리언 표현이 각 변수의 값을 참, 거짓 중 하나로 설정하여 전체 식의 결과를 참로 만들 수 있는지 결정하는 문제이다. SAT 식은 절과 리터럴(literal)로 이루어져 있으며 리터럴(literal)의 개수가 k개인 경우 k-SAT 문제라고 정의된다. 이러한 k-SAT 문제는 대표적인 NP-완전 문제이다. SAT 문제는 그래프 색칠 문제로 치환될 수 있어 GSA로 그래프 색칠 문제 또한 해결할 수 있다.[1,2]

그래프 색칠 문제는 노드와 실선으로 이루어진 그래프 상황에서 인접한 노드는 실선으로 연결되며 그 인접한 노드들은 같은 색을 사용할 수 없다. 이러한 조건으로 모든 노드에 색을 칠하는 것이 그래프 색칠 문제이다. 노드에 한 가지 색을 칠하면 단색 색칠 문제이며 여러 가지 색을 칠하면 다색 색칠 문제로 정의된다.

본 논문에서는 그래프 색칠 문제에 대응되는 이동통신 채널 할당 문제를 낮은 복잡도의 양자 알고리즘으로 해결하는 기법에 대해 다룬다. 디지털 알고리즘으로 채널 할당 문제를 해결하는 것은 여러 방법이 있지만, 대표적으로 그래프 색칠 문제로 대응하여 해결한다.[3] 이때 디지털 알고리즘 수행 복잡도가 굉장히 높으므로 본 논문에서는 양자 알고리즘으로 해결하여 채널 할당 문제의 복잡도를 줄이는 것을 밝힌다.

본 논문에서는 이동통신 채널 할당 문제를 색칠 문제로 변환하여 GSA로 해결하는 기법을 제안한다. 기존 단색 색칠 문제를 GSA로 해결할 경우 개선된 복잡도 이득을 얻을 수 없으므로 복잡한 환경인 다색 색칠 문제를 다룬다. 본 논문에서는 입력 데이터를 줄여 알고리즘 수행 반복 횟수를 줄이며 그에 따른 입력 데이터를 생성하는 양자 회로 기법을 제안한다. 제안 기법은 디지털 방식뿐만 아니라 기존 GSA 방식보다 개선된 복잡도를 가지며, 회로 설계에 대한 타당성 검증을 위해 Quirk 양자 시뮬레이터를 사용한다.

다음과 같은 차례로 논문이 구성되어 있다. 2장에서는 그래프 색칠 문제로 치환되는 이동통신 채널 할당 문제에 대해 다룰 것이다. 또한, 2.1장에서는 기본적인 GSA의 개념절차를 설명하여 양자 알고리즘이 생소한 이들의 이해를 돕고자 하였다. 2.2 장에서는 그래프 색칠 문제를 GSA로 해결하는 방법을 기술하여 실제 양자 회로에서 어떻게 치환되는지 설명한다. 또한, 다색 색칠 문제에 필요한 input state 생성 기법에 대해 알아볼 것이다. 3장에서는 제안하는 기법의 타당성을 검증하기 위해 양자 시뮬레이션을 보여줄 것이며 복잡도 성능의 수치적 분석을 살펴본다. 마지막으로 4장에서는 논문의 결론을 맺도록 한다.

Ⅱ. 본 론

미국 연방 통신 위원회는 주파수 공동사용 정책 추진에 대한 권고를 반영하여, 군사 및 위성에서 사용 중인 3.5GHz 대역의 150MHz 대역폭(3.55~3.7GHz)을 주파수 공동사용을 통해 넓은 주파수대역에서 광대역 서비스를 이용할 수 있도록 '시민 광대역 무선 서비스(CBRS)' 대역으로 신설하는 규정을 마련하였다[4].

CBRS 사용자는 크게 3계층으로 구분되며, 최상위 접속계층인 "Incumbents"와 2차 주파수 공동사용 면허권자인 우선순위접속(Priority Access), 최하위 접속계층인 일반허가접속(GAA)로 구성되어 있다. 계층별 간섭 보호를 위해 SAS(Spectrum Access System)의 관리하에 운영된다. 주파수 접속 시스템은 우선순위접속 혹은 일반허가접속 이용자에게 주어진 위치에 따

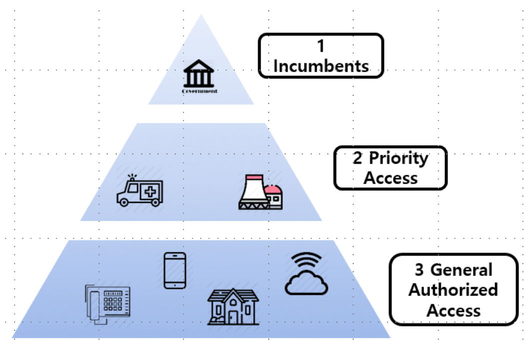


그림 1. 3.5GHz CBRS 대역의 3계층 스펙트럼 엑세스
Fig. 1. 3-layer spectral access in the 3.5GHz CBRS band

라 가용 주파수를 결정하여 할당하게 된다. 이때, 일반허가접속은 공인된 스몰셀 등을 활용한 CBSD(Citizen Broadband Radio Service Device)를 사용하여 주파수를 사용하게 된다. 일반허가접속은 기존이용자, 우선 접속이용자가 사용하지 않는 주파수를 할당받아 사용하며, 간섭을 유발하면 안 된다. 따라서 일반허가접속을 위한 공인된 CBSD의 분포에 따라 주파수 할당을 간섭 그래프 상황으로 변환하여 할당하게 된다.[3-5]

CBRS 시스템 모델의 배경은 일반허가접속으로 주파수를 할당받는 CBSD를 노드로 설정하고 인접한 CBSD는 실선으로 연결되어 서로 다른 주파수를 할당하게 된다. 대역폭을 10MHz로 나누어 할당하게 될 경우 150MHz를 15개의 채널로 나누어 할당하게 된다. 이때 그래프 색칠 문제로 치환할 경우 총 색의 개수는 15개이다.

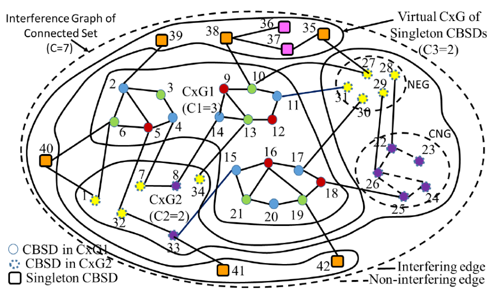


그림 2. CBRS 모델을 그래프 색칠 모델로 해결하려는 예시
Fig. 2. Examples of resolving CBRS models with graphing models

2.1 그래프 색칠 문제

색칠 문제는 크게 다색 색칠과 단색 색칠 문제로 나누어지는데, 다색 색칠 문제는 그래프의 노드에 칠할 수 있는 색이 1가지 이상인 경우를 의미한다. 그리고 단색 색칠 문제는 노드에 칠할 수 있는 색이 1가지인 경우를 의미한다.

그림 3은 채널 할당 문제에 대해 다색 색칠 문제가 적용되는 예시를 나타낸다. 그림 3에서 Base Station(BS)은 Channel(CH) 1부터 5까지 할당할 수 있다고 가정한다. 이때 (a) 에서는 User Equipment(UE) A, B, C가 BS와 통신이 가능[6]하고 A와 B, A와 C는 서로 간섭의 영향으로 같은 채널을 할당받지 못하고 A, B, C는 각각 3개, 1개, 2개의 CH를 할당받는다고 가정한다. 이러한 가정으로 CH 할당 문제를 그래프 색칠 문제으로 치환하면 그림 3의 (b)와 같다. UE는 그래프 색칠 문제에서 노드에 해당하고 할당하려는 CH는 노드에 칠하는 색을 의미한다. 또한, 할당받아야 하는 CH의 수는 노드에 칠하는 색의 수로 치환된다. 같은 채널을 할당받지 못하는 A와 B, A와 C는 실선으로 연결되어 같은 색을 칠할 수 없도록 위 그림의 (b) 에 표현되어 있다[7].

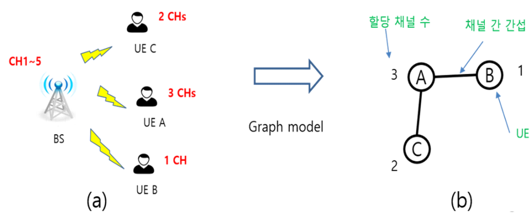


그림 3. Channel Allocation을 위한 색칠 문제
Fig. 3. Coloring Problem for Channel Allocation

2.2 Grover 데이터베이스 검색 알고리즘

GSA는 주어진 데이터베이스에서 원하는 자료를 찾는 것이 목적이다. 데이터베이스의 크기가 N일 때, 원하는 자료의 개수가 m개 있을 때, 디지털 알고리즘은 $O(N)$의 복잡도로 연산을 수행한다. 하지만 GSA는 $O(\sqrt{N})$의 알고리즘 수행 복잡도로 연산을 수행한다. 이러한 알고리즘 수행 복잡도는 최적화된 기법으로 GSA는 해답을 찾을 확률이 정확히 1이 아닌 1에 가깝게 확률을 최대로 만들어 주는 것이 특징이다.

GSA는 총 4단계를 거쳐 알고리즘을 수행하게 된다. 첫 번째 단계에서 모든 데이터베이스를 양자 상태로 준비한다. 두 번째 단계에서는 oracle 연산자를 통하여 해답이 되는 양자 상태들의 위상을 반전시켜준다. 세 번째 단계인 diffusion 연산자를 적용하여 해답이 되는 양자 상태들의 amplitude를 높여주며 마지막으로 양자 측정을 통해 해답을 얻는다.

2.2.1 GSA의 구조

먼저 QSA의 전체 구조는 다음과 같은 그림으로 표현할 수 있다.[2]

초기 상태로 데이터베이스의 크기를 $N=2^n$이라 하고, n큐빗 시스템에서 다음 양자 상태를 준비한다. 이러한 양자 상태를 준비하는 방법은 n 큐비트 시스템에서 Hadamard gate를 n개 적용하는 방법이다.

$$|s\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle \tag{1}$$

Oracle 연산자의 기하학적 의미는 다음과 같은 그림으로 표현할 수 있다.

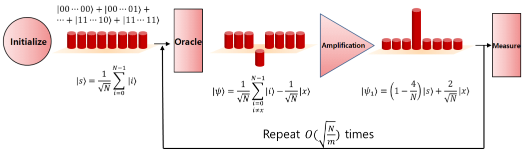


그림 4. QSA 전체 구조 블록도
Fig. 4. QSA full design block diagram

그림 5와 같이 $g(i)$는 i가 답일 경우 1이고, i가 답이 아닐 때 0이 값을 생성하는 함수이다. Oracle 연산자는 다음과 같이 정의된다.

$$O|i\rangle_1|w\rangle_2 = |i\rangle_1|w \oplus g(i)\rangle_2 \tag{2}$$

두 번째 시스템의 상태가 $|w\rangle = |-\rangle$일 때, 초기 상태에 Oracle 연산자 U_x를 작용시키면 아래와 같이 된다.

$$O|i\rangle_1|-\rangle_2 = (-1)^{g(i)}|i\rangle_1|-\rangle_2 \tag{3}$$

위에서 i가 답일 때만 부호가 바뀌므로 연산자 U_x

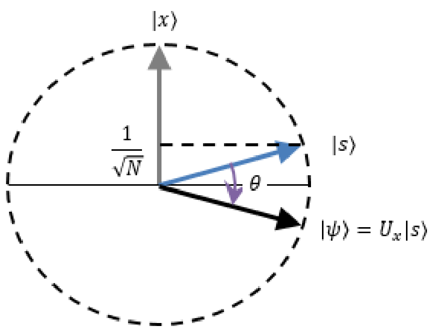


그림 5. Oracle 연산자의 기하학적 의미
Fig. 5. Geometric Meaning of Oracle Operator

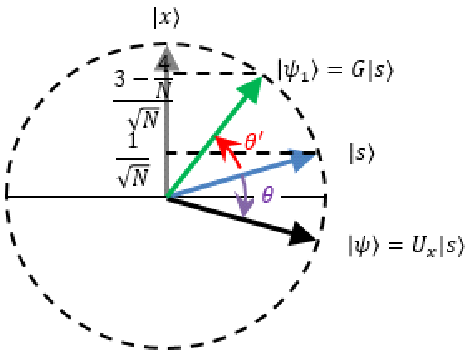


그림 6. Diffusion 연산자의 기하학적 의미
Fig. 6. Geometric Meaning of Diffusion Operator

는 가능한 모든 답이 중첩된 상태 $|s\rangle$에서 찾고자 하는 답의 계수만 부호를 바꾸어 주는 역할을 한다.

확산(diffusion) 연산자는 그림 6과 같이 기하학적 그림으로 표현할 수 있다. Oracle 연산자를 적용한 뒤 나온 양자 상태에서 확산 연산자 $H^{\otimes n}P_0^{\otimes n}H^{\otimes n}$를 취해준다. 여기서 H는 Hadamard 양자 gate를 뜻하며 $P_0^{\otimes n} = 2|0\rangle\langle 0| - I$이다.

$$H^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{i,j=0}^{2^n-1}(-1)^{ij}|i\rangle\langle j| \tag{4}$$

가 되므로 $H^{\otimes n}P_0^{\otimes n}H^{\otimes n} = 2|s\rangle\langle s| - I$가 된다. 확산 연산자 적용을 하여 주어진 문제에 대한 해답이 되는 state의 진폭을 증폭시킨다.

Grover 연산자는 oracle 연산과 확산 연산을 합한 것을 말하고 Grover 연산자 G라 정의한다. Grover 연산자 G를 거친 뒤 양자 상태는 아래와 같이 변환한다.

$$G|x\rangle = \sqrt{\frac{N-4}{N}}|s\rangle + \frac{2}{\sqrt{N}}|x\rangle \tag{5}$$

초기 상태에서 답 $|x\rangle$과 가까운 정도는 $|\langle t|s\rangle|^2 = \frac{1}{N}$ 이고 원래 답인 $|x\rangle$과 가까운 정도인 fidelity를 나타내는 것은 아래 식과 같다.

$$|\langle t|G|s\rangle|^2 = \left(\frac{3N-4}{N\sqrt{N}}\right)^2 = \frac{(3N-4)^2}{N^3} \tag{6}$$

$$|\langle t|s\rangle|^2 = \frac{1}{N} < \frac{(3N-4)^2}{N^3} = |\langle t|G|s\rangle|^2 \tag{7}$$

따라서 Grover 연산자 G는 초기 상태를 답 $|t\rangle$와 더 가깝게 만들어 준다.

초기 상태를 찾고자 하는 답과 그것의 수직인 상태를 다시 쓰면 다음과 같은 state이다.

$$|s\rangle = \sqrt{\frac{1}{N}}|x\rangle + \sqrt{\frac{N-1}{N}}|ns\rangle \tag{8}$$

이때 $|x\rangle$와 $|ns\rangle$가 이루는 각도는 $\varphi = \arcsin\sqrt{1/N}$가 된다. Oracle 연산자는 찾고자 하는 답에 수직인 부분 공간에 대한 반사 연산자이므로 $|x\rangle$를 $|ns\rangle$축에 대해 대칭 이동한 것이 된다. 확

산 연산자는 $|x\rangle$를 중심으로 반사하는 작용 원이다. 따라서 Grover 연산자를 반복할수록 정답 가까운 상태로 바뀐다.

2.3 Input state 준비과정 설계

기존 GSA 알고리즘은 앞선 장에서 설명한 Hadamard gate를 input qubit 개수만큼 할당하여 모든 state, 즉 모든 경우의 수를 중첩하여 알고리즘을 연산하였다.

기존 방법은 모든 경우의 수를 중첩하는 기법이기 때문에 노드 조건식이 필요하다. 노드 조건식이란 노드에 칠할 수 있는 색의 정보가 들어올 때 그에 대한 조건식을 Grover 알고리즘을 적용할 수 있도록 SAT 식으로 변환한 식을 말한다. 노드 조건식은 Grover 알고리즘에서 oracle 과정에서 실선 조건식과 동시에 할당되어 적용하게 된다.

모든 경우의 수를 중첩하는 기존 방법의 문제점은 oracle 연산자를 이루는 노드 조건식에서 수많은 toffoli gate와 ancilla qubit과 같은 양자 자원을 필요로 하게 된다. 그래프에서 전체 칠해야 하는 색의 개수가 많아지게 되면 ancilla qubit을 많이 필요로 한다. Ancilla qubit을 많이 사용하지 않으려면 재활용하기 역연산 양자 gate인 toffoli gate가 더 필요로 하게 된다.

제안하는 기법은 모든 state(경우의 수)를 중첩하여 알고리즘을 수행하는 기존 양자 알고리즘[1]에 비해 이득을 볼 뿐만 아니라 디지털 알고리즘[8]과 비교해도 개선된 복잡도로 연산을 수행한다. 제안하는 기법의 블록 도는 그림 8과 같다. 그림 8의 input state 준비 과정 블록은 W state[9]기법의 확장판을 나타낸 것이다.

주어진 그래프에서 칠할 수 있는 전체 색의 개수가 k개이고 n번째 노드에 1개의 색을 칠하는 경우 input state를 W state 기법을 활용하여 아래와 같이 중첩한다.[9]

$$|\Psi_{n,k,1}\rangle = \frac{1}{\sqrt{C_{k,1}}}(|10\cdots0\rangle + |01\cdots0\rangle \cdots + |0\cdots01\rangle) \tag{9}$$

$|\Psi_{n,k,1}\rangle$state는 1의 개수가 1개이고 0의 개수는 $n-1$개인 state를 k개 중첩해 만든 state이다.

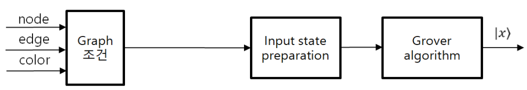


그림 7. 그래프 색칠 문제를 해결하는 제안하는 기법
Fig. 7. Overview diagram of proposed techniques to solve the Graph coloring problem

제안하는 기법은 input state를 그래프에서 칠할 수 있는 전체 색의 개수가 k개이고 n번째 노드에 l개의 색을 칠할 때 W state 기법을 활용하여 1의 개수가 l개인 state를 중첩하여 state를 만든다. 이러한 input state는 아래와 같이 중첩한다.

$$|\Psi_{n,k,l}\rangle = \frac{1}{\sqrt{C_{k,l}}}(|1\cdots10\cdots0\rangle + \cdots + |0\cdots01\cdots1\rangle) \tag{10}$$

위와 같은 조건이 주어지면 총 $C_{k,l} = \binom{k}{l}$개의 state가 같은 확률로 중첩되어 있다. State는 k개의 qubit으로 중첩 시키며 l개의 qubit이 1로 할당된다. 노드에는 l개의 색을 칠해야 한다는 것을 뜻한다. 기존 방법은 총 2^{kn}개의 input state를 중첩 시켜 알고리즘을 수행하게 된다. 따라서 각 노드에 칠해야 하는 색의 개수가 고정된 상황에서 다음과 같은 $|\Psi_{n,k,l}\rangle$state를 각 노드에 중첩 시켜 알고리즘을 수행한다.

Input state의 예시를 들어본다. n번째 노드에 전체 3가지 색 중 2개의 색을 칠하는 경우는 두 개의 경우를 합하여 만들게 된다. 첫 번째는 전체 2가지 색 중 1가지 색을 칠하는 경우에서 새로운 색 한 가지를 추가하여 칠하게 되는 경우다. 두 번째는 전체 2가지 색 중 2가지 색을 칠하는 경우에서 새로운 색 한 가지를 추가한 뒤 칠하지 않는 것이다. 따라서 다음과 같은 중첩된 state가 만들어진다.

$$|\Psi_{n,3,2}\rangle = \sqrt{\frac{2}{3}} \cdot \sqrt{\frac{1}{2}}(|01\rangle + |10\rangle) \otimes |1\rangle + \sqrt{\frac{1}{3}}|11\rangle|0\rangle \tag{11}$$

위 양자 상태는 제안하는 state 준비 기법 일반화를 위해 간단한 경우로 시작하여 state 중첩 예시를 나타낸 것이다. 다시 밑의 양자 상태로 변환할 수 있다.

$$|\Psi_{n,3,2}\rangle = \sqrt{\frac{2}{3}}|\Psi_{n,2,1}\rangle|1\rangle + \sqrt{\frac{1}{3}}|\Psi_{n,2,2}\rangle|0\rangle \tag{12}$$

같은 방식으로 n번째 노드에 전체 4가지 색 중 2개의 색을 칠하는 경우는 다음과 같은 중첩된 state로 만들어진다.

$$|\Psi_{n,4,2}\rangle = \sqrt{\frac{2}{4}}|\Psi_{n,3,1}\rangle|1\rangle + \sqrt{\frac{2}{4}}|\Psi_{n,3,2}\rangle|0\rangle \tag{13}$$

이와 같은 state는 다음과 같은 양자 회로로 구성된다.

그림 8 회로의 박스형 gate는 rotation gate인 controlled-Y rotation gate이다. 이러한 양자 gate는 다음과 같은 operator로 표현된다.[10]

$$R_Y = \begin{pmatrix} \cos\left(\frac{\alpha}{2}\right) & -\sin\left(\frac{\alpha}{2}\right) \\ \sin\left(\frac{\alpha}{2}\right) & \cos\left(\frac{\alpha}{2}\right) \end{pmatrix} \tag{14}$$

$\cos\left(\frac{\alpha}{2}\right)$가 위 state의 $\sqrt{\frac{2}{4}}$ 값으로 표현되므로 $\alpha = 2\arccos\left(\sqrt{\frac{l}{k}}\right)$으로 구할 수 있다. State의 상숫값을 설계하는 회로를 각각의 경우에 대하여 모두 설계한 뒤 l개의 색을 칠하는 경우 l개의 X gate를 회로 가장 앞에 할당하여 각 노드의 state를 구성한다.

위와 같은 방식을 반복하여 전체 k가지 색 중 l개의 색을 칠하는 경우, 다음과 같은 일반화된 state로 만들 수 있다.

$$|\Psi_{n,k,l}\rangle = \sqrt{\frac{l}{k}}\,|\Psi_{n,k-1,l-1}\rangle|1\rangle + \sqrt{\frac{k-l}{k}}\,|\Psi_{n,k-1,l}\rangle|0\rangle \tag{15}$$

State 회로는 노드에 칠해야 하는 색의 개수 l과 관계없이 총 $\frac{(k-1)(k-2)}{2}$개의 연산 시간이 가장 긴 3개의 qubit을 얽히게 하는 2qubit controlled-Y rotation 양자 gate로 구성된다.

기존 방법과 같이 모든 state를 중첩하기 위해서는 input qubit 개수만큼 Hadamard gate 연산을 한다. 제안하는 기법에서는 기존 기법과 같은 input qubit을 준비하고 toffoli gate와 CNOT gate들이 필요로 한다. 하지만 제안하는 기법은 input state를 노드에 칠해야 하는 색의 개수 조건을 만족하도록 state를 미리 설계하기 때문에 노드 조건식에 대한 양자 회로를 요구하지 않는다. 따라서 기존 기법 대비 알고리즘을 한번

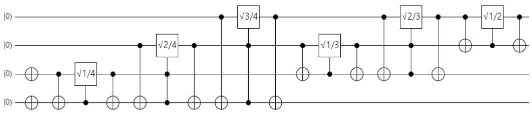


그림 8. 전체 4개의 색 중 2개의 색을 할당하는 노드에 관한 양자 회로
Fig. 8. Quantum circuit for nodes that allocate two colors out of four colors

수행할 때의 필요한 자원은 제안하는 기법에서 크게 달라지지 않는다.

제안하는 기법은 알고리즘을 한번 iteration 할 때 필요한 시간이 기존 방법과 큰 차이가 없다. 하지만 input state 개수와 수행 반복 횟수가 비례하는 Grover 알고리즘의 특성상 input state를 줄임으로써 알고리즘 복잡도에서 이득을 볼 수 있는 이점이 있다.

Ⅲ. 시뮬레이션 결과 및 기법 효과 정리

본 기법의 복잡도 이득 효과와 회로 설계 타당성을 입증하기 위해 시뮬레이션을 진행한다. 양자 회로 스텝 수가 가장 길고 state의 진폭을 즉시 확인 가능한, 양자 시뮬레이터 Quirk로 시뮬레이션을 진행한다. 이 때 양자 시뮬레이터의 qubit 수 제약 조건으로 인해 간단한 그래프로 시뮬레이션을 진행하여 회로 설계 타당성을 확인한다.

그림 11은 그림 9와 같은 그래프에 대해 노드 2개에 칠할 수 있는 색의 개수는 2개, 전체 칠할 수 있는 색의 개수는 4개로 가정한 간단한 그래프 상황에 대한 실제 설계 회로이다.

그림 10에서는 첫 단계에서 제안하는 state를 준비 과정을 통하여 input state를 중첩한다.

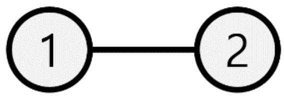


그림 9. 시뮬레이션 그래프
Fig. 9. Example of graph with two nodes for Simulation

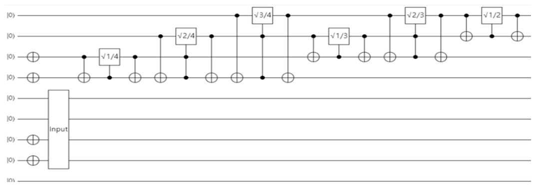


그림 10. Input state 준비과정 양자 회로도
Fig. 10. Input state preparation quantum circuit

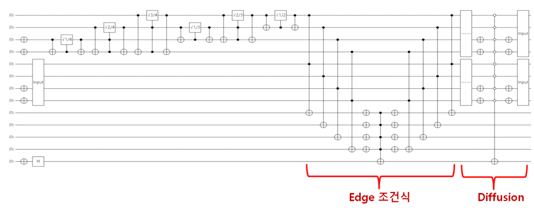


그림 11. Quirk 시뮬레이터를 이용한 전체 양자 회로도
Fig. 11. Full quantum circuit using Quirk simulator

Grover 알고리즘의 oracle 역할을 하는 실선(edge) 조건식에 대응하는 회로를 설계한다. 실선 조건식으로 인접한 노드에 같은 색을 칠하지 않는 답이 되는 state의 phase를 역전시킨다. 그림 11의 마지막 단계인 diffusion 과정을 통해 준비된 state의 평균 phase 값을 역전시키는 식을 다음과 같이 표현한다. diffusion 과정 식의 unitary gate인 U는 input state 준비 과정의 operator U이다. 다음과 같은 연산자를 통하여 이러한 과정을 연산하게 된다.

$$U^{\dagger}(I-2|0\rangle\langle 0|)\,U$$
$$U|0\rangle^{\otimes k}=\sqrt{\frac{l}{k}}\,|\Psi_{n,k-1,l-1}\rangle|1\rangle+\sqrt{\frac{k-l}{k}}\,|\Psi_{n,k-1,l}\rangle|0\rangle \tag{16}$$

제안하는 기법을 그림 9의 그래프 상황에 대입할 경우 양자 state dimension은 다음과 같이 감소 효과를 보인다.

다음은 시뮬레이션 결과표이다.

기존 양자 알고리즘이 iteration 횟수가 5번 필요한 것에 비해 제안하는 기법이 답이 되는 state가 100% 확률로 가져야 할 경우 iteration 수는 1.9회이다. 하지만 Grover 알고리즘의 제약 조건상 discrete 한 횟수로 iteration이 가능하므로 2회를 진행할 경우 답이 되는 state의 위상이 반전되어 오히려 확률값이 줄어들게 된다. 3개의 노드가 2개의 실선으로 연결된 다색 색칠 문제의 경우 기존 양자 알고리즘 대비 개선된 복잡도로 연산할 수 있다.

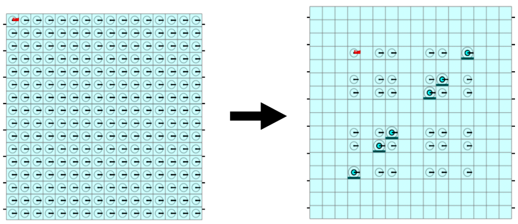
노드, 실선, 색 조건이 주어졌을 때 단색 색칠 문제의 경우 input state 준비 과정을 W state 기법을 이용한다. 기존 양자 알고리즘은 모든 문제에 대하여 input state를 모든 state, $H|0\rangle^{\otimes n}$로 중첩한다. 따라서 모든 문제를 알고리즘을 똑같은 복잡도로 수행한다. 다색 색칠 문제는 제안하는 기법을 이용하여 최종적으로 디지털 알고리즘에 비해 개선된 복잡도로 알고리즘을 수행한다.

표 2는 단색 색칠 문제와 다색 색칠 문제를 해결하는데 디지털 알고리즘[11]과 제안 기법 양자 알고리즘, 그리고 기존 양자 Grover 알고리즘의 복잡도를 비교한 표이다.

기존 양자 알고리즘의 경우 2^{kn}개의 input state로 알고리즘을 수행하기 때문에 복잡도가 $O(\sqrt{2^{kn}})$이다. 하지만 제안하는 기법은 input state의 개수가 s^n개이므로 복잡도가 $O(\sqrt{s^n})$이다. 직접적인 비교가 어려우나 간단한 예시를 보자. 10개의 노드가 임의의 실선으로 연결된 그래프 색칠 상황에서 전체 색의 개수는 7개이고 하나의 노드에 4개의 색을 칠해야 하는 상황을 가정한다. 디지털 알고리즘의 경우 알고리즘 수행 반복 횟수가 10^{15}번이라면 기존 알고리즘의 경우 수행 반복 횟수가 10^{13}, 제안하는 기법의 양자 알고리즘은 10^7이 되어 복잡도 측면에서의 이득을 얻을 수 있는 것을 알 수 있다.

$$s=\binom{k}{l} \tag{17}$$

기존 양자 알고리즘 대비 $O(\sqrt{2^{kn}})$에서 $O(\sqrt{s^n})$으로 복잡도를 줄일 수 있다. 디지털 양자 알고리즘 대비 $O(2^{n+s})$에서 $O(\sqrt{s^n})$으로 복잡도를 줄일 수 있다. 구체적으로 예시를 들면 노드가 10개, 색이 7개, 각 노드에 4개의 색을 할당을 할 경우를 예로 들자. 이 경우 디지털 알고리즘 대비 10^8 수행 반복 횟수 이



(a) (b)

그림 12. (a)는 state dimension이 2^8, (b)는 36
Fig. 12. (a) 2^8, (b) 36

표 1. 시뮬레이션결과 값
Table 1. Simulation result

	1회 iteration시 해답 확률	필요 iteration 횟수	5색, 3노드 2edge
기존 기법	33.75%	5회	31회
제안 기법	90.71%	1회	4회

표 2. 복잡도 비교표 2에서의 s는 다음과 같다.
Table 2. Complexity comparison

	디지털 알고리즘	기존 양자알고리즘	제안 기법 양자알고리즘
단색 색칠	$O(2^n)$	$O(\sqrt{2^{kn}})$	$O(\sqrt{k^n})$
다색 색칠 복잡도	$O(2^{n+s})$	$O(\sqrt{2^{kn}})$	$O(\sqrt{s^n})$
	10^{15}	10^{13}	10^7

득(10^{15}→10^7), 기존 양자 알고리즘 대비 10^6 수행 반복 횟수 이득(10^{13}→10^7)을 얻을 수 있다.

Ⅳ. 결 론

본 논문에서는 양자 Grover 알고리즘의 기본 개념을 설명하고 다색 색칠 문제를 해결할 때의 input state를 줄인 양자 알고리즘 기법에 관한 연구를 수행하였다. 본 논문에서는 자원 할당 문제를 그래프 색칠 문제로 변환하고, 그래프 색칠 문제를 낮은 복잡도로 해결할 수 있는 양자 알고리즘을 연구하였다. 특히, 복수개의 색을 할당하는 문제를 다색 색칠 문제로 변환 후 양자 알고리즘을 적용하여 더 많은 복잡도 이득을 얻었다. 단색 색칠 문제에서는 양자 알고리즘이 디지털 알고리즘 대비 복잡도 개선 효과를 볼 수 없었다. 하지만 더 복잡한 환경인 다색 색칠 문제에서 제안하는 기법인 input state를 설계하여 복잡도에서 큰 이득을 볼 수 있었다.

References

[1] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annual ACM Symp. Theory of Computing*, p. 212, Jul. 1996.

[2] M. A. Nielsen and I. L. Chuang, "*Quantum computation and quantum information*," Cambridge University Press, 2000.

[3] A. Mishra, S. Banerjee, and W. Arbaugh, "Weighted coloring based channel assignment for WLANs," *ACM SIGMOBILE Mobile Computing and Commun. Rev.*, vol. 9, no. 3, pp. 19-31, Jul. 2005.

[4] X. Ying, M. M. Buddhikot, and S. Roy, "SAS-Assisted coexistence-aware dynamic channel assignment in CBRS band," *arXiv:1805.06053v2* [cs.NI], Jul. 2018.

[5] A. P. Subramanian and H. Gupta, "Fast spectrum allocation in coordinated dynamic spectrum access based cellular networks," in *2nd IEEE Int. Symp. NewFrontiers in Dynamic Spectrum Access Netw.*, pp. 320-330, Apr. 2007.

[6] M. M. Buddhikot, et al., "Near-optimal dynamic spectrum allocation in cellular networks," in *3rd IEEE Symp. New Frontiers in Dynamic Spectrum Access Netw.*, pp. 1-11, Oct. 2008.

[7] F. Hessar and S. Roy, "Resource allocation techniques for cellular networks in tv white space spectrum," *IEEE Int. Symp. Dynamic Spectrum Access Netw.*, pp. 72-81, Apr. 2014.

[8] A. Bar-Noy, et al., "Sum multicoloring of graphs," *J. Algorithms*, vol. 37, no. 2, pp. 422-450, Nov. 2000.

[9] W. Dür, G. Vidal, and J. I. Cirac, "Three qubits can be entangled in two inequivalent ways," *Phys. Rev. A*, vol. 62, p. 062314, Nov. 2000.

[10] A. Eidenbenz, "Deterministic preparation of dicke states," *arXiv:1904.07358v1* [quant-ph] 15, Apr. 2019.

[11] P. Hansen, N. Brunswick, and B. Jaumard, "Experimental quantum algorithms for the maximum satisfiability problem," *Computing*, vol. 44, pp. 279-303, Oct. 1990.

민 건 식 (Gun-sik Min)

2018년 8월 : 고려대학교 전기전자전파공학부 학사 졸업

2020년 8월 : 고려대학교 전기전자공학부 석사 졸업

<관심분야> 양자컴퓨팅, 양자알고리즘, 채널 할당

허 준 (Jun Heo)

1989년 2월 : 서울대학교 전자공학과 학사 졸업
1991년 2월 : 서울대학교 전자공학과 석사 졸업
2002년 2월 : University of Southern California 박사 졸업
1991년~1996년 : LG전자 영상미디어 연구소, 주임연구원
1996년~2002년 : LG전자 중앙연구소, 선임연구원
2002년~2003년 : Hynix 반도체 System IC Comp. 책임연구원
2003년~2007년 : 건국대학교 전자공학부 조교수
2007년~2012년 : 고려대학교 전기전자공학부 부교수
2012년~현재 : 고려대학교 전기전자공학부 정교수
<관심분야> 양자 정보 이론, 양자 컴퓨팅, 양자 알고리즘, 채널 코딩,