Journal of the Korean Institute of Industrial Engineers
Vol. 46, No. 4, pp. 421-431, August 2020.
ISSN 1225-0988 | EISSN 2234-6457
https://doi.org/10.7232/JKIIE.2020.46.4.421

<Original Research>

게이트 패턴 기반 최적화 모형을 활용한 양자컴퓨팅 가역 논리 회로 합성

정지혜 · 최인찬†

고려대학교 산업경영공학과 시스템최적화연구실

Reversible Logic Circuit Synthesis for Quantum Computing via a Gate Pattern-based Optimization Model

Jihye Jung · In-Chan Choi

System Optimization Laboratory, Department of Industrial Management Engineering, Korea University

Quantum computing is the latest computing concept that can substantially reduce the computational burden of some difficult NP problems. Boolean reversible logic is frequently used as a key component in many quantum algorithms. This study proposes an approach based on a mixed integer programming model for reversible circuit synthesis. The proposed optimization model maps a given reversible function into a multiple-control Toffoli (MCT) circuit with minimum quantum costs. Our model exploits the relationship between MCT gate patterns and the operations on qubit states. We also report our experience in computational experiments on the circuit synthesis of reversible benchmark problems.

Keywords: Reversible Logic, Circuit Synthesis, Optimization Model, Quantum Computing, Mixed Integer Programming

1. 서 론

양자컴퓨팅은 양자역학의 불확정성을 활용하는 차세대 계산 환경으로, 소인수 분해, 이산 로그(Discrete Logarithm) 등의 어려운 NP 문제들에 대해 전통적 계산 환경에 비하여 효율적인 연산이 가능하다(Nielsen and Chuang, 2002). 양자컴퓨팅의 정보 단위인 큐빗(Qubit)은 전통적 계산 환경에서 활용되는 정보 단위인 비트(Bit)와 대응되는 개념으로서, 양자 중첩(Quantum Superposition) 및 양자 얽힘(Quantum Entanglement)과 같은 양자역학적 성질을 활용한다. 양자컴퓨팅에 대한 연구개발은 크게 하드웨어와 소프트웨어 측면의 두 방향으로 이루어지고 있다. 하드웨어 관련 연구의 경우, 규모와 안정성을 확보하여 실용성이 높은 양자컴퓨팅 기기를 개발하는 연구가 주를 이루고 있다(Kielpinski *et al*., 2002; Monroe *et al*., 2014). 소프트웨어 분야에서는 현실 활용도가 높은 양자 알고리즘의 개발과 더불어 효율적인 양자 회로 설계에 대한 연구가 진행되고 있다. 소인수 분해나 비정형 데이터베이스 탐색과 같이 기술적 중요도가 높으나 전통적 계산 환경에서 해결하기 어려운 연산들에 대해 이를 효율적으로 수행하는 양자 알고리즘 등이 해당 분야와 관련된 대표적인 연구 결과이다.

소인수 분해는 현대 암호 처리에 필수적인 연산으로, 전통적 계산 환경에서 지수시간(Exponential Time)의 계산복잡도를 갖는다. 대표적 양자 알고리즘인 쇼어 알고리즘(Shor's Algorithm)은 소인수 분해의 계산복잡도를 지수시간에서 다항시간(Polynomial Time)으로 대폭 개선한 알고리즘이다(Shor, 1994). 비정형 데이터베이스 탐색의 경우, 흔히 무작위로 뒤집혀 있는 N개의 카드들 중 특정 카드의 위치를 찾는 문제로 설명한다. 그로버 알고리즘(Grover's Algorithm)은 이와 같은 작업을 수행할 때에 데이터

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2017R1E1A1A03070988).
† 연락저자 : 최인찬 교수, 서울시 성북구 안암동 5가 고려대학교 자연계캠퍼스 공학관 521, Tel : 02-3290-3388, Fax : 02-3290-4550, E-mail : ichoi@korea.ac.kr
2019년 12월 27일 접수; 2020년 2월 4일 수정본 접수; 2020년 2월 21일 게재 확정.

베이스에 접근하는 횟수를 이차적(Quadratically)으로 개선하여 $O(\sqrt{N})$의 쿼리 복잡도(Query Complexity)만으로 답을 탐색하는 대표적인 양자 알고리즘이다(Grover, 1996; Figgatt *et al*., 2017).

위와 같은 활발한 연구에도 불구하고 물리적으로 구현된 기기가 갖는 상당한 계산 오차로 인해 아직은 현실 문제 해결에 범용 양자컴퓨팅을 활용하기가 어려운 실정이다. 이와 같은 물리적 오차를 보완하기 위해 하드웨어의 품질 개선뿐만 아니라 소프트웨어 분야에서도 결함 감내(Fault Tolerance) 알고리즘을 설계하는 연구들이 시도되고 있다(Preskill, 2018). 단위 양자 게이트(Quantum Gate)는 펄스 파동 등의 물리적 자극으로 구현되어 큐빗의 상태를 변화시킨다(Jaksch, 2008). 일반적으로 양자 알고리즘의 회로를 구성하는 단위 양자 게이트의 수가 많을수록 큐빗의 상태를 안정적으로 유지하기가 어려운데, 이는 물리적으로 구현된 큐빗이 안정적인 상태를 유지할 수 있는 시간인 결어긋남 시간(Decoherence Time)이 상당히 짧기 때문이다(Zurek, 2003). 따라서 양자 알고리즘의 계산정확도를 높이기 위해서는 적은 개수의 게이트를 사용함과 더불어 물리적 구현 비용이 낮은 게이트를 선택하여야 한다.

양자 알고리즘을 구성하는 모든 연산은 유니터리 변환(Unitary Transformation)이며, 그 중에서도 순열 행렬(Permutation Matrix)로 표현되는 이진 가역(Boolean Reversible) 연산은 양자 알고리즘의 핵심 요소로 활용된다. 이진 가역 연산은 다중 제어 토폴리 게이트(Multiple-Control Toffoli Gate)라는 논리 게이트를 활용한 회로로 매핑할 수 있는데, 이 때 각 논리 게이트를 구현하기 위해 필요한 단위 양자 게이트의 수를 양자 비용(Quantum Cost)이라 한다. 구현하고자 하는 다중 제어 토폴리 게이트의 제어 라인 개수가 많을수록 많은 단위 양자 게이트가 필요하기 때문에 양자 비용이 높다(Maslov and Dueck, 2003).

앞서 언급한 결함 감내 양자 알고리즘에 대한 연구의 일환으로, 본 연구에서는 진리표(Truth Table) 형태로 주어진 이진 가역 연산을 최소 양자 비용의 다중 제어 토폴리 회로로 설계하는 최적화 모형을 제안한다. 이 모형은 다중 제어 토폴리 게이트의 게이트 패턴과 게이트 작동 방식 간의 관계를 활용한다. 본 연구는 아래와 같은 두 가지 의의를 갖는다. 첫째, 제안된 방법론은 이진 가역 회로 합성 방법론에 수리 모형을 접목한 첫 연구로, 최적 가역 회로를 합성하는 기존의 방법론들에 비하여 강건성 높은 방법론에 대한 연구 방향을 제시한다. 둘째, 이 연구는 가역 회로 합성을 위한 수리모형에 다중 제어 토폴리 회로의 물리적 구현 비용인 양자 비용을 최소화하는 목적함수를 채택하여 가역 회로 합성을 양자컴퓨팅에 접목한다는 의의를 갖는다.

이 논문은 다음과 같이 구성된다. 제 2장에서는 이진 가역 연산의 회로 설계 방법론 및 회로 평가 지수에 대한 대표적 선행 연구들을 제시하며, 제 3장에서는 양자컴퓨팅 및 이진 가역 연산에 대한 배경 개념을 설명한다. 제 4장에서는 해결하고자 하는 문제에 대한 설명과 모형화 아이디어를 제시하며, 이어지는 제 5장에서는 해당 아이디어를 활용해 구성한 최적화 모형을 설명한다. 제 6장에서는 벤치마크 데이터에 대해 해당 모형을 적용하여 실험한 결과를 제시하며, 제 7장에서는 이 연구의 결론 및 추후 연구의 방향을 제안한다.

2. 선행 연구에 대한 고찰

양자컴퓨팅 및 양자 알고리즘 연구의 일환으로 효율적인 양자 회로 및 가역 회로 합성을 위한 연구가 진행되어 왔다. 게이트 개수, 계산속도, 양자 비용, 큐빗 상호작용 비용, 보조 큐빗 개수, 회로 깊이 등이 회로의 효율성을 평가하는 대표적인 지표들이다(Saeedi and Markov, 2013). 특히 양자 비용은 논리 게이트의 물리적인 구현에 필요한 단위 양자 게이트의 총 개수를 의미하기 때문에 실질적인 회로의 비용을 표현할 수 있다. 양자 비용에 대한 연구들을 통해 양자 게이트 및 양자 회로의 비용 체계가 정립되어 왔다(Barenco *et al*., 1995; Shende and Markov, 2008).

회로 평가 지표를 이용하여 효율적인 가역 회로를 합성하는 방법론에 대한 연구가 다수 존재한다. 초기 연구는 직관적인 관찰에 의한 회로의 특성과 사전에 구성된 회로 라이브러리를 활용하는 방법론이 주를 이룬다. 대표적으로 작은 규모의 가역 연산들에 대한 회로 라이브러리를 먼저 구성하고, 이를 활용한 템플릿 매칭(Template Matching)과 관찰을 통해 큰 사이즈의 가역 회로를 합성하는 방법론들이 존재한다(Miller *et al*., 2003; Golubitsky and Maslov, 2011; Szyprowski and Kerntopf, 2011). 위와 같은 방법론을 이용해 큰 규모의 가역 회로를 합성한 후 결과 회로에 대한 재배치 알고리즘 등의 사후 최적화에 대한 연구들이 진행되어 왔다(Prasad *et al*., 2006; Saeedi *et al*., 2010).

체계적 탐색 방식을 활용한 회로 합성 방법론들에 대한 연구도 존재한다. 이진 함수를 이진 변수들의 곱의 합으로 표현하는 리드-뮬러 분해(Reed-Muller Decomposition)와 우선순위 기반의 탐색 나무(Search Tree)를 활용한 휴리스틱 알고리즘을 활용하여 양자 비용을 개선하는 연구들이 진행되어 왔다(Agrawal and Jha, 2004; Gupta *et al*., 2006). 상대적으로 큰 규모의 회로를 다루기 위해 이진 의사결정 다이어그램(Binary Decision Diagram)을 활용하기도 하였다(Wille and Drechsler, 2009). 평가 함수를 기반으로 탐색 그래프 내의 최적 경로를 추정하여 탐색에 활용하는 에이-스타 알고리즘(A* Algorithm)을 가역회로 합성에 접목한 연구 또한 제안되었다(Datta *et al*., 2012). 휴리스틱 기반의 가역회로 합성은 규모가 큰 문제에 적용할 수 있지만, 최적성이 보장되지 않으며 물리적 구현을 위한 제약조건을 충분히 고려하지 못한다는 단점이 있다.

이러한 휴리스틱 알고리즘의 단점을 보완하기 위해 회로의 사후 최적화에 초점을 맞춘 알고리즘들이 제안되어 왔다. 대표적으로 템플릿 기반의 회로 단순화를 통한 휴리스틱 알고리즘(Maslov *et al*., 2007; 2008)과 더불어, 회로의 물리적 구현 시 고려되는 큐빗 간 상호작용 및 선형 최근접 이웃(Linear Nearest Neighbor) 제약을 만족시키기 위한 회로 재배치 알고리즘에 대한

연구가 존재한다(Wille *et al*., 2010; Hirata *et al*., 2011).

최적성이 보장된 가역 회로를 합성하기 위하여 SAT 문제(Satisfiability Problem) 모형을 활용하여 양자 비용 및 게이트 개수를 최소화하는 연구 또한 진행되었으나(Große *et al*., 2009), 해결 가능한 문제의 크기가 제한적이라는 한계점을 가진다. 최적에 가까운 가역 회로의 탐색을 위해 진화적 메타 휴리스틱(Evolutionary Metaheuristics)을 활용한 방법론들이 제시되기도 하였는데, 적응적 유전 알고리즘(Adaptive Genetic Algorithm)(Sasamal *et al*., 2015)과 유전 프로그래밍(Genetic Programming)(Abubakar *et al*., 2017) 등을 활용한 연구가 그 대표적인 예다.

3. 배경 지식

3.1 큐빗

큐빗은 양자컴퓨팅에서 활용하는 정보 단위로, 전통적 컴퓨팅 환경에서 사용되는 정보 단위인 비트와는 다르게 확률적인 성질을 갖는다. 비트의 경우, 0 또는 1 중 하나만의 상태를 확정적으로 저장하는 반면 큐빗은 상태 $|0\rangle$과 상태 $|1\rangle$에 대한 확률 정보를 포함하며 그 확률 분포에 따라 $|0\rangle$과 $|1\rangle$ 중 하나의 상태가 관측된다. 이러한 현상을 일컬어 양자 중첩(Quantum Superposition)이라 한다.

단일 큐빗의 양자 상태는 블로흐 구면(Bloch Sphere)을 통해 기하학적으로 표현할 수 있다. 구면의 최상단과 최하단은 각각 $|0\rangle$과 $|1\rangle$을 표현하며, 구체 내의 화살표의 위치를 통해 다양한 중첩 상태를 나타낸다. <Figure 1(a)>와 <Figure 1(b)>의 경우, 블로흐 구면은 각각 $|0\rangle$과 $|1\rangle$을 확정적으로 표현하고 있다. 반면, <Figure 1(c)>는 두 계산적 기저 상태가 동일하게 50% 확률로 관측될 중첩 상태를 표현하고 있으며, <Figure 1(d)>의 경우 $|0\rangle$과 $|1\rangle$이 각각 75%와 25%의 확률로 관측될 중첩 상태를 표현하고 있다.

3.2 계산적 기저 상태 (Computational Basis State)

큐빗은 확률 분포에 따라 관측 시 상태가 $|0\rangle$ 혹은 $|1\rangle$로 나타날 수도 있는 확률적인 성질을 갖는다. 이와 같이 관측 가능한 큐빗의 상태를 계산적 기저 상태라 한다. 일반적으로 기저 상태는 브라-켓 표기법(Bra-ket Notation)에 따라 $|0\rangle$과 $|1\rangle$로 표현하며, 1의 값을 갖는 원소가 1개인 2차원 단위 벡터로 표현하기도 한다. 이 때, 단일 큐빗에 대한 기저 상태의 중첩은 아래 식 (1)과 같이 기저 상태들의 선형결합으로 나타낸다. 각 선형 결합 계수는 해당 기저 상태가 관측될 확률에 대한 정보를 담고 있다.

$$|\psi\rangle = \alpha_1|0\rangle + \alpha_2|1\rangle = \alpha_1\begin{bmatrix}1\\0\end{bmatrix} + \alpha_2\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}\alpha_1\\\alpha_2\end{bmatrix} \quad (1)$$

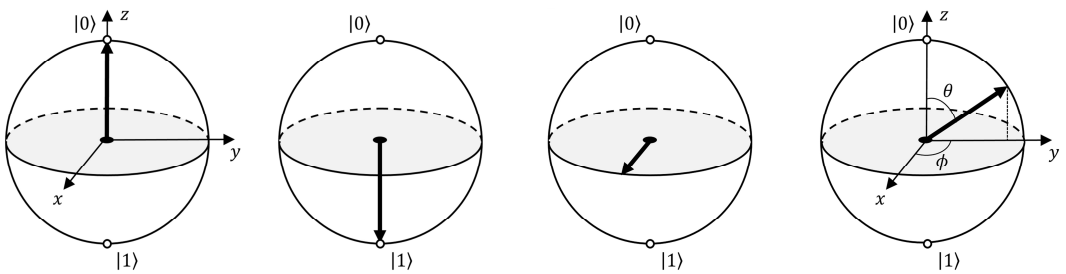
단일 큐빗의 양자 상태에 대한 식 (1)을 n개의 큐빗들이 갖는 양자 상태에 대한 식으로 확장하면 2^n개의 계산적 기저 상태에 대한 선형결합으로 표현이 가능하다. 각 큐빗들은 $|0\rangle$ 또는 $|1\rangle$의 2가지 기저 상태를 가질 수 있으며, 이러한 성질을 가진 큐빗이 n개 존재하기 때문이다. 아래 식 (2)는 n개의 큐빗들이 갖는 양자 상태를 각 기저 상태의 선형 결합으로 표현한 식이다. 기저 상태를 벡터로 표기하면 주어진 n개 큐빗들의 양자 상태는 하나의 2^n차원 복소수 벡터로 표현할 수 있다. 식 (2)와 같이 다수의 큐빗을 하나의 개체로 취급하는 경우 이를 큐빗 레지스터(Qubit Register)라고 한다.

$$|\psi\rangle = \alpha_1|00\cdots0\rangle + \alpha_2|00\cdots1\rangle + \cdots + \alpha_{2^N}|11\cdots1\rangle \quad (2)$$

$$= \alpha_1\begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix} + \alpha_2\begin{bmatrix}0\\1\\\vdots\\0\end{bmatrix} + \cdots + \alpha_{2^N}\begin{bmatrix}0\\0\\\vdots\\1\end{bmatrix} = \begin{bmatrix}\alpha_1\\\alpha_2\\\vdots\\\alpha_{2^N}\end{bmatrix}$$

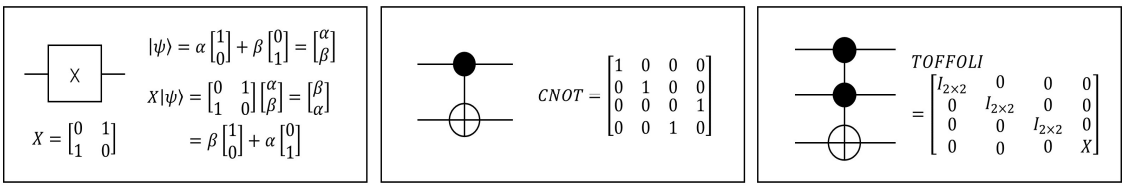
3.3 가역 논리 게이트

가역 논리 게이트란 이진 가역 연산을 실현한 논리 게이트로, 순열 행렬(Permutation Matrix)로 표현 가능하다(Saeedi and Markov, 2013). 가역 논리 게이트는 양자 논리 게이트의 부분집합으로, 양자 기본 게이트로써 표현할 수 있다. 이러한 형태를 만족하는 다수의 게이트 라이브러리들 중 이 연구에서 활용하는 다중 제어 토폴리 게이트 라이브러리의 경우 0개 이상의 제어 라인(Control Line)과 1개의 목표 라인(Target Line)으로 구성된 모든 게이트들을 일컫는다. 특별히 제어 라인이 0개일 때 NOT 게이트, 1개일 때 CNOT 게이트, 2개일 때 토폴리 게이트(Toffoli Gate)라고 불린다(<Figure 2> 참조).



(a) $\theta = 0, \phi = 0$ (b) $\theta = \pi, \phi = 0$ (c) $\theta = \pi/2, \phi = 0$ (d) $\theta = \pi/3, \phi = \pi/2$

Figure 1. Examples of Quantum States Represented in Bloch Sphere form



(a) NOT gate (b) CNOT gate (c) Toffoli gate

Figure 2. Various Types of Reversible Gates and their Matrix Representations

NOT 게이트는 단일 큐빗 게이트로, 해당 큐빗에 대응되는 기저 상태를 반대로 뒤집는 역할을 한다. <Figure 2(a)>와 같이 특정 큐빗에 대응되는 라인에 NOT 게이트가 존재하는 경우, 선형 결합 계수의 값 자체는 변하지 않으나 계산적 기저 상태 $|0\rangle$과 $|1\rangle$이 서로 뒤집히며 선형 결합 계수를 교환하는 연산이 이루어진다. CNOT 게이트의 경우, 제어 라인이 1개인 다중 제어 토폴리 게이트의 일종으로 양자 얽힘을 형성하기 위해 중요한 역할을 수행하는 논리 게이트다. 제어 라인에 대응되는 큐빗의 기저 상태가 $|1\rangle$인 경우, 목표 라인에 대응되는 큐빗에 NOT 게이트가 작동된다. 제어 라인 2개와 목표 라인 1개로 이루어진 토폴리 게이트 또한 입력된 기저 상태에서 2개 제어 라인에 대응되는 큐빗의 기저 상태가 모두 $|1\rangle$인 경우 목표 라인에 NOT 게이트를 작동시키는 게이트이다.

3.4 양자 게이트와 양자 비용

양자 게이트는 특정 유니터리 변환(Unitary Transformation)을 물리적으로 구현한 기기이다. 유니터리 변환이란 특정 변환 U를 행렬로 표현한 후 해당 행렬을 자기 자신의 복소수 전치 행렬인 $U^{\dagger}$와 곱할 시 단위행렬이 되는 모든 변환을 일컫는다. 기본적인 양자 게이트로는 하다마드(Hadamard) 게이트, 위상 변환(Phase Shift) 게이트, 제어- V(Controlled- V) 게이트, 제어- $V^{\dagger}$(Controlled- $V^{\dagger}$) 게이트, 파울리(Pauli) 게이트 등이 있다.

이 연구에서 활용한 다중 제어 토폴리 게이트 라이브러리 중 NOT 게이트와 CNOT 게이트를 제외한 나머지 게이트는 물리적인 구현을 위해 단위 양자 게이트로의 재표현이 필요하다. 제어 라인의 개수가 많은 다중 제어 토폴리 게이트일수록 물리적 구현 시 필요한 단위 양자 게이트의 개수가 많아지며, 이 때 필요한 단위 양자 게이트의 개수를 해당 게이트의 양자 비용이라고 한다. <Table 1>은 다중 제어 토폴리 게이트의 제어 라인 개수에 따른 양자 비용을 제시한다(Große *et al*., 2009).

Table 1. Quantum Costs of Multiple Control Toffoli Gates According to their Number of Control Lines

No. of control lines	Quantum costs
0 (NOT gate)	1
1 (CNOT gate)	1
2 (Toffoli gate)	5
3	13
4	26, if at least 2 lines are empty 29, otherwise
5	50, if at least 4 lines are empty 80, if at least 1-3 lines are empty 125, otherwise

4. 문제 설명 및 아이디어

4.1 문제 설명

가역 회로로 표현하고자 하는 이진 가역 함수는 입력 기저 상태와 출력 기저 상태의 관계를 나타내는 진리표의 형태로 제시된다. 이 때 진리표의 출력값은 미결정 비트(Don't Cares)를 포함할 수 있다. 미결정 비트란 출력 값이 확정되지 않은 비트로, 0 또는 1의 값들 중에 어느 값을 가져도 상관없는 출력 비트이다. <Table 2>는 이진 가역 함수의 예시를 진리표로 제시한다. <Table 2(a)>는 미결정 비트를 포함하지 않는 경우, <Table 2(b)>는 미결정 비트를 포함하는 경우이다(Wille *et al*., 2008).

Table 2. Example of Boolean Reversible Functions

(a) peresgate

Input	Output
000	000
001	011
010	010
011	101
100	100
101	111
110	110
111	001

(b) decod24

Input	Output	Input	Output
0000	0001	1000	----
0001	0010	1001	----
0010	0100	1010	----
0011	1000	1011	----
0100	----	1100	----
0101	----	1101	----
0110	----	1110	----
0111	----	1111	----

문제에서 주어진 이진 가역 함수를 가역 회로로 표현하기 위해 다중 제어 토폴리 게이트 라이브러리를 활용한다. 주어진 가역 함수를 가역 회로로 표현하기 위해 사용할 수 있는 게이트의 최대 개수는 상수로 주어지는데, 이 상수는 선행 연구들에서 동일한 가역 함수를 가역 회로로 표현한 결과 사용된 게이트 개수 중 최소값으로 결정된다. 이 연구에서 제시하는 수리모형은 진리표 형태로 주어진 이진 가역 함수와 동일한 연산을 수행하는 최소 양자 비용의 회로를 탐색하는 것을 목적으로 한다.

4.2 모형에 사용된 성질

이 연구는 다중 제어 토폴리 게이트의 게이트 패턴과 게이트 작동 방식 간의 관계에 대한 관찰을 통해 발견한 2개의 성질을 기반으로 한다. 게이트 패턴은 목표 라인의 위치 및 제어 라인의 위치 패턴으로 나누어 설명된다. 또한 다중 제어 토폴리 게이트는 큐빗 레지스터의 계산적 기저 상태가 갖는 선형 결합 계수를 서로 교환하는 방식으로 작동하는데, 이러한 작동방식을 교환쌍의 형성 규칙과 각 교환쌍의 작동 여부를 결정하는 규칙으로 나누어 설명한다. 성질 (1)은 목표 라인의 위치와 교환쌍의 형성 규칙 간의 관계를, 성질 (2)는 제어 라인 위치 패턴과 교환쌍의 작동 여부 간의 관계를 정의한다.

성질 (1) 목표 라인의 위치와 교환쌍(Permutation Pair) 간의 관계

모든 다중 제어 토폴리 게이트는 순열 행렬로 나타냈을 때, 선형 결합 계수를 교환하는 기저 상태들이 서로 쌍을 이루어 나타난다. 다중 제어 토폴리 게이트는 제어 라인에 대응되는 큐빗들의 기저 상태에 따라 목표 라인의 NOT 게이트 작동 여부를 결정한다. 따라서 목표 라인을 제외한 나머지 라인에 대응되는 큐빗 레지스터의 계산적 기저 상태가 동일한 경우, 목표 라인에 대응되는 큐빗에 대해서만 $|0\rangle$과 $|1\rangle$이 서로 뒤집히게 되어 선형 결합 계수(관측 확률 정보)를 교환하는 교환쌍의 관계를 갖게 된다.

<Figure 3(a)>는 A, B, C 3개의 큐빗으로 이루어진 큐빗 레지스터의 8개 계산적 기저 상태를 표현한다. 표기상 편의를 위해 각 계산적 기저 상태를 이진수로 환산한 후 그 값의 오름차순으로 자연수 번호를 붙인다. <Figure 3(b)>와 같이 큐빗 A에 목표 라인을 설정하면 큐빗 B와 C에 대응되는 상태가 동일한 계산적 기저 상태만이 서로 선형 결합 계수를 교환할 수 있기 때문에 교환 쌍이 (1 ↔ 5), (2 ↔ 6), (3 ↔ 7), (4 ↔ 8)로 결정된다. <Figure 3>의 예시를 통해 계산적 기저 상태의 교환 쌍은 실제 회로 상의 목표 라인의 위치에 따라 결정되는 것을 알 수 있다.

성질 (2) 게이트 스키마(Gate Schema)와 교환쌍 작동 여부와의 관계

성질 (1)에 의해 목표 라인의 위치에 따라 구성된 교환쌍 후보 중 실제로 작동될 교환쌍은 제어 라인들의 위치 패턴을 표현하는 게이트 스키마(Gate Schema)에 의해 결정된다. 각 교환쌍 후보와 게이트 스키마에 간에 일대일 대응 관계를 형성한 후, 주어진 다중 제어 토폴리 게이트와 맞아떨어지는 게이트 스키마를 선택한다. 선택된 게이트 스키마와 대응되는 교환쌍이 해당 다중 제어 토폴리 게이트를 통해 서로 선형 결합 계수를 교환하는 계산적 기저 상태이다.

이 연구에서 게이트 스키마란 목표 라인의 위치가 결정되었을 때 목표 라인 외의 라인들에 대해 게이트가 걸리지 않은 공라인(Empty Line)의 위치 패턴을 나열한 것을 의미한다. 목표 라인은 T, 공라인을 N, 공라인 혹은 제어 라인 모두 무관한 라인을 *로 표현한다(<Figure 3(c)> 참조). 이 때, 목표 라인을 제외한 큐빗들에 대해 N을 0, *를 1에 대응하면 각 게이트 스키마에 대응되는 이진수를 결정할 수 있으며, 그 크기의 내림차순에 따라 게이트 스키마를 정렬한다. 성질 (1)을 통해 결정된 교환쌍 후보들 또한 각 교환쌍을 이루는 두 계산적 기저 상태에 부여한 자연수 번호 중 최소값에 대해 내림차순으로 정렬한다. 이렇게 정렬된 게이트 스키마와 교환쌍 간에 순서대로 일대일 대응 관계를 형성한다. 주어진 다중 제어 토폴리 게이트에 일치하는 게이트 스키마를 선택한 뒤, 미리 형성해둔 일대일 대응 관계를 활용해 활성화시킬 교환쌍을 선택한다. 해당 교환쌍에 포함되는 계산적 기저 상태들이 주어진 다중 제어 토폴리 게이트에 의해 서로 선형 결합 계수를 교환하게 된다.

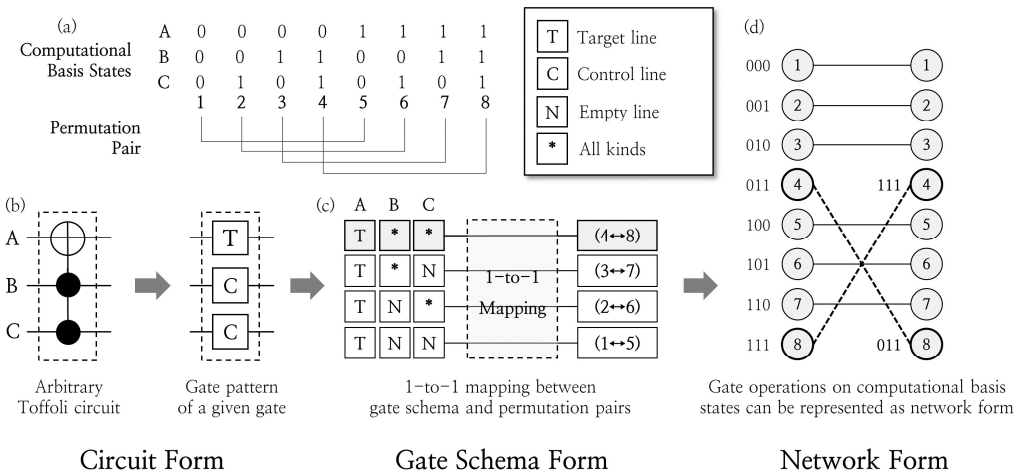


Figure 3. Relationship between Multiple Control Toffoli Gate and Permutation Pairs

<Figure 3(b)>의 토폴리 게이트를 예시로 살펴보면, 큐빗 A에 대응되는 목표 라인을 가지므로 그에 상응하는 교환쌍 후보가 형성되었다(<Figure 3(a)> 참조). 또한 앞서 설명된 순서에 따라 각 교환쌍이 큐빗 B, C에 대한 게이트 스키마와 일대일 대응 관계를 형성하였다(<Figure 3(c)> 참조). 주어진 게이트는 목표 라인을 제외한 모든 라인이 제어 라인이므로 공라인을 의미하는 N을 포함한 모든 게이트 스키마가 주어진 게이트와 일치하지 않는다는 것을 알 수 있다. 따라서 주어진 게이트는 게이트 스키마 (T, *, *)와만 일치하며, 작동하는 교환쌍은 $(4 \leftrightarrow 8)$ 뿐이다. 이를 계산적 기저 상태로 표현하면 $|011\rangle$과 $|111\rangle$이 서로 선형 결합 계수를 교환한다는 것을 의미한다. 위와 같은 게이트 작동방식은 <Figure 3(d)>와 같이 네트워크로 표현할 수 있어 문제를 모형화하는 주요한 아이디어로 활용되며, 관련된 자세한 내용은 제 4.3절에서 제시한다.

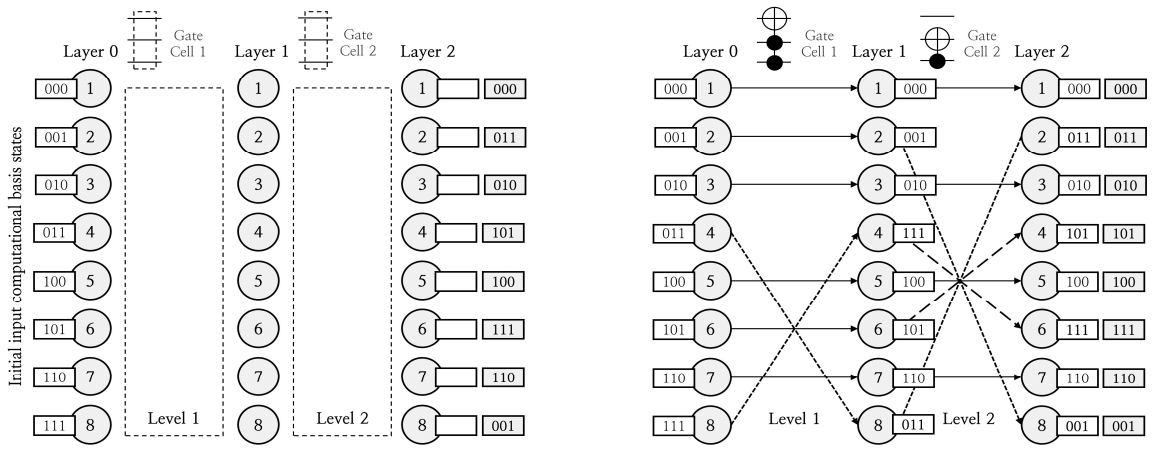
4.3 모형화 아이디어

다중 토폴리 게이트로 이루어진 회로의 작동 방식은 유방향 층화 네트워크(Directed Layered Network)로 표현 가능하며, <Figure 4>는 <Table 2(a)>의 *peresgate*를 예시로 삼아 회로와 네트워크 관점의 대응관계를 보여준다. 먼저 회로 관점에서 문제를 정의하기 위해 문제에서 주어진 전체 큐빗 개수 n_Q와 최대 가용 게이트 수 n_D를 통해 <Figure 4(a)>와 같이 빈 회로를 구성한다. $n_D = 2$, $n_Q = 3$인 *peresgate*의 경우 2개의 게이트 셀과 각 게이트 셀 내의 3개 큐빗 셀이 구성된다. 각 큐빗 셀에는 목표 라인, 제어 라인, 공라인 중 하나가 할당된다. 회로단에서 결정된 각 다중 제어 토폴리 게이트는 제 3.3절에서 설명된 바와 같이 입력된 양자 상태의 기저 상태 선형결합 계수를 교환시키는데, 이러한 게이트 작동 방식을 유방향 층화 네트워크 내의 아크로 표현한다.

게이트 작동 방식을 표현하는 유방향 층화 네트워크는 총 (n_D+1)개의 레이어(Layer)로 구성되며, 각 레이어 내에는 2^{n_Q}개의 노드(Node)가 포함된다. 아크(Arc)는 인접한 두 레이어의 사이에만 형성되며, 인접한 레이어 간의 n_D개 공간을 레벨(Level)이라 정의한다. 각 레벨 상의 아크들을 통해 인접한 레이어 내의 노드들은 서로 일대일 대응을 이룬다. 각 레이어는 게이트를 지나기 전후의 양자 상태를 표현하며, 특히 레이어 0은 초기 양자 상태를, 레이어 n_D는 회로를 모두 거친 후 최종 양자 상태를 표현한다. 레이어 내의 노드는 양자 상태를 선형결합으로 구성하는 각 기저 상태에 대응된다. 각 레벨은 게이트 셀에 대응되는데, 해당 게이트 셀 내에 결정된 게이트의 기저 상태 교환쌍을 레벨 상의 유방향 아크로 표현한다. 즉 주어진 문제는 초기 레이어를 출발한 기저 상태가 목표한 최종 레이어에 도착할 수 있도록 각 레벨 상의 아크를 구성하고자 하며, 이 아크들은 해당 레벨에 대응되는 게이트 셀 내의 다중 제어 토폴리 게이트에 의해 정해진다. 위와 같은 조건을 모두 만족함과 동시에 각 게이트 셀 내의 다중 제어 토폴리 게이트의 양자비용을 최소화하는 것이 문제의 목표이다.

<Figure 4(b)>는 위의 모형화 아이디어를 *peresgate*에 적용한 결과를 표현한다. 레이어 0 내의 노드는 게이트 셀을 지나기 전의 초기 기저 상태가 배치되어 있으며, 각 기저 상태는 이진수로 환산한 값의 오름차순의 순서를 따른다. 또한, 문제에서 주어진 진리표를 기반으로 마지막 레이어인 레이어 2의 각 노드에 목표 출력 기저 상태가 결정된 상태이다. <Figure 4(a)>의 비어있는 게이트 셀에 각각 토폴리 게이트와 CNOT 게이트가 채워지면 제 4.2절의 성질들을 활용하여 해당 게이트의 작동 방식을 <Figure 4(b)>의 아크와 같이 표현할 수 있다.

예를 들어, 게이트 셀 1에 주어진 토폴리 게이트의 경우 제 4.2절의 성질 2에 따라 1개의 교환 쌍만 작동하게 되며, 이를 통해 레벨 1을 지난 뒤 계산적 기저 상태 011과 111은 네트워크상에서 그 위치를 교환하게 된다. 게이트 셀 2에 주어진 토폴리 게이트의 경우 2개 교환 쌍이 발생하게 되는데, 그 대상은 기저 상태를 나타내는 이진수의 세 번째 자리에 1을 포함한 기저 상태들인 001, 011, 101, 111이다. 이들은 제 4.2절의 성질 1에 따라 쌍을 이루어 위치를 교환한다. <Figure 4(b)>의 게이트 조합으로 인해 초기 입력 기저 상태가 네트워크를 따라 움직이며 서로 위치를 교환하였고, 그 결과 각 기저 상태가 적절한 목표 노드에 도착한 것을 확인할 수 있다.



(a) Empty network layout of *peresgate* (b) Network representation of *peresgate* Toffoli circuit

Figure 4. Network form Representation of Reversible Circuit Synthesis

5. 수리모형

5.1 집합 및 인덱스

이 연구에서 제안하는 수리모형은 다음과 같은 집합과 인덱스 체계를 따른다.

$q \in Q$ 큐빗 인덱스의 집합으로, 총 큐빗 개수 $|Q| = n_Q$는 상수

$d \in D$ 게이트 셀 인덱스의 집합으로, 총 게이트 셀 개수 $|D| = n_D$는 상수

$i, j \in M$ 각 레이어의 노드 집합으로, 레이어 당 노드의 개수는 $2^{|Q|}$개

$k \in M$ 계산적 기저 상태의 집합으로, 총 기저 상태의 개수는 $2^{|Q|}$개

$S_q \in P_q$ 목표 라인이 q번째 큐빗에 존재하는 다중 제어 토폴리 게이트의 게이트 스키마 집합으로, 각 게이트 스키마 S_q는 공라인(N)에 대응되는 큐빗 인덱스 집합으로 표현

r_{S_q} 게이트 스키마 S_q의 인덱스

$(k_1, k_2) = g(r_{S_q})$ 게이트 스키마 S_q의 인덱스를 입력하면 해당 게이트 스키마와 대응되는 교환쌍으로 변환하는 함수로, 2개의 기저 상태 k_1, k_2를 출력

$t \in T_i$ 마지막 레이어의 노드 i에 도착할 수 있는 기저 상태의 인덱스 집합

QC_q q개의 제어 라인을 가진 다중 제어 토폴리 게이트의 양자 비용

5.2 결정변수

이 연구에서 제안하는 수리모형은 다음과 같은 결정변수들을 가지며, 그 역할과 의미에 따라 4개의 모듈로 나뉜다.

회로 결정 모듈 : 회로 내에서 목표라인 및 공라인의 위치를 결정한다.

t_q^d 게이트 셀 d의 큐빗 q가 목표 라인인 경우 1인 이진 변수

e_q^d 게이트 셀 d의 큐빗 q가 공라인인 경우 1인 이진 변수

ξ^d 게이트 셀 d에 게이트가 형성된 경우 1인 이진 변수

R_q^d 게이트 셀 d에 q개 큐빗이 공라인에 해당되는 경우 1인 이진 변수

회로-게이트 스키마 관계 모듈 : 각 게이트에 적합한 게이트 스키마를 결정한다.

$Y_{qr_{S_q}}^d$ 게이트 셀 d의 목표 비트가 q번째 큐빗에 존재하며, 게이트 스키마 S_q와 일치하는 경우 1인 이진 변수

목적함수 모듈 : 각 게이트 셀의 양자 비용을 표현한다.

z^d 게이트 셀 d의 양자 비용을 나타내는 실수 변수

네트워크 결정 모듈 : 아크 발생 여부와 기저 상태의 노드 방문 여부를 결정한다.

p_{ij}^d 게이트 셀 d에 대응되는 레벨 d 상에 아크 (i,j)가 형성된 경우 1인 이진 변수

f_{ik}^d 기저 상태 k가 레이어 d의 i번째 노드를 방문한 경우 1인 이진 변수

5.3 목적함수와 제약조건

$$\min \sum_{d \in D} z^d \tag{0}$$

$$t_q^d + e_q^d \le 1 \qquad \forall q \in Q, \forall d \in D \tag{1}$$

$$\sum_{q \in Q} R_q^d = 1 \qquad \forall d \in D \tag{2}$$

$$\sum_{q \in Q} e_q^d = \sum_{q \in Q} q R_q^d \qquad \forall d \in D \tag{3}$$

$$\xi^d = \sum_{q \in Q \cup \{0\} - \{|Q|\}} R_q^d \qquad \forall d \in D \tag{4}$$

$$\xi^d = \sum_{q \in Q} t_q^d \qquad \forall d \in D \tag{5}$$

$$\xi^{d+1} \le \xi^d \qquad \forall d \in D - \{|D|\} \tag{6}$$

$$\sum_{i \in M} p_{ii}^d + 2 \sum_{j \in M} \sum_{S_q \in P_q} Y_{qr_{S_q}}^d = 2^{|Q|} \qquad \forall q \in Q, \forall d \in D \tag{7}$$

$$\left(t_q^d + \sum_{q \in S_Q} e_q^d \right) \times \frac{1}{N(S_q)+1} - \nu \le Y_{qr_{S_q}}^d \qquad \forall q \in Q, \forall d \in D, \forall S_q \in P_q \tag{8}$$

$$\left(t_q^d + \sum_{q \in S_Q} e_q^d \right) \times \frac{1}{N(S_q)+1} \ge Y_{qr_{S_q}}^d \qquad \forall q \in Q, \forall d \in D, \forall S_q \in P_q \tag{9}$$

$$t_q^d \ge Y_{qr_{S_q}}^d \qquad \forall q \in Q, \forall d \in D, \forall S_q \in P_q \tag{10}$$

$$f_{ik_1}^{d-1} + f_{ik_2}^{d-1} - 1 \le p_{ij}^d + \left(1 - Y^{d_{qr_{S_q}}}\right) \qquad \forall q \in Q, \forall d \in D, \forall S_q \in P_q, \forall i,j \in M, \forall (k_1,k_2) \in g(r_{S_q}) \tag{11}$$

$$p_{ij}^d = p_{ji}^d \qquad \forall i,j \in M \tag{12}$$

$$z^d = \sum_{q \in Q} QC_{(q-1)} R_{|Q|-q}^d \qquad \forall d \in D \tag{13}$$

$$p_{ij}^d + f_{ik}^{d-1} - 1 \le f_{ik}^d \qquad \forall d \in D, \forall i,j,k \in M \tag{14}$$

$$\sum_{k \in M} f_{ik}^d = 1 \qquad \forall d \in \{0\} \cup D, \forall i \in M \tag{15}$$

$$\sum_{i \in M} f_{ik}^d = 1 \qquad \forall d \in \{0\} \cup D, \forall k \in M \tag{16}$$

$$f_{ii}^0 = 1 \qquad \forall i \in M \tag{17}$$

$$\sum_{t \in T_i} f_{it}^{|D|} = 1 \qquad \forall i \in M \tag{18}$$

$$\sum_{j \in M} p_{ij}^d = 1 \qquad \forall d \in D, \forall i \in M \tag{19}$$

$$t_q^d, e_q^d, R_q^d \in \{0,1\} \qquad \forall q \in Q, \forall d \in D \tag{20}$$

$$p_{ij}^d \in \{0,1\} \qquad \forall d \in D, \forall i,j \in M$$

$$\xi^d \in \{0,1\} \qquad \forall d \in D$$

$$f_{ik}^d \in \{0,1\} \qquad \forall d \in D, \forall i,k \in M$$

$$Y_{qr_{S_q}}^d \in \{0,1\} \qquad \forall q \in Q, \forall d \in D, \forall S_q \in P_q$$

위의 식 (0)~(19)는 이 연구에서 제안하는 수리모형을 표현하는 수식이다. 목적함수 (0)은 각 게이트 셀에 할당된 다중 제어 토폴리 게이트의 총 양자비용을 최소화한다는 모형의 목적을 표현한다. 제약식 (1)~(6)은 회로 결정 모듈 관련 조건들로, 다중 제어 토폴리 게이트를 이용한 회로를 구성할 때에 필수적인 조건들이다. 제약식 (1)의 경우 각 게이트 셀 내의 각 큐빗은 목표 라인, 제어 라인, 공라인 중 하나만 할당된다는 조건을 표현한다. 제약식 (2)는 각 게이트 셀 내의 공라인의 개수를 결정하는 식이다. 제약식 (3)은 각 게이트 셀에 존재하는 공라인의 개수를 이진 변수로 나타내는 식으로, 양자비용은 각 게이트 셀 내의 제어라인 개수에 의해 결정되기 때문에 목적함수의 양자비용의 계산에 활용된다. 제약식 (4)와 (5)의 경우, 특정 게이트 셀이 사용되지 않는 경우 공라인과 목표라인이 할당되지 않도록 한다. 제약식 (6)의 경우, 연속된 게이트 셀에만 게이트를 할당하도록 하는 조건이다.

제약식 (7)~(12)는 회로-게이트 스키마 관계 모듈과 관련된 제약조건이다. 제약식 (7)은 각 게이트 셀에 할당된 다중 제어 토폴리 게이트의 작동 형태는 총 $2^{|Q|}$개 아크로 표현된다는 조건이다. 제약식 (8)~(9)는 특정 게이트 셀에 존재하는 목표라인과 공라인의 패턴과 일치하는 게이트 스키마를 결정하는 식이다. 특정 게이트 스키마에 포함된 라인이 게이트 셀 내에 공라인으로 모두 결정되어 있다면 해당 게이트 셀과 게이트 스키마 간의 대응 관계를 형성한다. 제약식 (10)의 경우, 해당 게이트 셀에 목표 비트가 할당되지 않으면 게이트 셀을 사용하지 않는다는 의미이므로 게이트와 일치하는 게이트 스키마는 없다는 조건을 표현한다. 제약식 (11)은 할당된 게이트 스키마에 따라 인접한 단계 사이의 아크를 형성하고, 형성된 아크에 따라 각 기저 상태의 단계별 위치를 할당하는 역할을 수행한다. 제약식 (12)은 4.2절의 성질 1을 표현하기 위한 식으로, 모든 기저 상태는 서로 쌍을 이루어 위치를 변경한다는 조건이다. 제약식 (13)은 목적함수 모듈을 구성하는 유일한 제약조건으로, 각 게이트 셀에 존재하는 공비트의 개수에 따라 양자 비용을 할당하여 목적함수 계산을 보조하는 역할을 수행한다.

제약식 (14)~(19)은 네트워크 결정 모듈로, 네트워크가 주어진 가역 함수를 표현하도록 결정하기 위해 만족해야 하는 조건들로 구성된다. 제약식 (14)는 특정 아크가 결정되면 해당 아크의 머리 노드(Head node)에 있던 기저 상태가 꼬리 노드(Tail node)로 이동한다는 조건을 표현한다. 제약식 (15)는 각 노드는 1개의 기저 상태만이 방문할 수 있다는 조건을 의미하며, 제약식 (16)은 각 기저 상태가 각 레이어에서 1개의 노드만을 방문한다는 조건을 의미한다. 제약식 (17)~(18)은 초기 및 목표 기저 상태를 네트워크상에서 표현하는 제약으로, 제약식 (17)은 첫 레이어에서 출발하는 기저 상태의 위치를 설정한다. 제약식 (18)의 경우 최종 레이어의 노드들은 목표 기저 상태 집합에 포함된 기저 상태의 방문을 받게 된다는 것을 의미한다. 마지막으로 제약식 (19)는 인접한 레이어 간에 아크가 생성될 때, 두 아크가 하나의 공통된 꼬리 노드를 가질 수 없다는 조건을 나타낸다.

6. 실험방법 및 결과

6.1 실험 방법

이진 가역 연산과 그 회로에 대한 명세를 수집한 벤치마크 라이브러리인 REVLIB(Wille *et al*., 2008)를 활용하여 실험을 수행하였다. 큐빗 4개에서 6개 사이즈의 벤치마크 데이터 14개를 선정하여 이를 5.3절에 제시된 수리모형에 적용하였다. <Table 3>은 위의 14개 이진 가역 함수에 대해 제안된 수리모형을 구성했을 때, 모형이 포함하는 실수 및 이진 결정변수의 개수와 제약식의 개수를 각각 제시한다.

구성된 수리모형은 최적화 패키지인 Gurobipy 8.0.1을 활용하여 해결하였으며, 24시간 내에 최적해를 찾지 못하면 탐색된 가장 좋은 가능해(Feasible Solution)를 출력하였다. 최적해 탐색에 상대적으로 긴 시간이 걸린 7-14번 데이터에 대해서는 Gurobipy 8.0.1에서 제공하는 MIP Start 기능을 활용하여 REVLIB(Wille *et al*., 2008)에 제시된 최소 양자비용의 회로를 초기 해로 모형에 제공하였다. 모형 구성 시 필요한 최대 가용 게이트 수인 $|D|$는 선행연구(Maslov *et al*., 2005; Wille *et al*., 2008; Große *et al*., 2009)에서 동일한 데이터에 대해 구성한 가역회로 중 최소 게이트 수로 지정하였다. 본 실험은 Intel(R) CoreTM i7-7700 CPU@3.60GHz 3.60GHz 16.0GB RAM의 실험 환경 하에서 진행되었으며, 소스코드는 python 3으로 작성하였다.

Table 3. Number of Variables(continuous : CON/binary : BIN) and constraints

No	Function Name	Variables		Constraints
		CON	BIN	
1	ex1	4	676	8503
2	ham3	5	827	10621
3	3_17	6	978	12739
4	1bit_adder	4	2648	82603
5	4gt13-v0	3	8227	590995
6	4gt11-v0	3	8227	590995
7	decod24	6	3800	123873
8	4mod5	5	12517	984907
9	graycode6	5	46180	9179200
10	4gt5-v1	4	10372	787951
11	mod5mils	5	11781	984907
12	mod5d1	7	16071	1378819
13	ALU	6	14406	1181863
14	4gt12-v0	5	12517	984907

6.2 REVLIB 벤치마크 데이터 실험 결과

<Table 4>는 5.3절의 수리모형을 기반으로 14개의 이진 가역 함수를 가역 회로로 표현한 실험결과를 대표적인 선행 연구에 발표된 결과와 비교하여 제시하며, 게이트 수(Gate Count)와

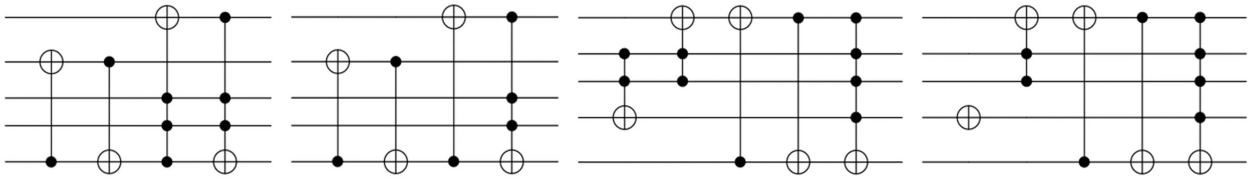
양자 비용 및 계산 시간을 포함한다. 선행 연구는 각각 템플릿 매칭(Maslov *et al*., 2005), QBF(Quantified Boolean Formula) (Wille *et al*., 2008), SAT(Große *et al*., 2009) 기반의 방법론을 채택하였으며, 위 방법론들의 특성 상 양자 비용 최소화를 직접적인 목적함수로 반영하기 어렵기 때문에 게이트 수 최소화를 목적함수로 활용하였다.

14개의 데이터 중 10개의 데이터는 선행 연구의 실험 결과들 중 양자비용 측면에서 가장 좋은 결과와 동일한 수치를 얻었다. 7번과 13번의 2개 데이터에 대해서는 선행 연구에 비해 높은 양자 비용을 갖는 해가 계산되었다. 해당 2개 데이터에 대하여 제한 시간을 48시간으로 늘려 추가 실험을 진행하였으나 양자 비용의 개선이 일어나지 않은 것을 확인하였다. 10번과 14번의 2개 데이터는 선행 연구에 비해 낮은 양자 비용을 갖는 해가 계산되었다. 10번 데이터의 경우 양자 비용 측면에서 42.8%, 14번 데이터의 경우 9.8% 개선된 해가 계산되었다. 해당 2개 데이터에 대해서는 개선된 해가 처음으로 발견된 시간을 <Table 4>에 제시하였다.

<Figure 5>는 10번 데이터와 14번 데이터의 결과를 회로로 제시한다. (a)(Große *et al*., 2009), (b)는 10번 데이터의 회로 변화를, (c)(Große *et al*., 2009), (d)는 14번 데이터의 회로 변화를 표현하고 있다(Wille *et al*., 2008). <Figure 5>를 통해 새로이 구성된 회로에서는 선행연구에서 제시된 회로에 비해 제어 라인의 개수가 감소하였다는 사실을 확인할 수 있다. 주어진 최대 계산 시간인 24시간 내에 최적성이 검증된 해를 얻은 데이터는 총 6개로, 이들 회로는 평균적으로 3.8개의 큐빗으로 구성되어 있다. 반면, 나머지 10개 데이터의 경우 최대 계산 시간인 24시간 내에 얻어진 가장 좋은 해의 최적성이 검증되지 않았으며, 이들 데이터에 대한 결과 회로의 평균 큐빗 개수는 5.0개로 함수를 표현하는 회로의 크기가 커질수록 최적해를 구하기가 어려워진다는 대략적인 경향성을 확인할 수 있다.

Table 4. Computational Results on Benchmark Data

No	Function Name	# of Qubit	Maslov et al., 2005		Wille et al., 2008		Große et al., 2009		Our model-based approach		
			Gate Count **Objective	Quantum Cost	Gate Count **Objective	Quantum Cost	Gate Count **Objective	Quantum Cost	Gate Count	Quantum Cost **Objective (Rate of change, %)	Optimality Gap (%)
			Time (sec)		Time (sec)		Time (sec)		Time(sec) *Time limit reached		★: Optimal solution
1	ex1	3	-	-	-	-	4	8	4	8	★
			-		-		<1		2		
2	ham3	3	-	-	-	-	5	9	5	9	★
			-		-		<1		15		
3	3_17	3	-	-	6	14	6	14	6	14	★
			-		<1		<1		323		
4	1bit_adder	4	-	-	4	12	4	12	4	12	★
			-		<1		3		2475		
5	4gt13-v0	5	-	-	-	-	3	15	3	15	★
			-		-		7		11555		
6	4gt11-v0	5	-	-	-	-	3	7	3	7	★
			-		-		9		76007		
7	decod24	4	-	-	6	14	6	18	6	18 (+28.6)	77.8
			-		1		7		*		
8	4mod5	5	8	24	5	9	5	9	5	9	66.7
			-		40		123		*		
9	graycode6	6	-	-	5	5	5	5	5	5	60.0
			-		145		583		*		
10	4gt5-v1	5	-	-	-	-	4	28	4	16 (-42.8)	81.2
			-		-		51		17550		
11	mod5mils	5	-	-	5	13	5	13	5	13	76.9
			-		32		48		*		
12	mod5d1	5	-	-	7	11	7	11	7	11	72.7
			-		406		2094		*		
13	ALU	5	-	-	6	14	6	22	6	22 (+57.1)	90.9
			-		182		>5000		*		
14	4gt12-v0	5	-	-	-	-	5	41	5	37 (-9.8)	94.6
			-		-		442		55418		



Toffoli circuit of function No.10 suggested in (a) previous study (b) in our study
Toffoli circuit of function No.14 suggested in (c) previous study (d) in our study

Figure 5. Circuit Form Results with Improved Quantum Costs

또한, 최적성이 검증된 6개 데이터에 대해 선행연구의 휴리스틱 알고리즘으로 얻은 해가 양자 비용 측면에서 최적해라는 것을 알 수 있다. 따라서 선행연구의 휴리스틱 알고리즘은 작은 사이즈의 문제에 대해서 최적해를 탐색하는 성능이 상대적으로 높다는 것을 알 수 있다. 최적성이 검증되지 않은 가능해를 얻은 10개 데이터에 대해서는 계산시간 제한 조건을 완화하거나 수리 모형을 개선하여 추후 연구를 진행하였을 때 선행연구 및 이 연구에서 제시된 해보다 개선된 해가 발견될 가능성이 있다.

7. 결 론

이 연구는 진리표 형태로 주어진 가역함수에 대하여 다중 제어 토폴리 게이트로 구성된 최소 양자 비용의 가역 회로로 표현하는 최적화 모형을 제안하였다. 또한, 벤치마크 데이터를 활용한 실험을 통해 제안된 최적화 모형의 효용성을 제시하였다. 14개 벤치마크 데이터에 대한 실험 결과, 대부분의 케이스에서 선행연구와 같은 수준의 양자 비용을 갖거나 기존 수치보다 개선된 양자비용을 갖는 가역 회로를 구성할 수 있었다.

이 연구는 게이트 패턴을 활용한 최적화 모형을 가역회로 합성에 접목한 연구로써, 최적화 모형 기반의 새로운 접근 방식을 제시하여 휴리스틱 알고리즘이나 SAT 문제 등에 기반을 둔 기존의 접근방식과는 차별점을 갖는다. 특히, 이 연구에서 제시한 수리모형은 회로 설계 목적에 따라 제약을 추가하거나 목적함수를 변경하는 등 모형을 변형하여 사용할 수 있는 확장성과 강건성을 가진다. 예를 들어, 양자 비용 이 외의 회로 평가 요소인 상호작용 비용, 미결정 비트의 수, 회로 깊이 등을 목적함수와 제약조건으로 표현하여 회로 설계에 추가적으로 고려하는 등 다양한 활용이 가능하다. 제시된 수리 모형을 통해 계산된 최적 해는 기존에 제시된 휴리스틱 알고리즘에 대한 성능 평가 기준으로 삼을 수 있으며, 양자 알고리즘에서 반복적으로 활용되는 기초 가역 함수들에 대하여 양자 비용 측면에서의 최적 회로를 구성할 때 사용할 수 있다. 모형의 현실 적용을 위해 수리모형 재구성 및 모형 해결에 특화된 휴리스틱 및 최적화 알고리즘 설계 등 계산효율성을 향상하는 추가 연구가 필요하다.

참고문헌

Abubakar, M. Y., Jung, L. T., Zakaria, N., Younes, A., and Abdel-Aty, A. H. (2017), Reversible Circuit Synthesis by Genetic Programming Using Dynamic Gate Libraries, *Quantum Information Processing*, **16**(6), 1-24.

Agrawal, A. and Jha, N. K. (2004), Synthesis of Reversible Logic, *In Proceedings Design, Automation and Test in Europe Conference and Exhibition*, IEEE, **2**, 1384-1385.

Aharonov, D. and Ben-Or, M. (1999), Fault-Tolerant Quantum Computation with Constant Error Rate, *arXiv preprint quant-ph/9906129*.

Barenco *et al*. (1995), Elementary Gates for Quantum Computation, *Physical Review A*, **52**(5), 3457-3467.

Datta, K., Rathi, G., Sengupta, I., and Rahaman, H. (2012), Synthesis of Reversible Circuits Using Heuristic Search Method, *In 2012 25th International Conference on VLSI Design*, IEEE, 328-333.

Figgatt, C., Maslov, D., Landsman, K. A., Linke, N. M., Debnath, S., and Monroe, C. (2017), Complete 3-qubit Grover Search on a Programmable Quantum Computer, *Nature Communications*, **8**(1), 1-9.

Golubitsky, O. and Maslov, D. (2011), A Study of Optimal 4-Bit Reversible Toffoli Circuits and their Synthesis, *IEEE Transactions on Computers*, **61**(9), 1341-1353.

Große, D., Wille, R., Dueck, G. W., and Drechsler, R. (2009), Exact Multiple-Control Toffoli Network Synthesis with SAT Techniques, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, **28**(5), 703-715.

Grover, L. K. (1996), A Fast Quantum Mechanical Algorithm for Database Search, *arXiv preprint quant-ph/9605043*.

Gupta, P., Agrawal, A., and Jha, N. K. (2006), An Algorithm for Synthesis of Reversible Logic Circuits, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, **25**(11), 2317-2330.

Hirata, Y., Nakanishi, M., Yamashita, S., and Nakashima, Y. (2011), An Efficient Conversion of Quantum Circuits to a Linear Nearest Neighbor Architecture, *Quantum Information and Computation*, **11**(1-2), 142-166.

Kielpinski, D., Monroe, C., and Wineland, D. J. (2002), Architecture for a Large-Scale Ion-Trap Quantum Computer, *Nature*, **417**(6890), 709-711.

Maslov, D. and Dueck, G. W. (2003), Improved Quantum Cost for n-bit Toffoli Gates, *Electronics Letters*, **39**(25), 1790-1791.

Maslov, D., Dueck, G. W., and Miller, D. M. (2005), Toffoli Network Synthesis with Templates, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, **24**(6), 807-817.

Maslov, D. and Miller, D. M. (2007a), Comparison of the Cost Metrics through Investigation of the Relation between Optimal NCV and Optimal NCT Three-Qubit Reversible Circuits, *IET Computers and Digital Techniques*, **1**(2), 98-104.

Maslov, D., Dueck, G. W., and Miller, D. M. (2007b), Techniques for the Synthesis of Reversible Toffoli Networks, *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, **12**(4), 42.

Maslov, D., Dueck, G. W., Miller, D. M., and Negrevergne, C. (2008), Quantum Circuit Simplification and Level Compaction, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, **27**(3), 436-444.

Miller, D. M., Maslov, D., and Dueck, G. W. (2003), A Transformation based Algorithm for Reversible Logic Synthesis, *In Proceedings 2003. Design Automation Conference (IEEE Cat. No. 03CH37451)*, IEEE, 318-323.

Monroe, C., Raussendorf, R., Ruthven, A., Brown, K. R., Maunz, P., Duan, L. M., and Kim, J. (2014), Large-scale Modular Quantum-Computer Architecture with Atomic Memory and Photonic Interconnects, *Physical Review A*, **89**(2), 1-15.

Nielsen, M. A. and Chuang, I. (2002), Quantum Computation and Quantum Information, *American Journal of Physics*, **70**(5), 1-58.

Prasad, A. K., Shende, V. V., Markov, I. L., Hayes, J. P., and Patel, K. N. (2006), Data Structures and Algorithms for Simplifying Reversible Circuits, *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, **2**(4), 277-293.

Preskill, J. (2018), Quantum Computing in the NISQ Era and Beyond, *Quantum*, **2**, 1-20.

Saeedi, M. and Markov, I. L. (2013), Synthesis and Optimization of Reversible Circuits-A Survey, *ACM Computing Surveys(CSUR)*, **45**(2), 21.

Saeedi, M., Zamani, M. S., Sedighi, M., and Sasanian, Z. (2010), Reversible Circuit Synthesis Using a Cycle-based Approach, *ACM Journal on Emerging Technologies in Computing Systems(JETC)*, **6**(4), 1-25.

Sasamal, T. N., Singh, A. K., and Mohan, A. (2015), Reversible Logic Circuit Synthesis and Optimization Using Adaptive Genetic Algorithm, *Procedia Computer Science*, **70**, 407-413.

Shende, V. V. and Markov, I. L. (2008), On the CNOT-cost of TOFFOLI Gates, *arXiv preprint arXiv:0803.2316*.

Shor, P. W. (1994), Algorithms for Quantum Computation : Discrete Logarithms and Factoring, *In Proceedings 35th Annual Symposium on Foundations of Computer Science*, IEEE, 124-134.

Szyprowski, M. and Kerntopf, P. (2011), Reducing Quantum Cost in Reversible Toffoli Circuits, *arXiv preprint arXiv:1105.5831*.

Wille, R. and Grobe, D. (2007), Fast Exact Toffoli Network Synthesis of Reversible Logic, *In 2007 IEEE/ACM International Conference on Computer-Aided Design*, IEEE, 60-64.

Wille, R., Le, H. M., Dueck, G. W., and GroBe, D. (2008), Quantified Synthesis of Reversible Logic, *In 2008 Design, Automation and Test in Europe*, IEEE, 1015-1020.

Wille, R. and Drechsler, R. (2009), BDD-based Synthesis of Reversible Logic for Large Functions, *In Proceedings of the 46th Annual Design Automation Conference*, ACM, 270-275.

Wille, R., Saeedi, M., and Drechsler, R. (2010), Synthesis of Reversible Functions Beyond Gate Count and Quantum Cost, *arXiv preprint arXiv:1004.4609*.

Zurek, W. H. (2003), Decoherence, Einselection, and the Quantum Origins of the Classical, *Reviews of Modern Physics*, **75**(3), 715-775.

저자소개

정지혜 : 고려대학교 산업경영공학과에서 2015년 학사, 2017년 석사학위를 취득하고 박사과정에 재학 중이다. 연구분야는 수리계획법, 최적화응용이다.

최인찬 : 고려대학교에서 1982년 산업공학 학사학위를 취득하고, Iowa State University 1984년 산업공학 학사학위를 취득하였다. 1986년 Columbia University에서 경영과학(수리계획) 석사, 1990년 경영과학(수리계획) 박사학위를 취득하였다. 벨통신연구소(Bellcore) Tech Research Staff, 위치타 주립대학교 조교수, 매사추세츠 공과대학교 객원교수를 역임하고 1996년부터 고려대학교 산업경영공학과 교수로 재직하고 있다. 관심 연구분야는 수리계획법, 최적화 현실 응용, 양자컴퓨팅이다.