선형정수계획을 이용한 양자 컴퓨팅 이진 논리 오라클 회로 최적화

저자
(Authors)

정지혜, 최인찬

출처
(Source)

대한산업공학회 추계학술대회 논문집 , 2018.11, 164-182(19 pages)

발행처
(Publisher)

대한산업공학회
Korean Institute Of Industrial Engineers

URL

http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07561445

APA Style

정지혜, 최인찬 (2018). 선형정수계획을 이용한 양자 컴퓨팅 이진 논리 오라클 회로 최적화. 대한산업공학회 추계학술대회 논문집, 164-182

선형정수계획을 이용한 양자 컴퓨팅 이진 논리 오라클 회로 최적화

정지혜[1] · 최인찬[2*]

[1] 고려대학교 산업경영공학과 박사과정생
(cathy0324@korea.ac.kr)

[2*] 고려대학교 산업경영공학과 교수
(ichoi@korea.ac.kr)

목 차

1 연구 배경 연구 동기

양자 컴퓨팅

☑ **연구 분야의 중요성**

고난이도·초대규모의 최적화 문제를
해결하기 위한 **차세대 컴퓨팅 플랫폼**

☑ **최근 해외 연구 동향**

현실의 문제에 적용하기 위한 **기초 연구**가
최근 해외에서 활발히 수행 중

☑ **연구의 현실 적용성**

실제적인 활용을 위해 개발된 양자 알고리즘은
양자 게이트로 이루어진 회로로 구현

선형정수계획을 이용해 양자 알고리즘 구현에 필수적인
이진 논리 오라클 회로에 대한 최적화 연구를 진행

1 연구 배경 관련 선행 연구

Maslov et al. 2007 Techniques for the synthesis of reversible Toffoli networks

- Reed –Muller spectra를 활용한 반복적 형태의 알고리즘 제안
- 만들어진 회로 결과에 대해 비용 개선을 위한 재조정 단계를 포함

Wille et al. 2008 Quantified synthesis of reversible logic

- Quantified Boolean Formula(QBF) satisfiability 형태의 모델 제안
- Binary Decision Diagram을 활용하여 모델의 해를 계산

Grosse et al. 2008 Exact synthesis of elementary quantum gate circuits for reversible functions with don't cares

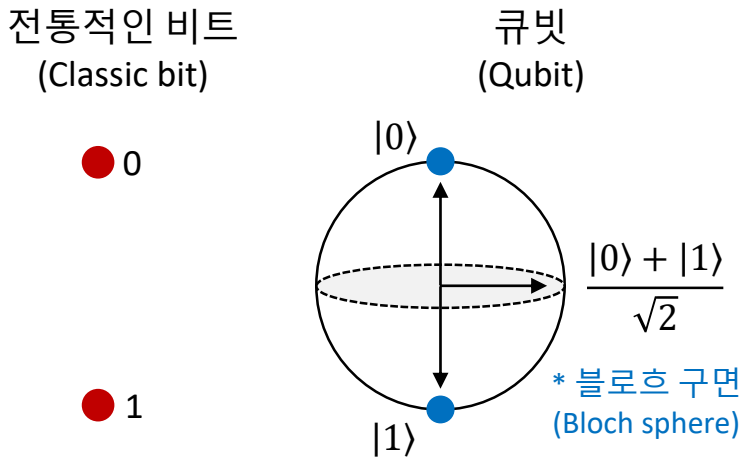
- Boolean satisfiability(SAT)를 활용하여 회로를 디자인하는 알고리즘 제안
- 최소한의 게이트를 사용하여 회로를 디자인

Grosse et al. 2009 Exact Multiple-Control Toffoli Network Synthesis with SAT Techniques

- Boolean satisfiability(SAT)와 SAT modulo theory (SMT)를 활용한 모델 제안
- 더 효율적인 문제 해결을 위해 주어진 문제의 특정적인 정보를 활용

2 이론적 배경 큐빗과 기저 상태

큐빗 (Qubit)



- 전통적인 비트 개념과는 다르게, $|0\rangle$과 $|1\rangle$의 두 상태가 서로 중첩된 형태 가능
- 양자 상태(quantum state)의 표현:
  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\begin{bmatrix}1\\0\end{bmatrix} + \beta\begin{bmatrix}0\\1\end{bmatrix}$
- 각 기저 상태는 단위 벡터로 표현
- 양자 상태는 기저 상태의 선형 결합으로 표현

기저 상태 (Computational Basis States: CBS)

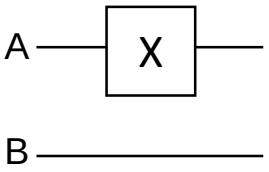
- 여러 개의 큐빗으로 상태 표현 (큐빗 3개)

Q_A	Q_B	Q_C	CBS	벡터 형태 표현
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|000\rangle$	$v_1 = [1,0,0,0,0,0,0,0]$
$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|001\rangle$	$v_2 = [0,1,0,0,0,0,0,0]$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|010\rangle$	$v_3 = [0,0,1,0,0,0,0,0]$
$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|110\rangle$	$v_4 = [0,0,0,1,0,0,0,0]$
$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|100\rangle$	$v_5 = [0,0,0,0,1,0,0,0]$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|101\rangle$	$v_6 = [0,0,0,0,0,1,0,0]$
$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|110\rangle$	$v_7 = [0,0,0,0,0,0,1,0]$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|111\rangle$	$v_8 = [0,0,0,0,0,0,0,1]$

- 기저 상태를 사용한 양자 상태 표현
  $|\psi\rangle = \alpha_1|000\rangle + \alpha_2|001\rangle + \cdots + \alpha_8|111\rangle$
  $= \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_8 v_8 = \sum_{i=1}^{2^3} \alpha_i v_i$

2 이론적 배경 X/CNOT/토폴리 게이트

X 게이트



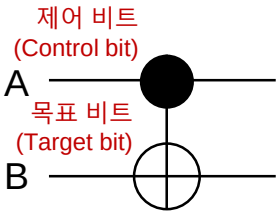
INPUT	OUTPUT
$\|0\rangle_A\|0\rangle_B$	$\|\mathbf{1}\rangle_A\|\mathbf{0}\rangle_B$
$\|0\rangle_A\|1\rangle_B$	$\|\mathbf{1}\rangle_A\|\mathbf{1}\rangle_B$
$\|1\rangle_A\|0\rangle_B$	$\|\mathbf{0}\rangle_A\|\mathbf{0}\rangle_B$
$\|1\rangle_A\|1\rangle_B$	$\|\mathbf{0}\rangle_A\|\mathbf{1}\rangle_B$

Input Output

$$\begin{bmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}=\begin{bmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{bmatrix}$$

- $X \otimes I = \begin{bmatrix}0&1\\1&0\end{bmatrix} \otimes \begin{bmatrix}1&0\\0&1\end{bmatrix}$
- 순열 행렬 (Permutation matrix)

CNOT 게이트



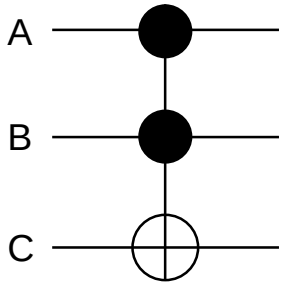
INPUT	OUTPUT
$\|0\rangle_A\|0\rangle_B$	$\|0\rangle_A\|0\rangle_B$
$\|0\rangle_A\|1\rangle_B$	$\|0\rangle_A\|1\rangle_B$
$\|1\rangle_A\|0\rangle_B$	$\|\mathbf{1}\rangle_A\|\mathbf{1}\rangle_B$
$\|1\rangle_A\|1\rangle_B$	$\|\mathbf{1}\rangle_A\|\mathbf{0}\rangle_B$

$$CNOT=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$$

제어 비트에 대응되는 큐빗의 기저 상태가 1일 때, 목표 비트의 상태를 반대 상태로 변환

- $X = \begin{bmatrix}0&1\\1&0\end{bmatrix}$
- 순열 행렬 (Permutation matrix)

토폴리(Toffoli) 게이트 : CNOT 게이트의 확장 형태, 제어 비트가 많을수록 양자 비용 증가



INPUT	OUTPUT
$\|0\rangle_A\|0\rangle_B\|0\rangle_C$	$\|0\rangle_A\|0\rangle_B\|0\rangle_C$
$\|0\rangle_A\|0\rangle_B\|1\rangle_C$	$\|0\rangle_A\|0\rangle_B\|1\rangle_C$
$\|0\rangle_A\|1\rangle_B\|0\rangle_C$	$\|0\rangle_A\|1\rangle_B\|0\rangle_C$
$\|0\rangle_A\|1\rangle_B\|1\rangle_C$	$\|0\rangle_A\|1\rangle_B\|1\rangle_C$

INPUT	OUTPUT
$\|1\rangle_A\|0\rangle_B\|0\rangle_C$	$\|1\rangle_A\|0\rangle_B\|0\rangle_C$
$\|1\rangle_A\|0\rangle_B\|1\rangle_C$	$\|1\rangle_A\|0\rangle_B\|1\rangle_C$
$\|1\rangle_A\|1\rangle_B\|0\rangle_C$	$\|\mathbf{1}\rangle_A\|\mathbf{1}\rangle_B\|\mathbf{1}\rangle_C$
$\|1\rangle_A\|1\rangle_B\|1\rangle_C$	$\|\mathbf{1}\rangle_A\|\mathbf{1}\rangle_B\|\mathbf{0}\rangle_C$

- 본 연구에서는 제어 비트가 여러 개인 **다중 제어 (Multiple control) 토폴리 게이트**만을 사용하여 회로 구성

2 이론적 배경 오라클

- 양자 알고리즘을 구성하는 부분 중 “블랙박스” 형태를 띄는 함수
- 블랙박스가 수행하는 연산은 $f:\{0,1\}^n \rightarrow \{0,1\}^m$ 형태의 전통적인 함수 형태로 표현 가능

오라클 개념의 필요성 #1
함수의 차원을 보정하기 위해

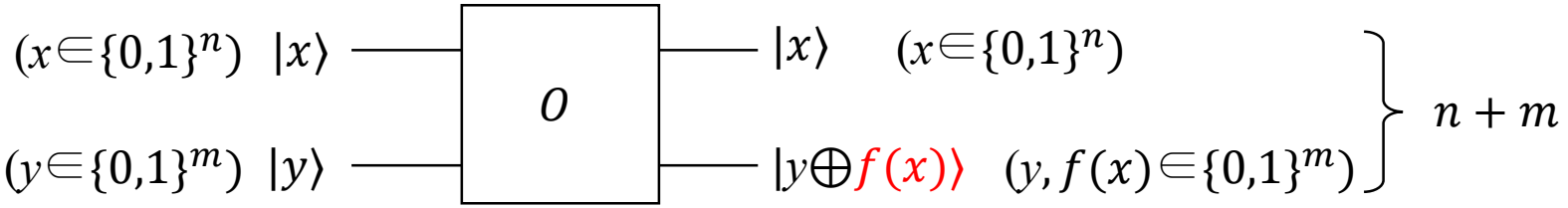
☑ $f:\{0,1\}^n \rightarrow \{0,1\}^m$

오라클 개념의 필요성 #2
역함수가 존재하도록 하기 위해

☑ $f:\{0,1\}^n \rightarrow \{0,1\}^n$

☑ f의 역함수가 존재하지 않음

양자 회로에서 오라클의 역할 : 위의 케이스에 대해 역함수가 존재하도록 구성

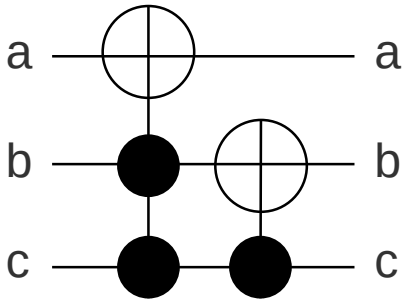


3 문제 설명 회로 관점

진리표

abc	abc	abc	abc
000	000	100	100
001	011	101	111
010	010	110	110
011	101	111	001

회로



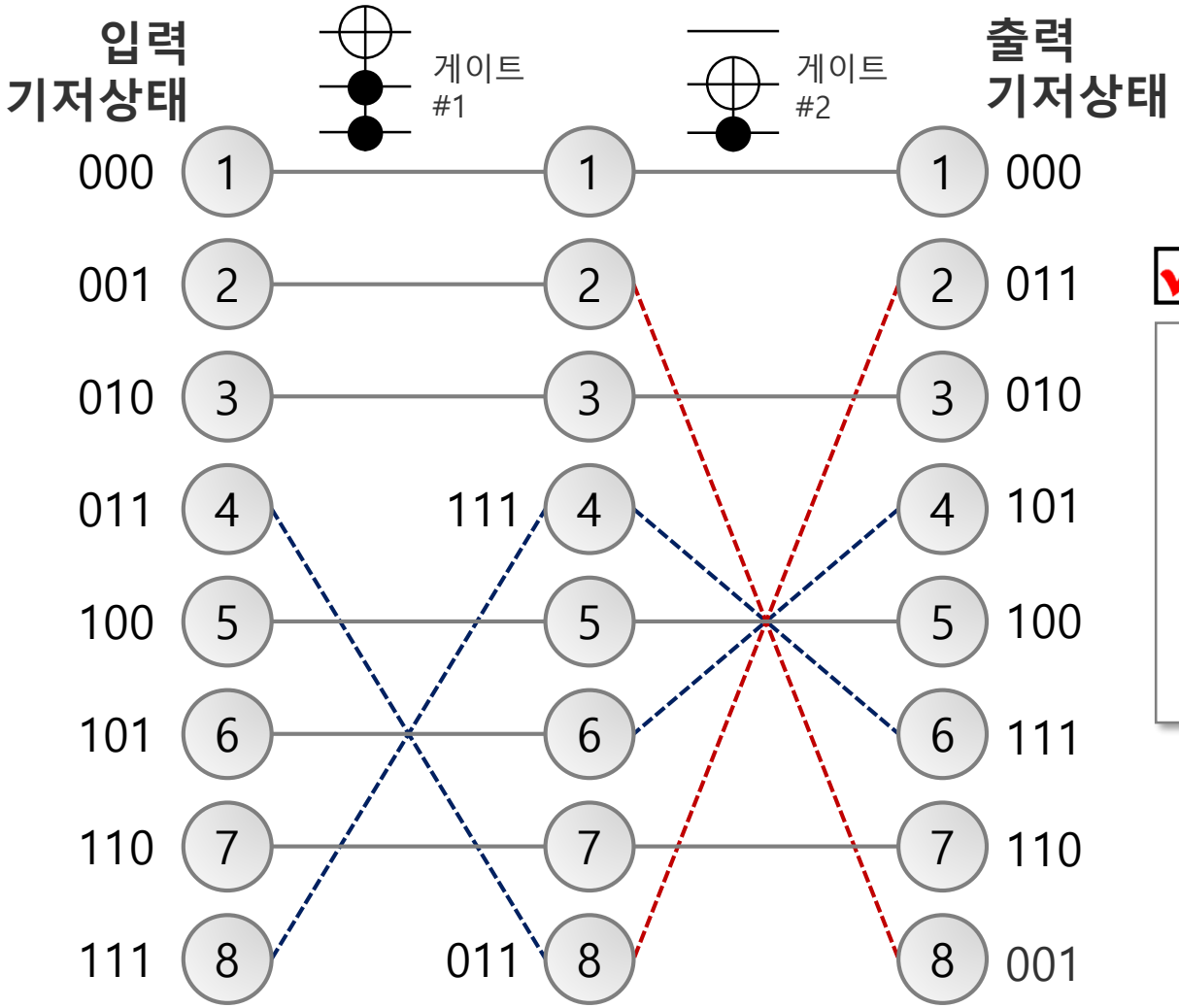
입력 요소
진리표(Truth table) 형태로
표현된 이진 오라클 함수
(Garbage bit 허용)

출력 요소
다중 제어 토폴리 게이트만을
사용하여 구성된
이진 오라클 회로

수리모델의 조건

- 주어진 이진 오라클 함수의 회로를 최소의 양자 비용을 통해 구성
- 다중 제어 토폴리 게이트만을 사용하여 회로 구성
- 결과로 나온 회로는 주어진 함수와 같은 연산을 수행

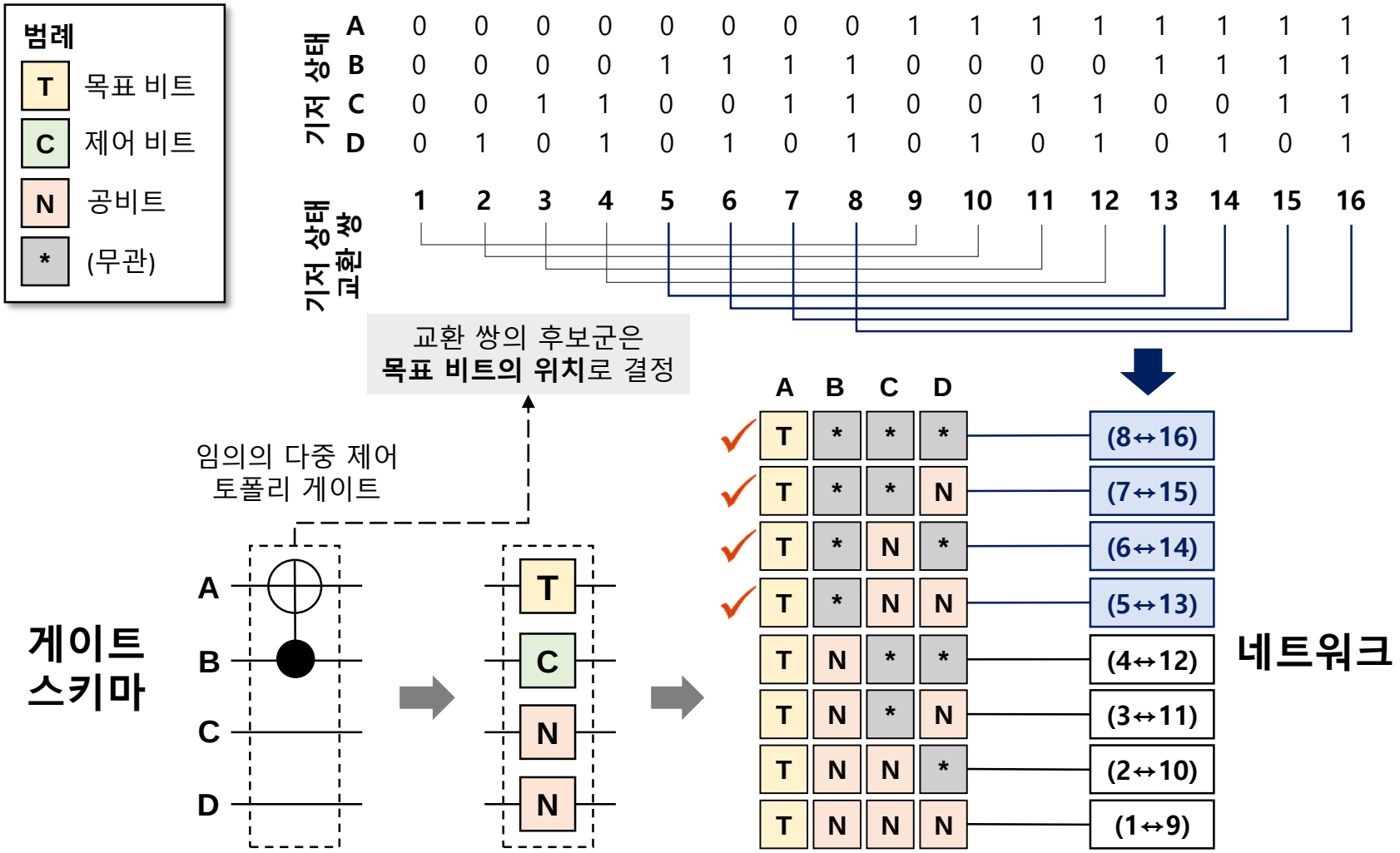
3 문제 설명 네트워크 관점



☑

특정 품종(commodity)의 흐름(flow)이 원하는 노드에 도착하도록 단계별 아크 지정하는 **네트워크 구성 문제**

3 문제 설명 게이트 스키마-네트워크 간의 관계



4 수리 모형 집합과 인덱스

- $\boldsymbol{q} \in \boldsymbol{Q}$ 큐빗의 집합
- $\boldsymbol{d} \in \boldsymbol{D}$ 게이트 레벨(depth)의 집합
- $\boldsymbol{i}, \boldsymbol{j} \in \boldsymbol{M}$ 각 레벨 내 포지션의 집합 (노드 인덱스), $|M| = 2^{|Q|}$
- $\boldsymbol{k} \in \boldsymbol{M}$ 기저 상태의 집합 (품종 인덱스), $|M| = 2^{|Q|}$
- $\boldsymbol{S_q} \in \boldsymbol{P_q}$ 목표 비트가 q번째 큐빗에 존재하는 다중 제어 토폴리 게이트의 게이트 스키마 집합
- $\boldsymbol{S_q}$ 게이트가 포함한 공비트의 큐빗 인덱스로 나타낸 게이트 스키마
- $\boldsymbol{r_{S_q}}$ 게이트 스키마 S_q의 인덱스
- $(\boldsymbol{k_1}, \boldsymbol{k_2}) = \boldsymbol{g}(\boldsymbol{r_{S_q}})$ 게이트 스키마 S_q를 두 기저 상태 k_1, k_2 간의 교환 쌍으로 변환하는 함수
- $\boldsymbol{t} \in \boldsymbol{T_i}$ 마지막 게이트 레벨의 포지션 i에 도착할 수 있는 기저 상태의 인덱스 집합
- $\boldsymbol{QC_q}$ q개 제어 비트를 가진 다중 제어 토폴리 게이트의 양자 비용

4 수리 모형 결정변수

네트워크 결정 모듈

p_{ij}^{d} 경로 변수: 레벨 d의 아크 (i,j)가 서로 이어진 경우 1

f_{ik}^{d} 품종 변수: 기저 상태(품종) k 가 레벨 d의 i번째 노드를 거친 경우 1

회로 결정 모듈

t_{q}^{d} 목표 비트 변수: 레벨 d의 큐빗 q가 목표 비트인 경우 1

e_{q}^{d} 공비트 변수(위치): 레벨 d의 큐빗 q가 공비트인 경우 1

ξ^{d} 레벨 변수: 레벨 d에 게이트가 형성된 경우 1

R_{q}^{d} 공비트 변수(개수): 레벨 d에 q개 큐빗이 공비트인 경우 1

목적함수 모듈

z^{d} 양자 비용 변수: 레벨 d의 양자 비용

회로-게이트 스키마 연결 모듈

$Y_{qr_{S_q}}^{d}$ 스키마 변수: 1 레벨 d의 목표 비트가 q번째 큐빗에 존재하며 스키마 r_{S_q}를 포함하는 경우 1

4 수리 모형 목적함수와 제약조건 (1/2)

목적함수 모듈

(0) $minimize \sum_{d \in D} z^d$

회로 결정 모듈

(1) $t_q^d + e_q^d \leq 1 \quad \forall q \in Q, d \in D$

(2) $\sum_{q \in Q} R_q^d = 1 \quad \forall d \in D$

(3) $\sum_{q \in Q} e_q^d = \sum_{q \in Q} q R_q^d \quad \forall d \in D$

(4) $\xi^d = \sum_{q \in Q \cup \{0\}/\{n_Q\}} R_q^d \quad \forall d \in D$

(5) $\xi^d = \sum_{q \in Q} t_q^d \quad \forall d \in D$

(6) $\xi^{d+1} \leq \xi^d \quad \forall d \in D - \{|D|\}$

회로-게이트 스키마 연결 모듈

(7) $\sum_{i \in M} p_{ii}^d + 2 \sum_{j \in M} \sum_{\mathcal{S}_q \in P_q} Y_{q r_{\mathcal{S}_q}}^d = 2^{|Q|} \quad \forall d \in D, q \in Q$

(8) $\left(t_q^d + \sum_{q \in \mathcal{S}_q} e_q^d\right) \times \frac{1}{N(\mathcal{S}_q)+1} - v \leq Y_{q r_{\mathcal{S}_q}}^d \quad \forall d \in D, q \in Q, \mathcal{S}_q \in P_q$

(9) $\left(t_q^d + \sum_{q \in \mathcal{S}_q} e_q^d\right) \times \frac{1}{N(\mathcal{S}_q)+1} \geq Y_{q r_{\mathcal{S}_q}}^d \quad \forall d \in D, q \in Q, \mathcal{S}_q \in P_q$

(10) $t_q^d \geq Y_{q r_{\mathcal{S}_q}}^d \quad \forall d \in D, q \in Q, \mathcal{S}_q \in P_q$

(11) $f_{i k_1}^{d-1} + f_{j k_2}^{d-1} - 1 \leq p_{ij}^d + (1 - Y_{q r_{\mathcal{S}_q}}^d)$ $\begin{cases} (k_1, k_2) = g\left(r_{\mathcal{S}_q}\right) \\ \forall d \in D, q \in Q, \mathcal{S}_q \in P_q, i, j \in M \end{cases}$

(12) $p_{ij}^d = p_{ji}^d \quad \forall i, j \in M$

4 수리 모형 목적함수와 제약조건 (2/2)

목적함수 모듈

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

네트워크 결정 모듈

(14) $p^d_{ij} + f^{d-1}_{ik} - 1 \leq f^d_{jk}$ $\forall d \in D, i, j, k \in M$

(15) $\sum_{k \in M} f^d_{ik} = 1$ $\forall d \in \{0\} \cup D, i \in M$

(16) $\sum_{i \in M} f^d_{ik} = 1$ $\forall d \in \{0\} \cup D, k \in M$

(17) $f^0_{ik} = 1, i = k, \ \forall i, k \in M$ $\forall i, k \in M$

(18) $\sum_{t \in T_i} f^{|D|}_{it} = 1 \, , \forall i \in M$ $\forall i \in M$

(19) $\sum_{j \in M} p^d_{ij} = 1, \forall d \in D, \ i \in M$ $\forall d \in D, i \in M$

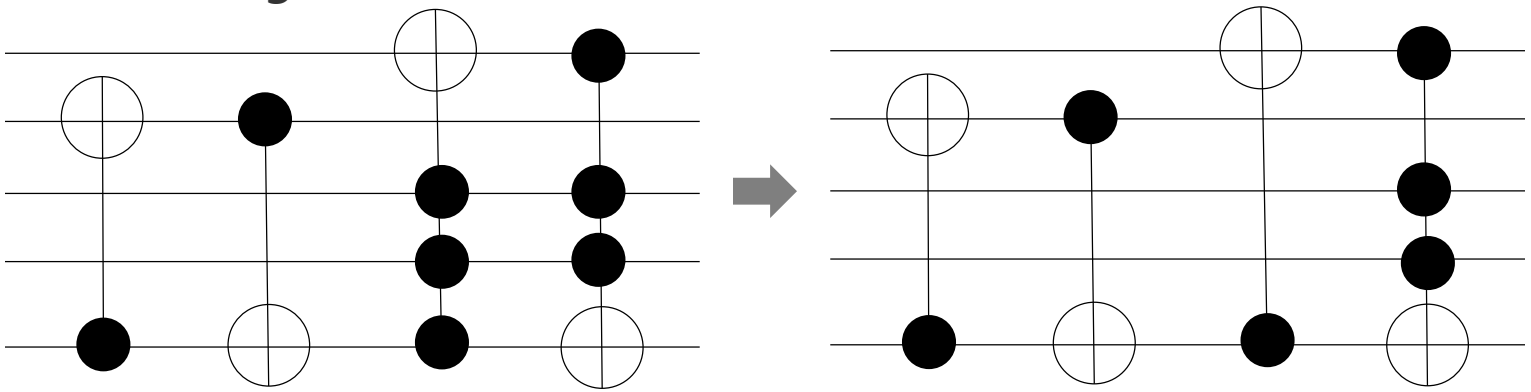
5 실험 결과 결과 테이블 (게이트 수/양자 비용)

번호	함수	큐빗 개수	REVLIB ([9])		SAT ([7])	IP	계산 시간 (초)	최적성 갭 (%)
			결과	문헌	결과	결과		
1	ex1	3	4/8	[1]	4/8	4/8	2.20	0.0*
2	ham3	3	5/9	[10]	5/9	5/9	15.32	0.0*
3	3_17	3	6/14	[3]	6/14	6/14	323.39	0.0*
4	1bit-adder	4	4/12	[3]	4/12	4/12	2475.30	0.0*
5	4gt13-v0	5	3/15	[3]	3/15	3/15	11155.28	0.0*
6	4gt11-v0	5	3/7	[3]	3/7	3/7	76006.96	0.0*
7	decod24	4	6/18	[3]	6/18	6/18	86400.00	77.8
8	4mod5	5	5/9	[3]	5/9	5/9	86400.00	66.7
9	graycode6	6	5/5	[10]	5/5	5/5	86400.00	60.0
10	4gt5-v1	5	4/28	[3]	4/28	**4/16 (42.8%)**	86400.00	81.2
11	mod5mils	5	5/13	[3]	5/13	5/13	86400.00	76.9
12	mod5d1	5	7/11	[3]	7/11	7/11	86400.00	72.7
13	ALU	5	6/14	[4]	6/22	6/22	86400.00	90.9
14	4gt12-v0	5	5/41	[3]	5/41	**5/37 (9.8%)**	86400.00	94.6

* 실험 환경: Intel® Core™ i7-7700 CPU @ 3.60GHz 3.60GHz 16.0GB RAM
** 최적화 패키지: gurobipy 8.0.1

5 실험 결과 회로 형태의 결과 (예시)

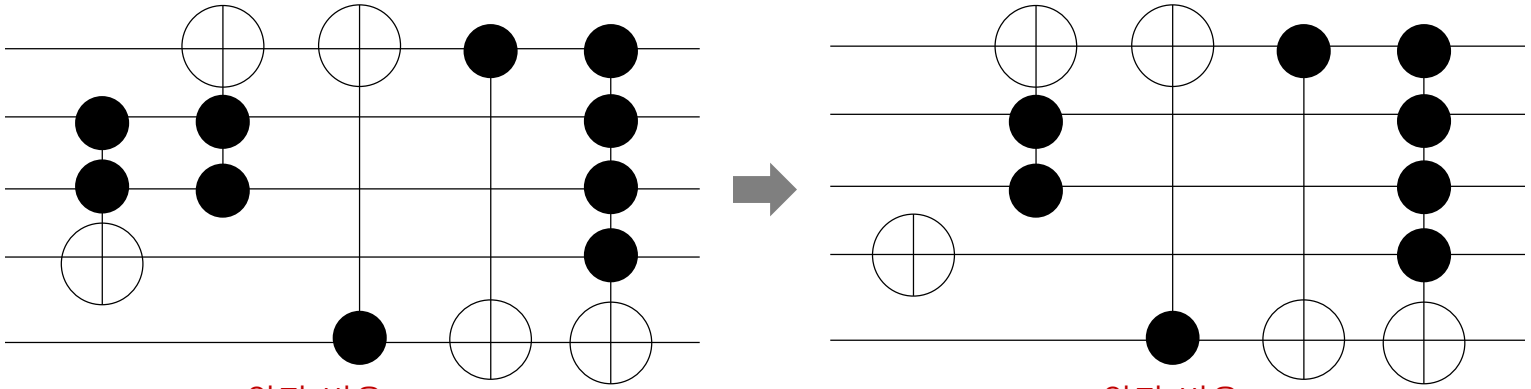
10번 함수 4gt5-v1 양자 비용이 28에서 16으로 감소



양자 비용 28 [3]

양자 비용 16

14번 함수 4gt12-v0 양자 비용이 41에서 37로 감소



양자 비용 41 [3]

양자 비용 37

6 결론

연구의 기대 효과

- 선행 연구들은 양자 비용을 최소화하는 최적화 문제 대신 게이트 수 최소화에 초점을 맞추어 연구를 진행한 반면 본 연구는 양자 비용 최소화에 그 목적을 둠
- 추후 대규모 양자 논리 오라클 회로 구성을 위해 필요한 휴리스틱 알고리즘 개발에 활용
- 위의 목적을 위한 여타 휴리스틱 알고리즘의 성능 평가 기준으로의 활용 가능성

향후 연구 방향

- 본 연구를 통해 제안한 정수계획 모형의 최적해를 효과적으로 탐색하는 최적해 탐색 알고리즘 개발
- 본 연구를 통해 제안한 정수계획 모형을 더 효율적으로 해결할 수 있는 휴리스틱 알고리즘의 개발 및 다양한 메타 휴리스틱 알고리즘 적용

참고 문헌

[1] Maslov et al. 2005 Toffoli network synthesis with templates
[2] Maslov et al. 2007 Techniques for the synthesis of reversible Toffoli networks
[3] Wille et al. 2007 Fast Exact Toffoli Network Synthesis of Reversible Logic
[4] Wille et al. 2008 Quantified synthesis of reversible logic
[5] Grosse et al. 2008 Exact synthesis of elementary quantum gate circuits for reversible functions with don't cares
[6] Wille et al. 2008 Quantified Synthesis of Reversible Logic
[7] Grosse et al. 2009 Exact Multiple-Control Toffoli Network Synthesis with SAT Technique
[8] A. Nielsen et al. 2011 Quantum Computation and Quantum Information
[9] University of Bremen http://www.revlib.org/index.php
(Latest reference: Wille et al. 2013 A Hardware Description Language for the Specification and Synthesis of Reversible Circuits)
[10] Maslov et al. Reversible Logic Synthesis Benchmarks Page. http://webhome.cs.uvic.ca/~dmaslov/

경청해 주셔서 감사합니다

End of document