ゴミラインをもつ量子桁上げ伝播加算器回路の深さに関する最適化

南山大学大学院
理工学研究科　ソフトウェア工学専攻
M2018SE012 柴田　心太郎
指導教員：横山　哲郎

シナリオ

1. 研究背景
2. 研究課題
3. 準備
4. 関連研究・既存方式
5. アプローチ
6. 提案方式
7. 評価
8. 混合方式
9. 結果・今後の課題

1.研究背景(1/3)

量子コンピュータ

量子ゲート（汎用）型

量子回路

・汎用的に利用可能

量子イジング（アニーリング）型

焼きなまし法

・組合せ最適化問題に特化

量子計算： **可逆性**（全域全単射の計算）

量子アルゴリズム

ショアの素因数分解法[1]，グローバーの探索アルゴリズム[2]

量子回路の最適化 → **加算器の最適化**

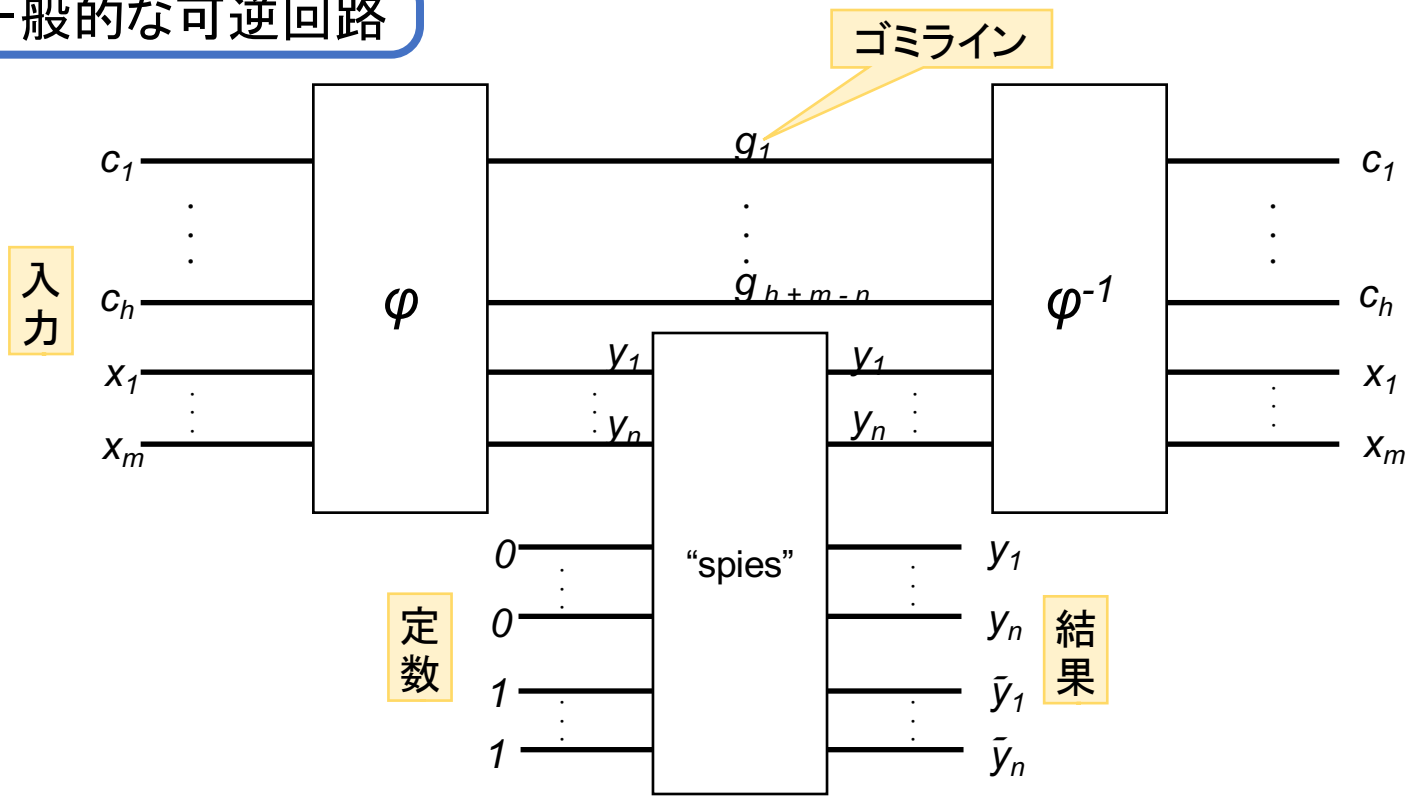
重要

[1]:P.W.Shor, et al.:Algorithms for quantum computation: discrete logarithms and factoring, Proc. 35th Annu. Symp. Foundations of Computer Science, pp. 124-134, 1994.

[2]:L.K.Grover, et al.: A fast quantum mechanical algorithm for database search, in *Proc. 28th ACM Symp. Theory of Computing*, pp. 212–219 , 1996.

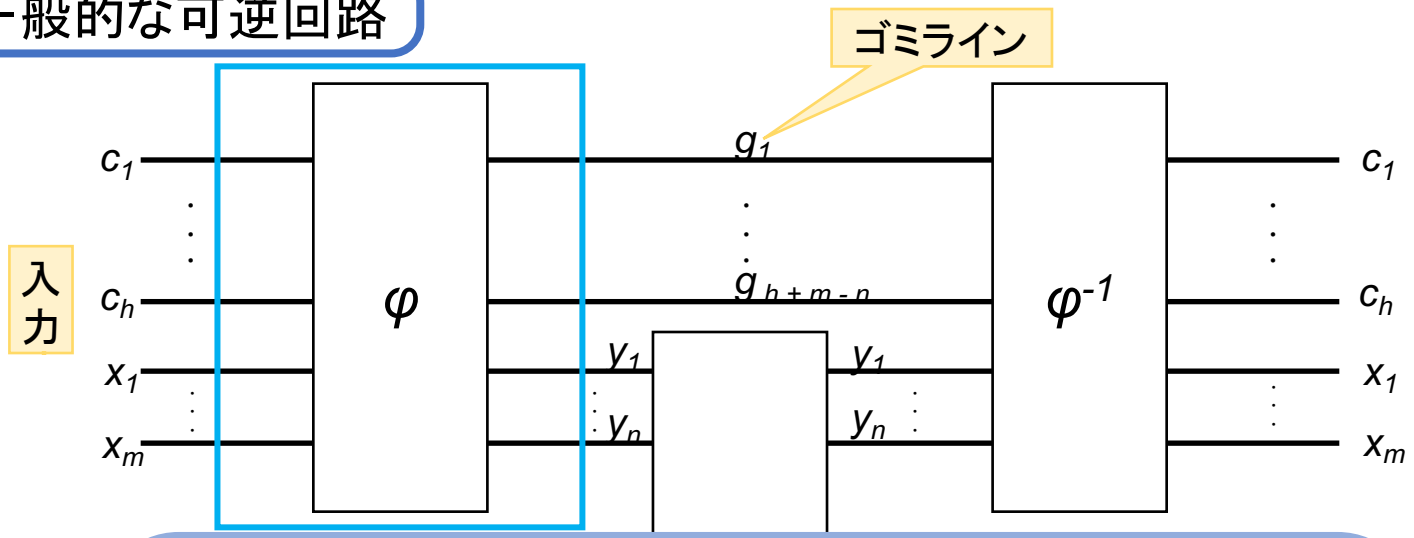
1.研究背景(2/3)

一般的な可逆回路



1.研究背景(3/3)

一般的な可逆回路



加算器の最適化

ラインを犠牲
深さの最適化

回路全体の
計算速度を上げる

2.研究課題

ゴール

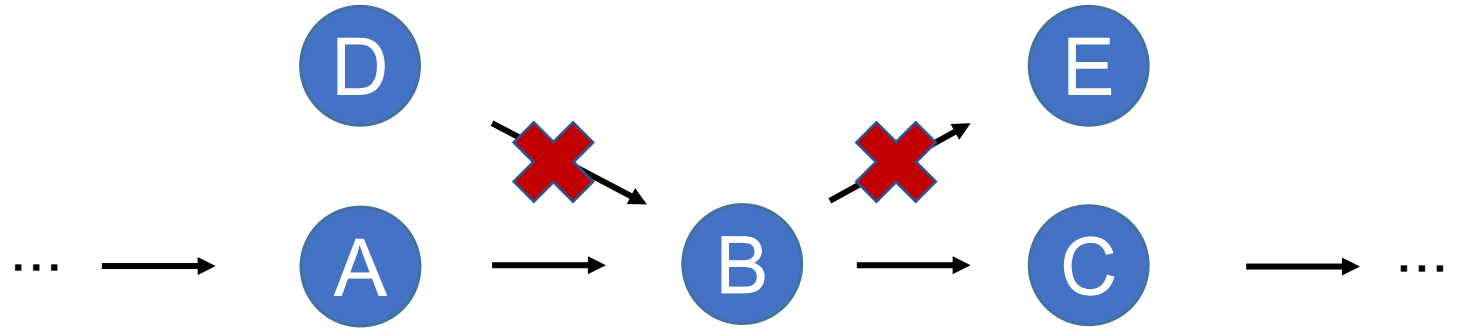
量子回路設計の自動化

研究課題

ゴミラインをもたせて
量子桁上げ伝播加算器の深さを最適化

3.準備(1/4)

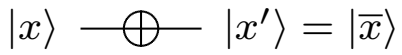
可逆性



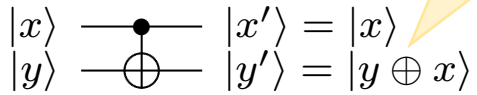
計算過程の任意の状態に対して
直前と直後にとり得る状態が高々1つ

3.準備(2/4)

量子回路



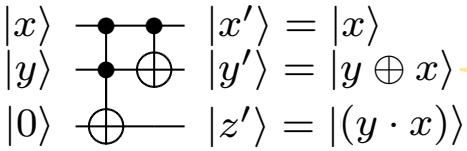
Not ゲート



CN ゲート
（制御付NOTゲート）

排他的論理和

量子ビット		古典ビット
$\|0\rangle = \binom{1}{0}$	$\Longleftrightarrow$	0
$\|1\rangle = \binom{0}{1}$	$\Longleftrightarrow$	1



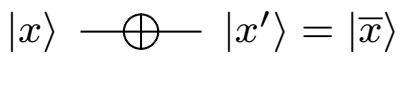
半加算器

和

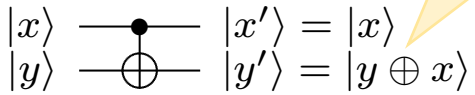
桁上げ情報

3.準備(3/4)

量子回路

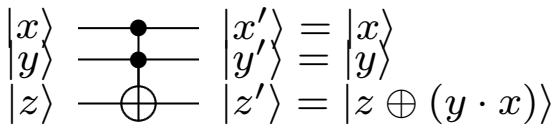


Not ゲート



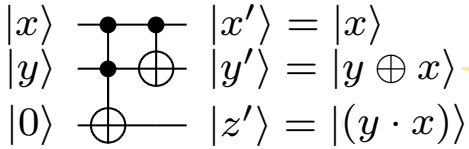
CN ゲート
（制御付NOTゲート）

排他的論理和



CCN ゲート（二重制御付NOTゲート）

x = y = 1 のとき z'= z̄



半加算器

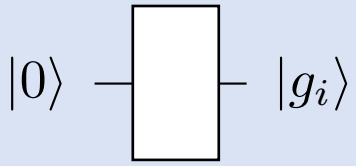
和

桁上げ情報

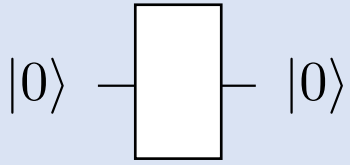
3.準備(4/4)

ライン

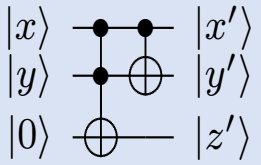
ゴミライン：入力もしくは出力が変数となっているライン



ancillaライン：入出力が定数となっているライン



深さ：各ラインを通る最大のゲート数



深さ＝ 2

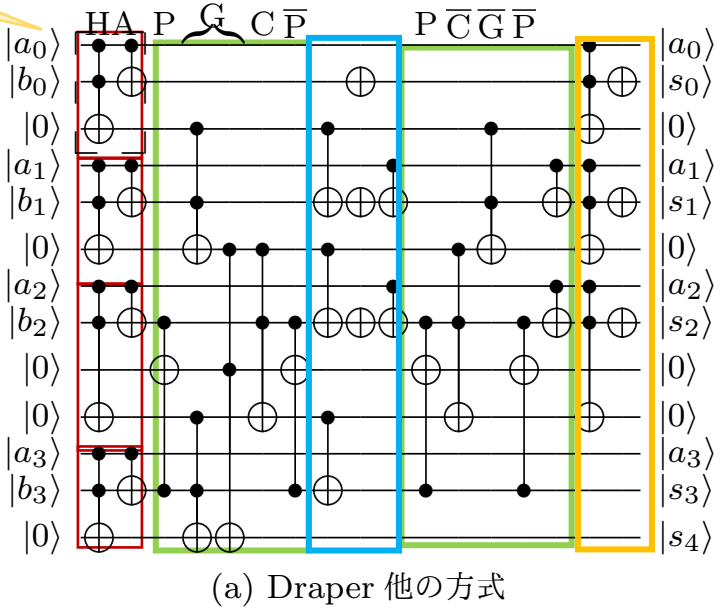
4.関連研究(1/4)

	ゴミライン有り	ゴミライン無し
桁上げ先見加算器 (CLA)		Draper 他, Mogensen
桁上げ伝播加算器 (RCA)	本研究, Rentergem 他	Vedral 他, Takahashi 他

4.関連研究(2/4)

半加算器

入力ビット数が4のとき



(a) Draper 他の方式

Draper他の方式[3]

- 古典的なCLAを応用
- 5段階から構成

伝播と生成をP-round, G-round, C-round で実行

- ancillaラインを使用
- Mogensen[4]はancilla ラインの数を半分にした　Fredkinゲートを追加

[3]:T.G.Draper, et al.: A Logarithmic-Depth Quantum Carry-Lookahead Adder,Quantum Information Computation, Vol.6, No.4¥&5, pp.351–369, 2006.

[4]:T.Æ.Mogensen.: Reversible In-Place Carry-Lookahead Addition with Few Ancillae ,RC 2019, LNCS, Vol.11497, pp.224–237, 2019.

4.関連研究(3/4)

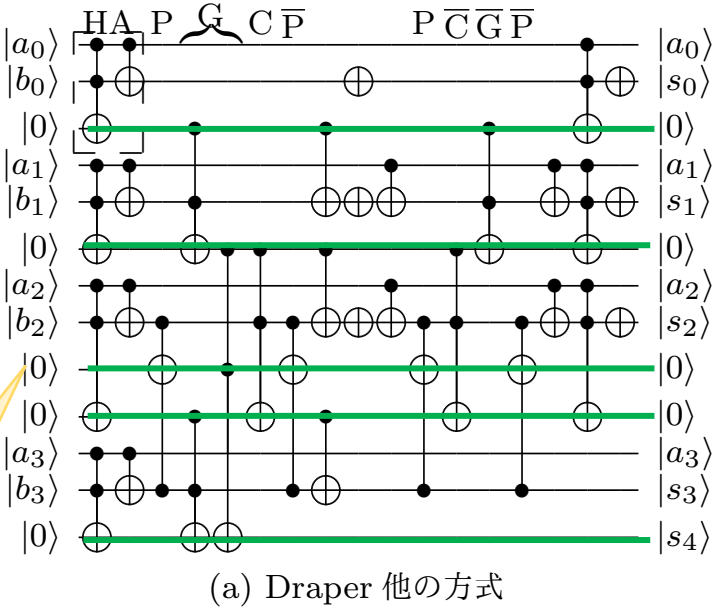
Draper他の方式[3]

- 古典的なCLAを応用
- 5段階から構成

伝播と生成をP-round, G-round, C-round で実行

- ancillaラインを使用
- Mogensen[4]はancilla ラインの数を半分にした　Fredkinゲートを追加

入力ビット数が4のとき



(a) Draper 他の方式

ancillae ライン

[3]:T.G.Draper, et al.: A Logarithmic-Depth Quantum Carry-Lookahead Adder,Quantum Information Computation, Vol.6, No.4¥&5, pp.351–369, 2006.

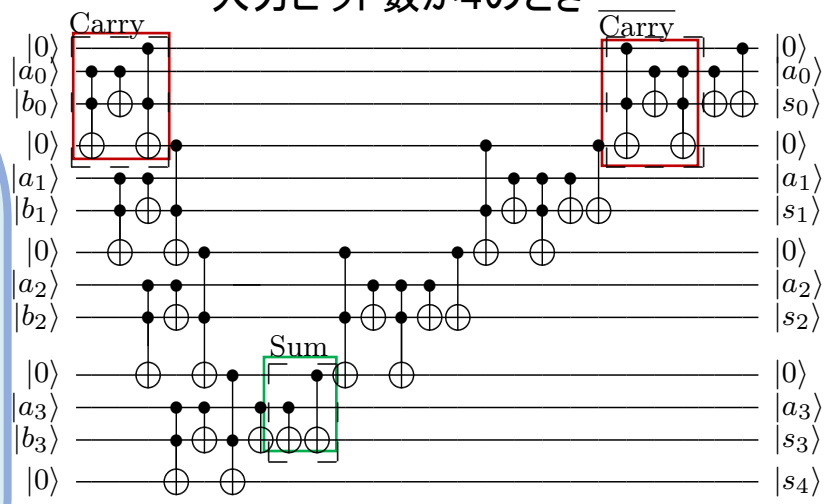
[4]:T.Æ.Mogensen.: Reversible In-Place Carry-Lookahead Addition with Few Ancillae ,RC 2019, LNCS, Vol.11497, pp.224–237, 2019.

4.関連研究(4/4)

Vedral他の方式[5]

- 古典的なRCAを応用
- 3段階から構成
- Carry,Sum
  CarryはCarryの逆計算
- ancillaラインを使用
- Takahashi他は，量子フーリエ変換を用いてancillaラインを消去[6]

入力ビット数が4のとき



(b) Vedral 他の方式

[5]:V.Vendral, et al.: Quantum Networks for Elementary Arithmetic Operations ,Physical Review A, Vol.54, No.1, pp.147-153, 1996.

[6]:Y.Takahashi,et al.: A Liner-size Quantum Circuit for Addition with No Few Ancillary Qubits ,Quantum Information and Computation, Vol.5, No.6, pp.440–448, 2005.

5.アプローチ

埋込み

古典的な桁上げ伝播方式の加算器において
途中で消去されるビットをゴミラインを許すことですべて記憶

6.提案方式(1/2)

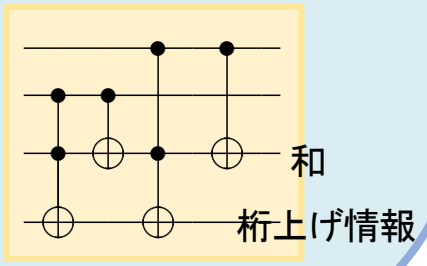
提案方式

- 古典的なRCAを応用
- 2段階から構成
  1. a_0 と b_0 の和 s_0 と桁上げ c_1 を半加算器で得る.
  2. i ≥ 1 のビットに対して，全加算器を置く

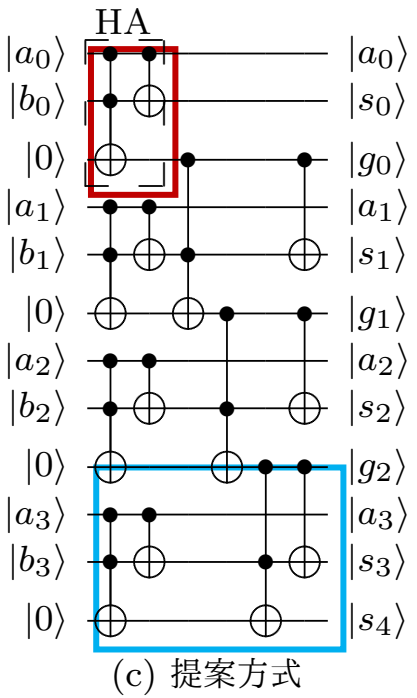
[7]

- ゴミラインを使用
- 逆計算を行わない

⇒ 深さ / ゲート数 } 削減



入力ビット数が4のとき



(c) 提案方式

[7]:Golubitsky, O. and Maslov, D.: A Study of Optimal 4-Bit Reversible Toffoli Circuits and Their Synthesis, IEEE Transactions on Computers, Vol.61, No.9, pp.1341-1353(2012).

6.提案方式(2/2)

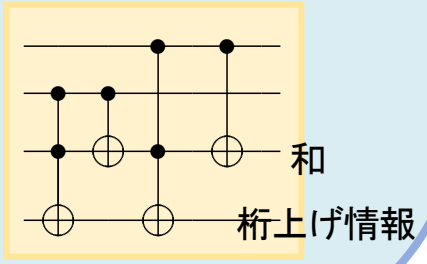
提案方式

- 古典的なRCAを応用
- 2段階から構成
  1. a_0 と b_0 の和 s_0 と桁上げ c_1 を半加算器で得る.
  2. $i \geq 1$ のビットに対して，全加算器を置く

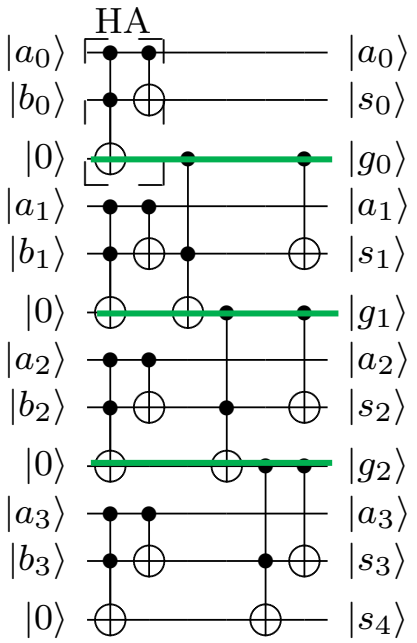
[7]

- ゴミラインを使用
- 逆計算を行わない

⇒ 深さ / ゲート数 } 削減



入力ビット数が4のとき



(c) 提案方式

[7]:Golubitsky, O. and Maslov, D.: A Study of Optimal 4-Bit Reversible Toffoli Circuits and Their Synthesis, IEEE Transactions on Computers, Vol.61, No.9, pp.1341-1353(2012).

7.評価(1/2)

入力ビット数	Draper 他 [3] ($n \geq 7$)				Vedral 他 [5] ($n \geq 3$)				提案方式 ($n \geq 2$)			
	ゲート数	深さ	ancilla ライン	ゴミライン数	ゲート数	深さ	ancilla ライン	ゴミライン数	ゲート数	深さ	ancilla ライン	ゴミライン数
1	2	2	0	0	6	6	1	0	2	2	0	0
2	9	7	1	0	14	13	2	0	6	4	0	1
3	19	11	2	0	22	20	3	0	10	5	0	2
4	34	18	4	0	30	24	4	0	14	6	0	3
n	$10n - o(\log n)$	$O(\log n)$	$2n - o(\log n)$	0	$8n - 2$	$4n + 8$	n	0	$4n - 2$	$n + 2$	0	$n - 1$

入力ビット数:nビットのとき

提案方式

深さ:[5]からnの係数が減少，[3]よりも増加

古典的にも桁上げ先見方式の深さが
桁上げ伝播方式の深さよりも漸近的に優れている

7.評価(2/2)

入力	Draper 他 [3] ($n \geq 7$)				Vedral 他 [5] ($n \geq 3$)				提案方式 ($n \geq 2$)			
ビット数	ゲート数	深さ	ancilla ライン	ゴミライン数	ゲート数	深さ	ancilla ライン	ゴミライン数	ゲート数	深さ	ancilla ライン	ゴミライン数
1	2	2	0	0	6	6	1	0	2	2	0	0
2	9	7	1	0	14	13	2	0	6	4	0	1
3	19	11	2	0	22	20	3	0	10	5	0	2
4	34	18	4	0	30	24	4	0	14	6	0	3
n	$10n - o(\log n)$	$O(\log n)$	$2n - o(\log n)$	0	$8n - 2$	$4n + 8$	n	0	$4n - 2$	$n + 2$	0	$n - 1$

入力ビット数:1～4ビットのとき

提案方式

ゴミライン数以外のすべての指標で既存方式[3][5]以下の値

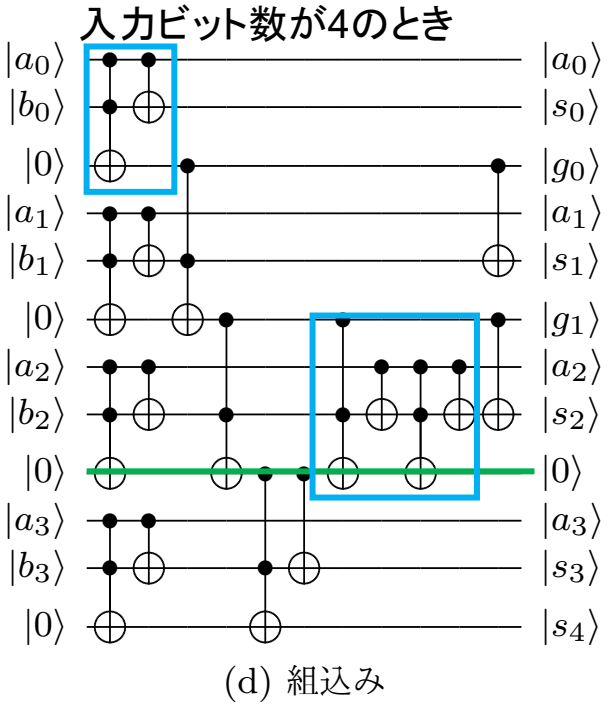
提案方式は既存方式よりも最適化

8. 混合方式(1/3)

Vedral[5]他の方式と提案方式

制約:入力ビット数　4 ビット
　　深さ　　15 以内
　　ゴミライン　　2　本まで許可

	混合方式	Vedral[5]他の方式	提案方式
深さ	11	24	6
ゴミライン	2	0	3

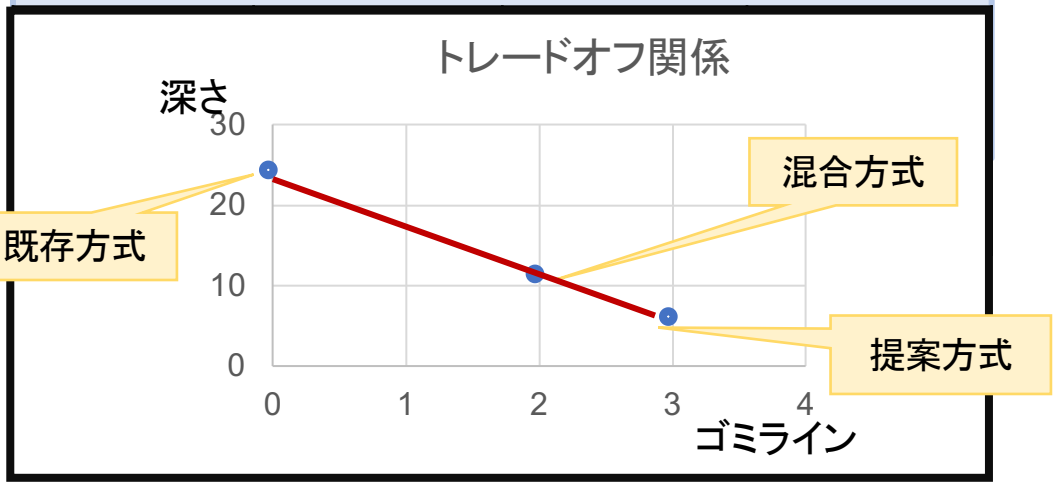


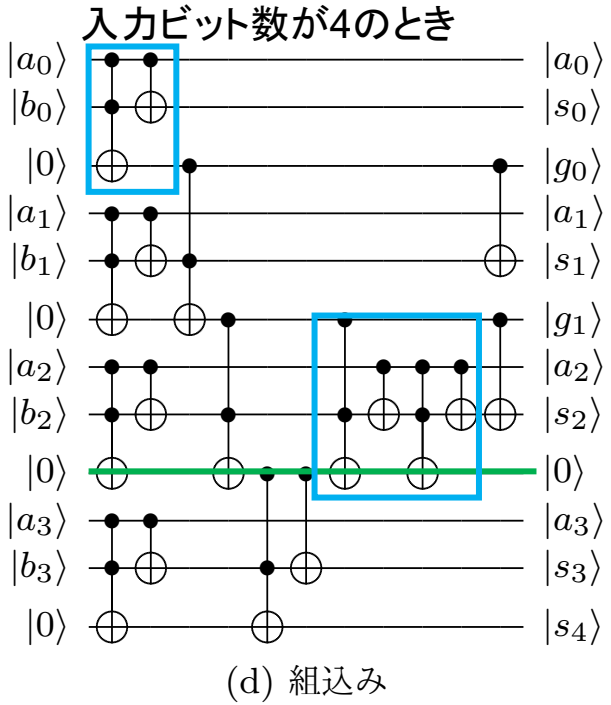
(d) 組込み

8. 混合方式(2/3)

Vedral[5]他の方式と提案方式

制約:入力ビット数　4 ビット
　　深さ　　15 以内
　　ゴミライン　　2　本まで許可





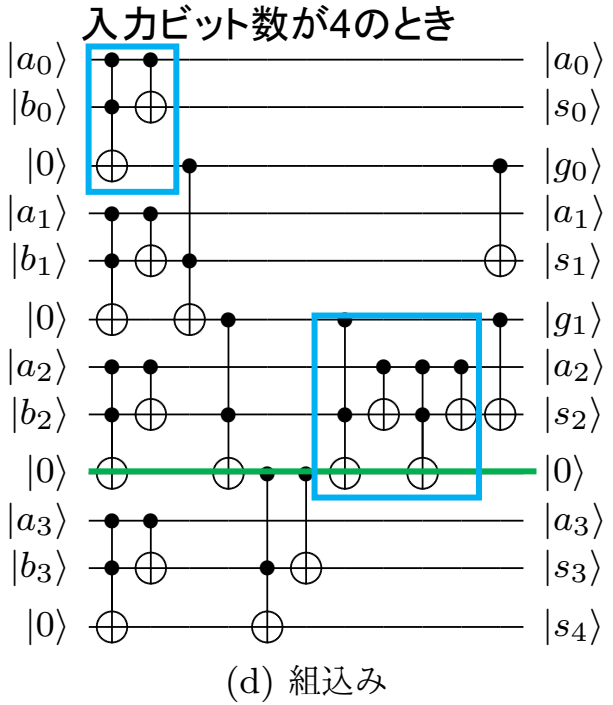
(d) 組込み

8. 混合方式(3/3)

Vedral[5]他の方式と提案方式

制約:入力ビット数　4 ビット
　　深さ　　15 以内
　　ゴミライン　　2　本まで許可

	混合方式	Vedral[5]他の方式	提案方式
深さ	11	24	6
ゴミライン	2	0	3



(d) 組込み

深さにおいて最適化

ある制約のもとでは既存方式を単体で用いるより，最適化された回路を構成可能

9.結果/今後の課題

結果

既存方式・提案方式のコスト解析

- 対象：ゲート，深さ，ancillaライン，ゴミライン
  ビット数　≦ 4 → 全列挙
  　　> 4 → 漸近的解析

提案方式

- 深さが最適
- 既存方式とのトレードオフ関係
  ゴミライン vs 深さ
- 資源量の制約に応じた最適化が可能に

今後の課題

- 入力ビット数の小さい場合のコストをさらに解析
- 最適な回路を得る一般的方法の解明
- 量子コストなど他の指標での比較

まとめ

研究課題

- 量子桁上げ伝播加算器の深さを最適化

アプローチ

- 埋込み

結果・今後の課題

- 既存方式とトレードオフ関係にある提案方式は，制約によって既存方式よりも最適化できる
- 入力ビット数の小さい場合のコストをさらに解析
- 効率的な回路を得る一般的方法の解明