

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
- ・可逆性(全域, 単射の計算)

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



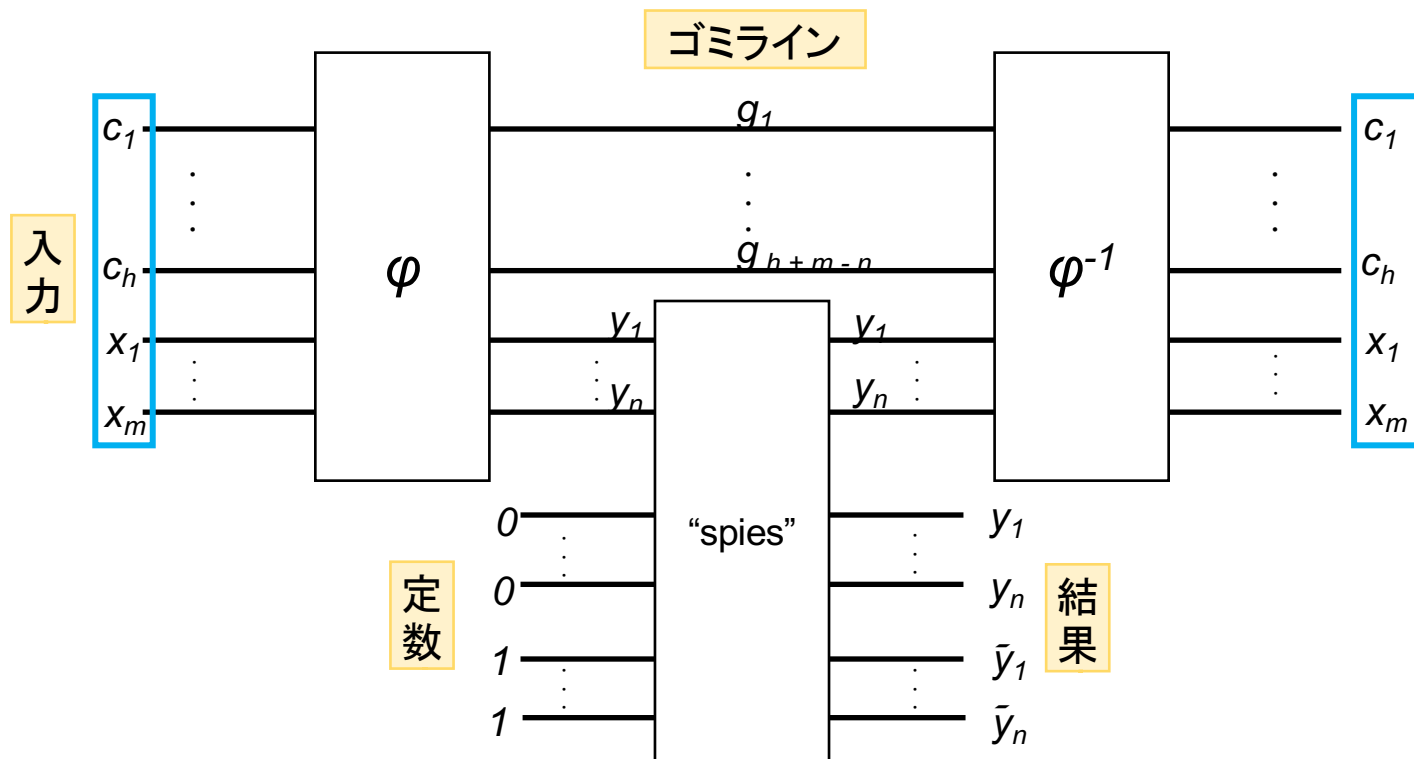
加算器の最適化

重要

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

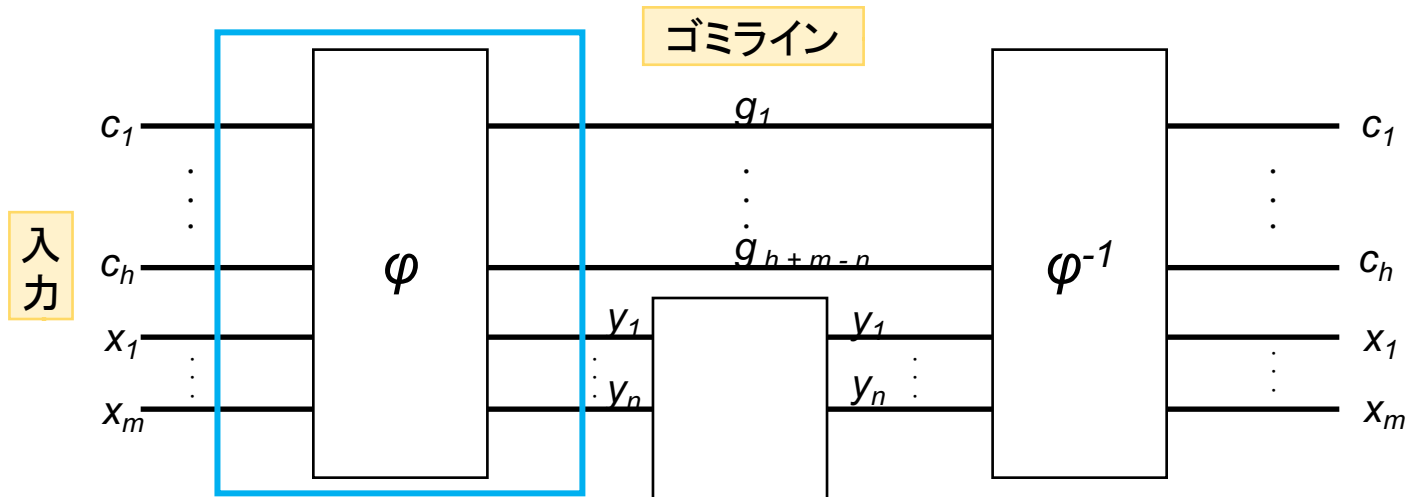
[2]:Grover, L.K. et al.: A fast quantum mechanical algorithm for database search, in Proc. 28th ACM Symp. Theory of Computing, pp. 212-219 (1996).

回路の可逆化



[8]:Fredkin, E. and Toffoli, T.: Conservative logic, (Int. J. Theor. Phys.), Vol.21, No.3&4, pp.219--253 (1982).

回路の可逆化



加算器の最適化
 ラインを犠牲(増加)
 深さの最適化 \longrightarrow 回路全体の計算速度を**向上**

2.研究課題

ゴール

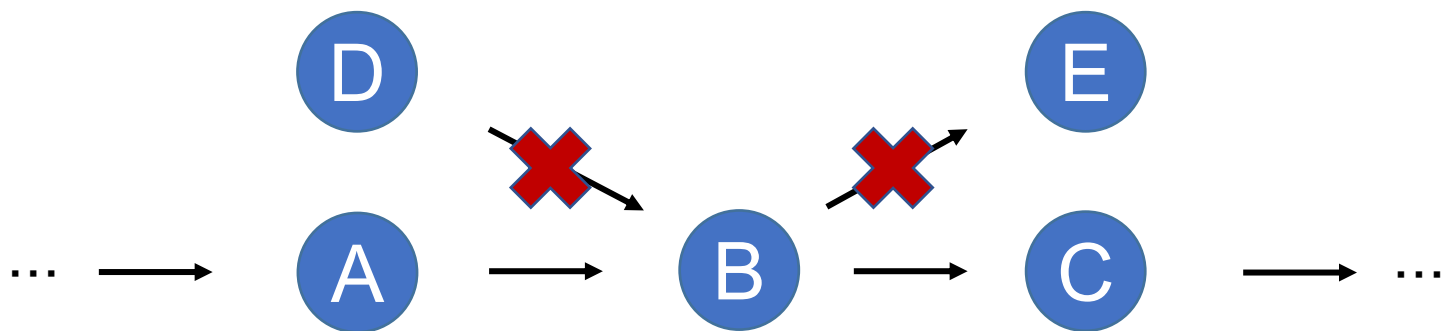
量子回路設計の**自動化**

研究課題

ゴミラインを許した
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

量子回路

$$|x\rangle \xrightarrow{\oplus} |x'\rangle = |\bar{x}\rangle$$

Not ゲート

量子ビット		古典ビット
$ 0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$	\leftrightarrow	0
$ 1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$	\leftrightarrow	1

排他的論理和

$$\begin{array}{l} |x\rangle \\ |y\rangle \end{array} \xrightarrow{\oplus} \begin{array}{l} |x'\rangle = |x\rangle \\ |y'\rangle = |y \oplus x\rangle \end{array}$$

CN ゲート
(制御付NOTゲート)

$$\begin{array}{l} |x\rangle \\ |y\rangle \\ |0\rangle \end{array} \xrightarrow{\oplus} \begin{array}{l} |x'\rangle = |x\rangle \\ |y'\rangle = |y \oplus x\rangle \\ |z'\rangle = |(y \cdot x)\rangle \end{array}$$

半加算器

入力ビットの和

桁上げ情報

量子回路

$$|x\rangle \text{---} \oplus \text{---} |x'\rangle = |\bar{x}\rangle$$

Not ゲート

$$\begin{array}{l} |x\rangle \text{---} \bullet \text{---} |x'\rangle = |x\rangle \\ |y\rangle \text{---} \oplus \text{---} |y'\rangle = |y \oplus x\rangle \end{array}$$

CN ゲート

(制御付NOTゲート)

排他的論理和

$$\begin{array}{l} |x\rangle \text{---} \bullet \text{---} |x'\rangle = |x\rangle \\ |y\rangle \text{---} \bullet \text{---} |y'\rangle = |y\rangle \\ |z\rangle \text{---} \oplus \text{---} |z'\rangle = |z \oplus (y \cdot x)\rangle \end{array}$$

CCN ゲート (二重制御付NOTゲート)

 $x = y = 1$ のとき $z' = \bar{z}$

$$\begin{array}{l} |x\rangle \text{---} \bullet \text{---} |x'\rangle = |x\rangle \\ |y\rangle \text{---} \bullet \text{---} \oplus \text{---} |y'\rangle = |y \oplus x\rangle \\ |0\rangle \text{---} \oplus \text{---} |z'\rangle = |(y \cdot x)\rangle \end{array}$$

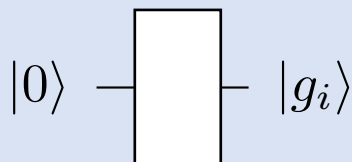
半加算器

入力ビットの和

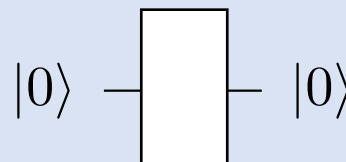
桁上げ情報

回路のコスト

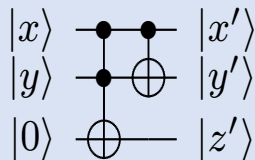
ゴミライン: 入力もしくは出力が変数



ancillaライン: 入出力が定数



深さ: 各ラインが通るゲート数の最大



深さ = 2

4. 関連研究(1/4)

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

4.関連研究(2/4)

Draper他の方式[3]

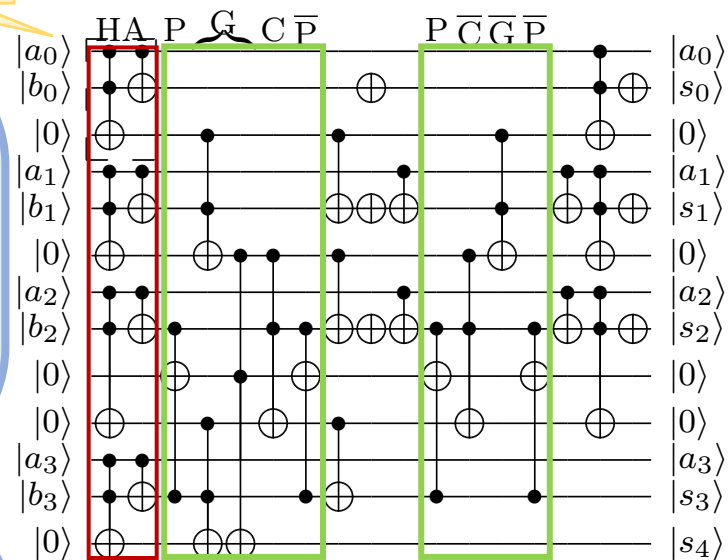
- 古典的な**CLA**を応用
- 5段階から構成
伝播と生成をP-round, G-round, C-round で実行
- ancillaラインを使用

上記方式の拡張

Mogensen[4]はancilla ラインの数を半分
Fredkinゲートを追加

半加算器

入力ビット数が4のとき



(a) Draper 他の方式

[3]: Draper, T.G., Kutin, S.A., Rains, E.M., et al.: A Logarithmic-Depth Quantum Carry-Lookahead Adder, Quantum Information and Computation, Vol.6, No.4&5, pp.351-369 (2006).

[4]: Mogensen T.Æ.: 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]

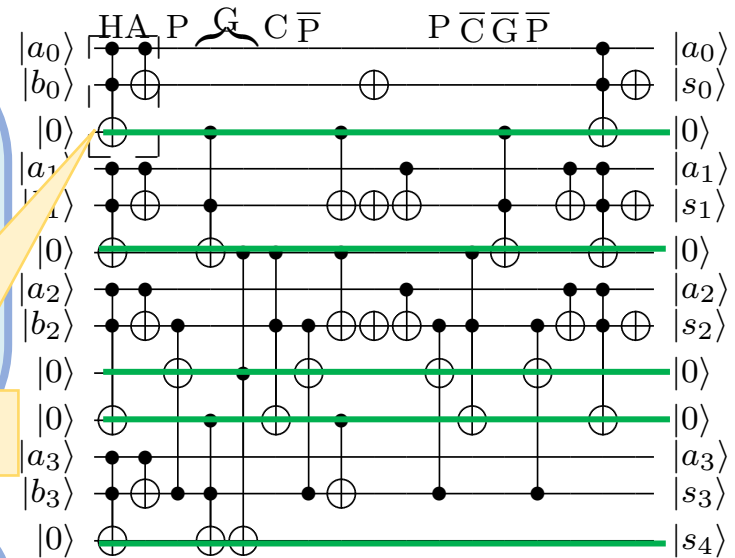
- 古典的な**CLA**を応用
- 5段階から構成
伝播と生成をP-round, G-round, C-round で実行
- ancillaラインを使用

ancilla ライン

上記方式の拡張

Mogensen[4]はancilla ラインの数を半分
Fredkinゲートを追加

入力ビット数が4のとき



(a) Draper 他の方式

[3]:Draper, T.G., Kutin, S.A., Rains, E.M., et al.: A Logarithmic-Depth Quantum Carry-Lookahead Adder, Quantum Information and Computation, Vol.6, No.4&5, pp.351--369 (2006).

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

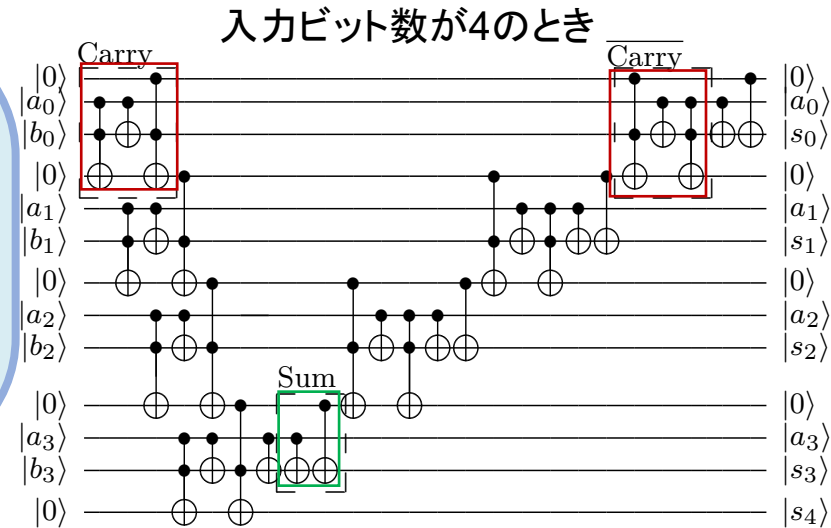
4.関連研究(4/4)

Vedral他の方式[5]

- 古典的なRCAを応用
- 3段階から構成
Carry, Sum, Carry で実行
- ancillaラインを使用 CarryはCarryの逆計算

上記方式の拡張

Takahashi他は, 量子フーリエ変換を用いて ancillaラインを消去[6]



[5]:Vedral, V., Barenco, A. and Ekert, A.: Quantum networks for elementary arithmetic operations, Phys. Rev. A, Vol.54, No.1, pp.147--153 (1996).

[6]:Takahashi, Y. and Kunihiro, N.: A linear-size quantum circuit for addition with no ancillary qubits, Quantum Information and Computation, Vol.5, No.6, pp.440--448 (2005). 14

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

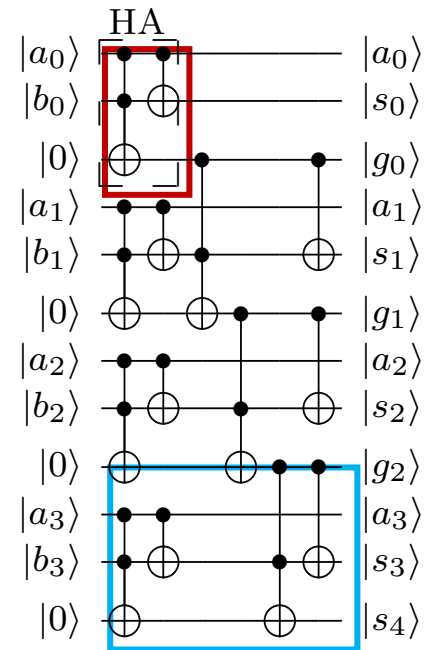
1. a_0 と b_0 の和 s_0 と桁上げ c_1 を半加算器で得る。
2. $i \geq 1$ のビットに対して, 全加算器を置く

[7]

- ゴミラインを使用
- 逆計算を行わない



入力ビット数が4のとき



(c) 提案方式

6.提案方式(2/2)

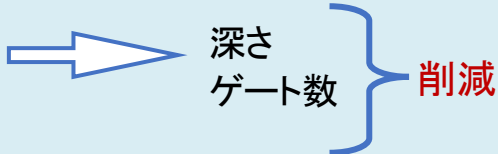
提案方式

- 古典的なRCAを応用
- 2段階から構成

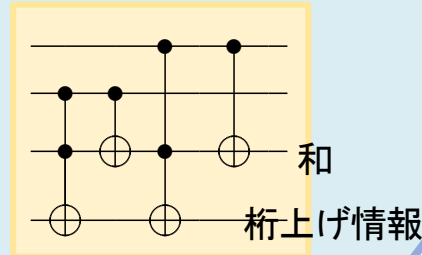
1. a_0 と b_0 の和 s_0 と桁上げ c_1 を半加算器で得る。
2. $i \geq 1$ のビットに対して, 全加算器を置く

[7]

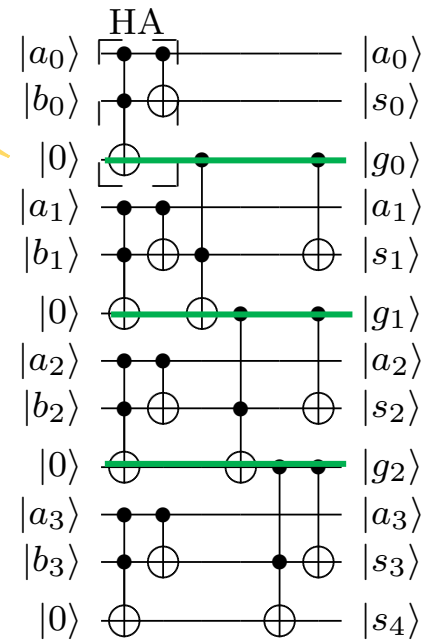
- ゴミラインを使用
- 逆計算を行わない



ゴミライン



入力ビット数が4のとき



(c) 提案方式

7.評価(1/2)

入力 ビット数	QCLA		QRCA			
	Draper 他 [3] ($n \geq 7$)		Vedral 他 [5] ($n \geq 3$)		提案方式 ($n \geq 2$)	
	深さ	ゴミライン数	深さ	ゴミライン数	深さ	ゴミライン数
1	2	0	6	0	2	0
2	7	0	13	0	4	1
3	11	0	20	0	5	2
4	18	0	24	0	6	3
n	$O(\log n)$	0	$4n + 8$	0	$n + 2$	$n - 1$

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**

減少

7.評価(2/2)

入力 ビット数	QCLA		QRCA			
	Draper 他 [3] ($n \geq 7$)		Vedral 他 [5] ($n \geq 3$)		提案方式 ($n \geq 2$)	
	深さ	ゴミライン数	深さ	ゴミライン数	深さ	ゴミライン数
1	2	0	6	0	2	0
2	7	0	13	0	4	1
3	11	0	20	0	5	2
4	18	0	24	0	6	3
n	$O(\log n)$	0	$4n + 8$	0	$n + 2$	$n - 1$

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

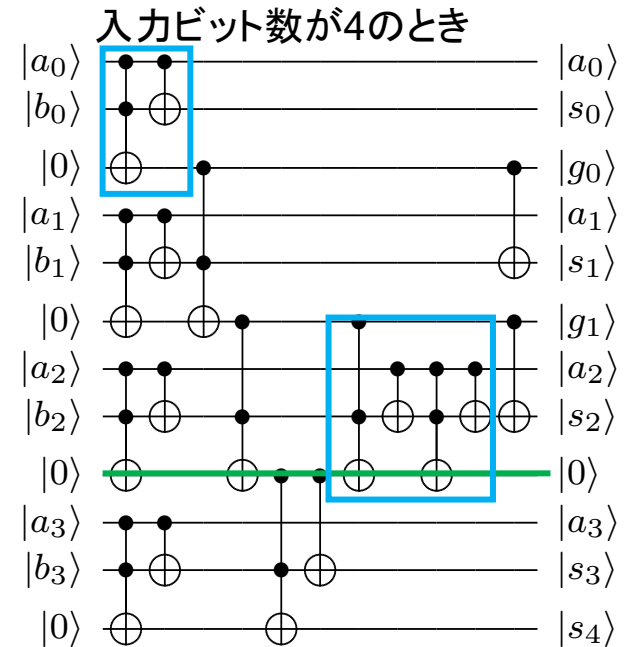
提案方式は既存方式
よりも**最適化**

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
 ゴミライン数 2まで許可

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

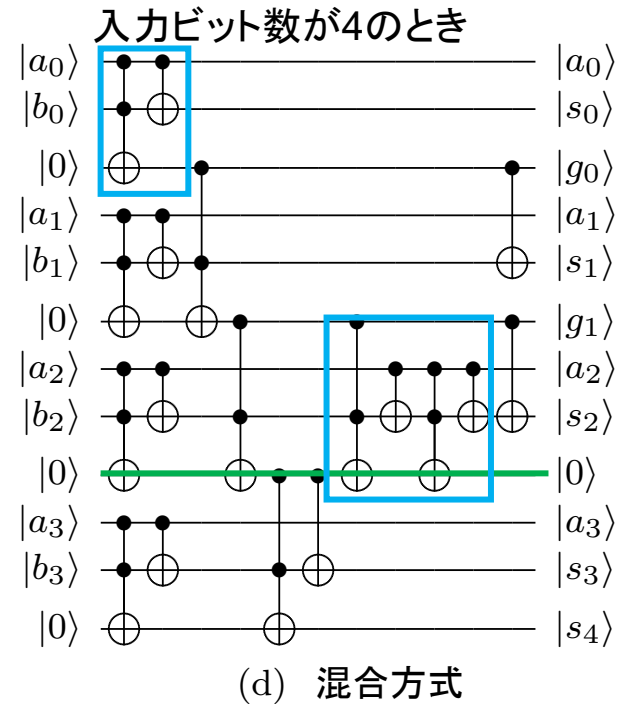
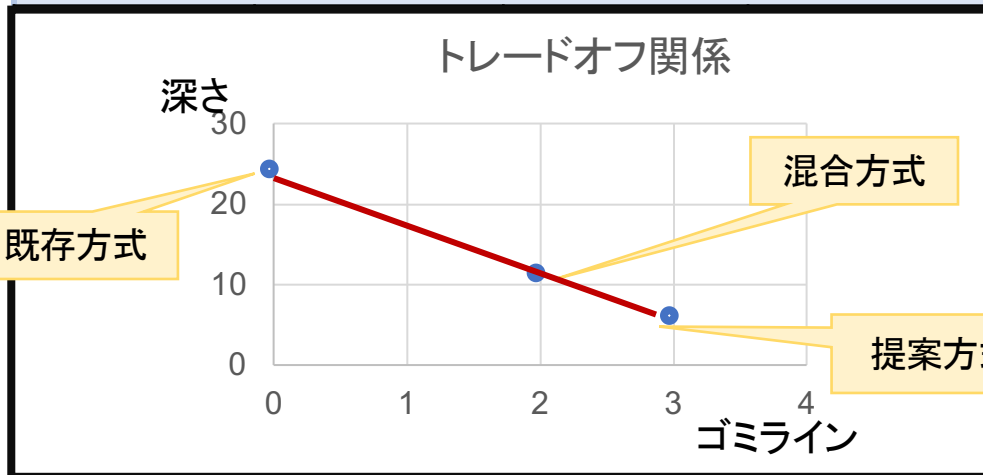


(d) 混合方式

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
 ゴミライン数 2まで許可



8. 混合方式(3/3)

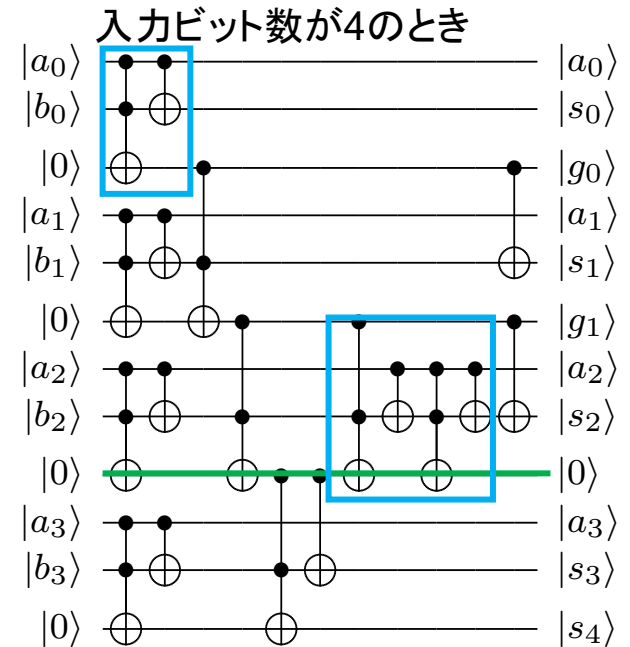
Vedral[5]他の方式と提案方式

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
ゴミライン数	2	0	3

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



(d) 混合方式

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: 深さ, ゴミライン, ゲート数, ancillaライン数
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

- 既存方式及び、提案方式のコスト解析
- 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
- 最適な回路を得る一般的方法の解明