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

M2018SE012 柴田心太郎
指導教員：横山哲郎

1 はじめに

近年，量子計算機の分野の研究は活発である．この量子計算機とは，古典計算機に量子力学を応用した計算機であり，高性能な計算が可能となっている．有名な量子アルゴリズムとして Shor の素因数分解法や Grover のデータベース探索が知られている．これらの量子アルゴリズムは抽象度が高いため量子回路で記述する必要がある．したがって，最適な量子回路の実現は重要な課題であり，演算回路の基本となる加算器回路を最適に設計することも重要である．また，量子回路では全域，かつ単射な計算のみを扱うため，可逆性をもつ．

回路の深さは計算速度に影響し，現在，量子加算器回路にはゴミラインがなく深さが $\mathrm{O}(\log n)$ の量子桁上げ先見方式（QCLA）[1] や $\mathrm{O}(n)$ の量子桁上げ伝播方式（QRCA）[8]，ゴミラインがある深さ $\mathrm{O}(n)$ の QRCA[7] が知られている．これらの回路は深さや量子コスト（QC）などの指標に関してトレードオフ関係にある．しかし，我々の知る範囲において，深さや QC などの制約に応じて最適な回路を得る一般的方法，及び量子回路設計の自動化は明らかにされていない．したがって，これらを明らかにする上で，様々な指標に関するトレードオフ関係を見つける必要がある．

本研究では，不要なビットをゴミラインが全て記憶する“埋込み”を用いた in-place な QRCA の設計方法，及び上記の提案方式にゴミ浄化法を適用し，ゴミラインの無い QRCA の設計を提案する．そして既存方式 [1, 8] に対して，入力ビット数が小さいときに QC・深さがより最適なことを示し，さらに一般の場合に QC がより最適であることを示す．本研究における“最適化”とは，提案方式と既存方式とを比較した際，提案方式の方が既存方式より，指標の値が下回った場合のことを指す．また，提案方式に既存方式を一部組み込むことで，最適化された回路を設計できることを示す．提案方式は既存方式とトレードオフ関係にある新方式であり，本稿のアイデアは他の算術・論理演算の量子回路への応用が期待される．

2 準備

本章では，量子演算，及び本稿で扱う量子ゲートと量子回路の性能を表す指標について説明をする．

2.1 量子演算

量子計算機における演算とは，量子ビットの状態を，目的とする状態へと遷移させる過程であり，量子演算を実行する量子ゲートを組み合わせたものが量子回路である．

量子ビットとは，古典計算機で用いられる古典ビットとは違い，量子計算機で用いることができるビットのことである．1 量子ビットの量子状態は，2 つの基底ベクトル $|0\rangle = \binom{1}{0}$, $|1\rangle = \binom{0}{1}$ と，複素数として α, β を用いて，$\alpha|0\rangle + \beta|1\rangle = \binom{\alpha}{\beta}$ のように 2 次元ベクトルで記述することができる．ここで，量子状態を表すベクトルは単位ベクトルであり，$|\alpha|^2 + |\beta|^2 = 1$ である．n 量子ビットの量子状態は，テンソル積を用いて記述でき，ベクトルの次元は，2^n 次元となる．また，古典ビットの 0 と 1 はそれぞれ量子ビットの $|0\rangle$ と $|1\rangle$ を表している．

ここで，入出力の行列はユニタリ行列となる．したがって，行列 M の共役転置行列 $M^\dagger$ は，M の逆行列 M^{-1} と一致する．このことから，ユニタリ行列は逆演算を持つため量子演算は可逆である．

2.2 量子ゲート

本稿で用いる量子ゲートを図 1(a)–(f) に示す．各ラインの左側の変数を入力として右側の式の値が出力となる．図 1(a)(b)(d) は 2 入出力ゲート，図 1(e)(f) は 3 入出力ゲートである．それぞれの縦のラインで論理演算を表す．● で表される制御ビットによって $\oplus$, $\times$, $\boxed{f}$ で表される目標ビットを変化させる．ここで，$\oplus$ は排他的論理和，$\times$ は値の入替え，f は任意の演算を表す．制御 V ゲートは $|x\rangle = 1$ のときのみ $|y'\rangle = |\overline{y}\rangle$ にし，制御 $\mathrm{V}^\dagger$ ゲートは $|x\rangle = 0$ のときのみ $|y'\rangle = |\overline{y}\rangle$ にする．制御付 NOT（CN）ゲートと二重制御付 NOT（CCN）ゲート，Fredkin ゲートは制御ビットが全て 1 の場合にのみ目標ビットを変化させる．

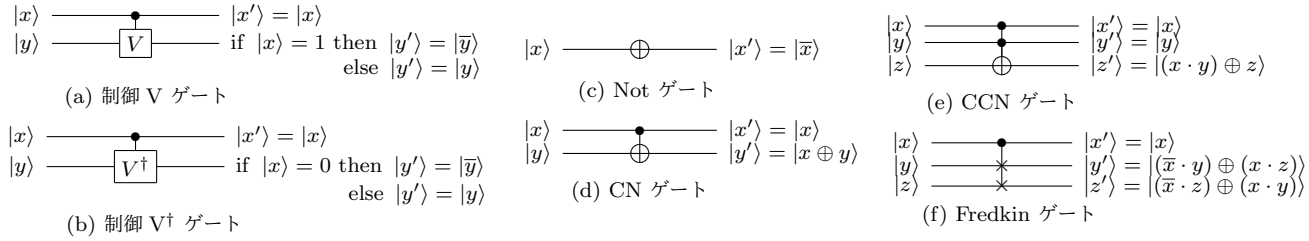
2.3 量子コスト（QC）

プリミティブ量子ゲートとは，入出力数が 1 または 2 となるゲートのことであり，量子回路の QC は，その構成に使われたプリミティブ量子ゲート数である [4]．図 1(a)–(d) はプリミティブであり $\mathrm{QC} = 1$ である．

また，CN と CCN ゲートを図 2(a) のように並べることで半加算器を構成することができる．このとき，半加算器の QC は，図 2(a) では，$\mathrm{QC} = 6$ である．しかし，プリミティブ量子ゲートのみで最適に構成した図 2(b) においては，$\mathrm{QC} = 4$ となる．本稿では，図 2(b) の方が QC の値が小さくより最適であるため，半加算器の QC は図 2(b) の構成として計算を行う．

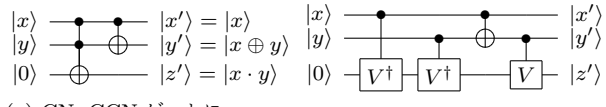
2.4 ancilla ラインとゴミライン

計算結果には含まれない不要な情報をもつ出力において，ancilla ラインとは，入出力が定数となっているライン



(a) 制御 V ゲート　(b) 制御 V† ゲート　(c) Not ゲート　(d) CN ゲート　(e) CCN ゲート　(f) Fredkin ゲート

図 1　量子ゲート



(a) CN, CCN ゲートによる構成　(b) プリミティブ量子ゲートのみによる構成

図 2　1 量子ビット半加算器

のことをいい，ゴミラインとは，入力もしくは出力が変数となっているラインのことをいう．

また，入力量子ビットが $|0\rangle$ のラインを $|0\rangle$ に初期化されたラインと呼ぶ．本稿では，ancilla ラインとゴミラインは $|0\rangle$ に初期化されたもののみを考える．

2.5　埋込み

非可逆な計算で失われる情報を全て保持することで可逆な計算にすることを，埋込みという [2]．例えば，非可逆である AND 演算を行うゲートなどに対して，入出力のライン数を増やすことで可逆性をもたせることができる．

2.6　ゴミラインの浄化方法

量子ビットは，現在維持できる数が少ないため貴重な資源となっている．よって再利用可能な定数に戻す，つまりゴミラインを ancilla ラインへと変換する方法としてゴミ浄化法がある [2]．

ゴミ浄化法は以下の 3 段階で構成することができる．

(i)　ゴミラインを用いて，任意の関数 f を求めるための論理回路 ϕ を構成する．

(ii)　ϕ を通すことで，関数 f に対応するラインの値を CN ゲートを用いてコピーする．

(iii)　ϕ の逆回路 $\overline{\phi}$ を通すことで，ゴミラインとなっていたラインを全て ancilla ラインに変換する．

以上より，ゴミ浄化法を適用することにより出力には元々の入力と解，及び ancilla ラインのみが残る．

3　関連研究

QRCA に関して，Vedral 他の方式 [8] では，最上位以外のラインにおいて，逆回路を計算することで ancilla ラインにした．Takahashi 他 [6] は，量子フーリエ変換を用いることで ancilla ラインを必要としない量子回路を構成した．以上の方式はゴミラインをもたない．一方，ゴミラインを許し CN ゲートと Fredkin ゲートを用いて最適化を行う方式 [7] が知られている．

QCLA に関して，CN ゲートと CCN ゲートのみを用いる Draper 他の方式 [1] では，最上位以外のラインにおいて，逆回路を計算することで不要な情報を含むラインを ancilla ラインにした．Fredkin ゲートも用いる Mogensen の方式 [5] では，[1] よりゲート数や QC が大きいが，ancilla ライン数が約半分である．

4　既存方式

本章では，3 章で扱った既存方式の内，[1, 8] の具体的な説明をする．なお，入力ビット列を A, B, それらの和である出力ビット列を S, 桁上げビット列を C とし，A, B, S, C の最下位から i 番目のビットをそれぞれ a_i, b_i, s_i, c_i と表す ($i \in \mathbb{Z}, i \geq 0$, $c_0 = 0$)．

4.1　Vedral 他の方式 [8]

QRCA である Vedral 他の方式 [8] の加算器は CN ゲートと CCN ゲートのみを用いて，3 段階で構成されている．

第 1 段階では，入力 a_i, b_i と前の桁からの桁上げ c_{i-1} から，桁上げ c_i を最上位ビットまで計算し（図 3(a) の回路 CARRY），その値を $|0\rangle$ に初期化されたラインに更新する．第 2 段階では，最上位ビットのラインに対して CN ゲートを適用した後，更新されたラインを ancilla ラインにするために第 1 段階の逆回路を計算する．第 3 段階では，第 1 段階で得られた桁上げ情報を元に和 s_i を計算し（図 3(a) の回路 SUM），b_i のラインにその値を更新する．

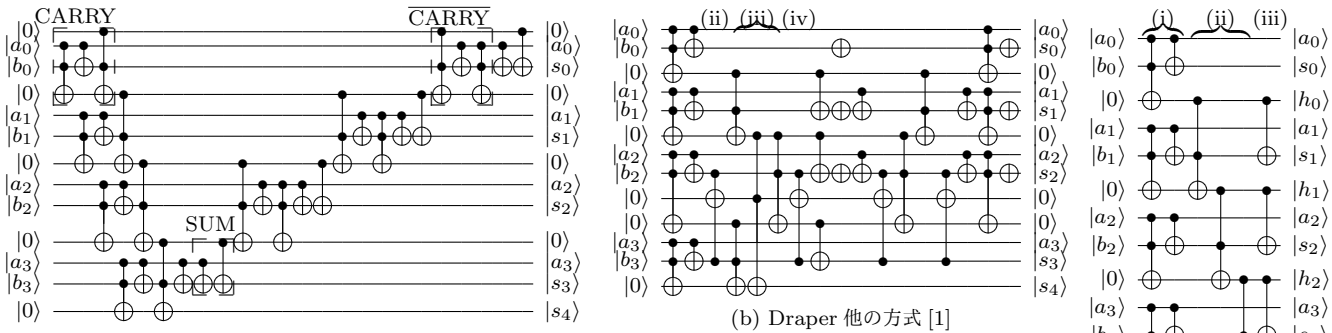
図 3(a) は，入力が 4 ビット のときの Vedral 他の方式 [8] である．

4.2　Draper 他の方式 [1]

QCLA である Draper 他の方式 [1] の加算器は CN ゲートと CCN ゲートのみを用いて，6 段階で構成されている．

第 1 段階では，入力ライン a_i と b_i に対して，生成 $g_i = a_i \cdot b_i$ と伝播 $p_i = a_i \oplus b_i$ を計算する．g_i の値は $|0\rangle$ に初期化されたラインに，p_i の値は b_i のラインにそれぞれ更新する．第 2 から第 4 段階で，桁上げ情報を二分木状に伝播させる（図 3(b) の (ii)–(iv)）．第 5 段階では，第 4 段階の桁上げ情報をもとに和 s_i を計算し，その値を b_i のラインに更新する．第 6 段階では，生成で用いたラインをそれぞれの逆回路に通すことでゼロクリアし，ancilla ラインとする．

図 3(b) は，入力が 4 ビット のときの Draper 他の方式 [1] である．



(a) Vedral 他の方式 [8]　(b) Draper 他の方式 [1]　(c) 提案方式

図 3　既存方式，及び提案方式による 4 量子ビット加算器（ただし，$A + B = S$ である）

5　提案方式

ゴミラインを使って量子桁上げ伝播加算器の深さを減少させる．そのためのアプローチとして，古典的な RCA の加算器において途中で消去される全ビットを記憶する．これは古典的な加算器の “埋込み” といえる．

5.1　構成方法

提案方式の QRCA は CN ゲートと CCN ゲートのみを用いて，3 段階で構成されている：

(i)　入力ライン a_i と b_i に対して，桁上げ $c_i = a_i \cdot b_i$ とその桁の和 $s_i = a_i \oplus b_i$ を計算する．c_i の値は $|0\rangle$ に初期化されたラインに，s_i の値は b_i のラインにそれぞれ更新をする．

(ii)　$i \geq 1$ のビットに対して，c_{i-1} と s_i から桁上げを最上位ビットまで計算し，その値を第 1 段階で計算した桁上げのラインに更新する．

(iii)　第 2 段階で求めた桁上げ情報を元に和を計算し，その値を b_i のラインに更新する．

図 3(c) は，入力が 4 ビット のときの提案方式である．埋込みのためのラインは，入力とは関係がない $|0\rangle$ のラインを用意し，そのラインに桁上げ情報を記憶させた．また，提案方式はゴミ出力 h_i を許すため，逆回路を計算しない分の QC，深さが小さくなる．

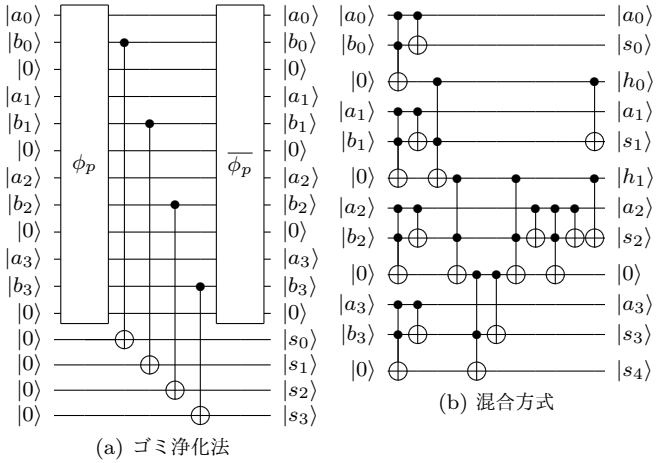
5.2　ゴミ浄化法

提案方式に 2.6 節で説明したゴミ浄化法を適用する．図 4(a) は，入力が 4 ビット のときのゴミ浄化法の提案方式（以下，ゴミ浄化法）である．ϕ_p には提案方式，$\overline{\phi_p}$ には提案方式の逆回路がはいる．提案方式を計算した後に，CN ゲートを用いて $|0\rangle$ に初期化されたラインにその桁の和を更新する．その後，提案方式の逆回路を挟むことでゴミラインをゼロクリアし ancilla ラインに変換する．

6　結果

6.1　比較

既存方式 [1, 8] と提案方式，及びゴミ浄化法の深さ（d），QC，ゴミライン数（gline），$|0\rangle$ に初期化されたライン数（iline）は表 1, 2の通りである．



(a) ゴミ浄化法　(b) 混合方式

図 4　提案方式による 4 量子ビット加算器

一般の場合の提案方式，及びゴミ浄化法は，係数比較した場合，深さに関しては [8] から n の係数が減少したが，[1] よりも増加した．これは古典的にも CLA の深さが RCA の深さよりも漸近的に優れていることによる．また，QC に関して，提案方式は [1] より 89.2%，[8] より 70.0% 減少し，ゴミ浄化法は，[1] より 76.7%，[8] より 35.0% 減少した．よって，QC は [1], [8] より提案方式，及びゴミ浄化法の方が指標は下回った．

入力が 2–8 ビットの場合に提案方式は，ゴミライン数以外の全ての指標で既存方式 [1, 8] を上回ることはなかった．一方，ゴミ浄化法は，$|0\rangle$ に初期化されたライン数以外の全ての指標で既存方式 [8] を上回ることはなかった．また，既存方式 [1] において入力が 4 ビットのときのみ，深さが下回った．以上より，入力ビット数が小さいときにも本方式が最適となり，有効な場合があるといえる．

6.2　混合方式

次に，提案方式に既存方式を一部組み込むことで既存方式を単体で用いるより，最適化された回路を設計できることを示す．本研究では，QRCA の設計方法を提案したため，既存方式 [8] を組み込んだ回路を例に挙げる．

入力量子ビット数が 4 ビットでゴミライン数を 2 まで許

表 1　一般の場合の量子加算器回路のコストの比較

量子	既存方式 [1]				既存方式 [8]				提案方式				ゴミ浄化法			
ビット数	QC	d	gline	iline	QC	d	gline	iline	QC	d	gline	iline	QC	d	gline	iline
n	$56n - o(\log n)$	$O(\log n)$	0	$\frac{3}{2}n - 1$	$20n - 8$	$6n$	0	$n + 1$	$6n - 2$	$n + 2$	$n - 1$	n	$13n - 4$	$3n + 4$	0	$2n$

表 2　入力量子ビット数が小さい場合の量子加算器回路のコストの比較

量子	既存方式 [1]			既存方式 [8]			提案方式			ゴミ浄化法		
ビット数	d	gline	iline	d	gline	iline	d	gline	iline	d	gline	iline
2	8	0	2	12	0	3	4	1	2	10	0	4
4	18	0	5	24	0	5	6	3	4	16	0	8
6	20	0	9	36	0	7	8	5	6	22	0	12
8	25	0	12	48	0	9	10	7	8	28	0	16

す制約があった場合，提案方式に既存方式 [8] を組み込むことで図 4(b) のように回路を構成することができる．このとき，混合方式は上記の制約を満たした上で，深さ 11，QC = 40 となる．よって，既存方式 [8] より深さと量子コストが最適な回路を設計することができる．以上より，既存方式 [8] を単体で用いるより，提案方式に既存方式を一部組み込むことで最適に設計できる場合がある．

7　評価・考察

7.1　評価

既存方式と提案方式の漸近的な複雑さの解析から，提案方式は，深さに関して，一般の場合は既存方式 [8] より最適となり，入力ビット数が小さいとき既存方式 [1, 8] より最適となった．QC に関して，常に既存方式 [1, 8] より最適となった．したがって，既存方式と提案方式からゴミライン数と深さ，及び QC はトレードオフ関係にあるといえる．

ゴミ浄化法は，深さに関して，一般の場合は既存方式 [8] より最適となる．入力ビット数が小さいときは既存方式 [8] より最適となり，既存方式 [1] に対してはある範囲においては最適となった．QC に関して，常に既存方式 [1, 8] より最適となった．既存方式とゴミ浄化法は，$|0\rangle$ に初期化されたライン数と深さ，及び QC はトレードオフ関係にあるといえる．

7.2　考察

本研究では，深さの最適化を目指したが，副次的な効果として QC も同時に最適化を図ることができた．これは，既存方式よりも使用するゲート数が少ないからだと考えられる．また，回路設計では，漸近的振る舞いだけでなく，有限個においての議論をすることにも価値がある．したがって，入力が定数における指標の減少も有意義な結果といえる．

また，量子ビットは，現在維持できる数が少ないため貴重な資源となっている．よって既存方式 [1, 8] では，深さなどの指標より量子ビットを優先した設計方法を行なっていた．しかし，量子ビットを作成，及び制御する技術が，いくつかの研究グループにおいて小さな量子計算機で原理実証を行うまでに達している．したがって，今後維持できる量子ビット数が増加したとき，本方式の設計方法は，量子ビットより他の指標を優先した設計を考える際の有用な知見になり得ると考えられる．

8　おわりに

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ことがある．今回，提案方式は既存方式 [1, 8] に対して，入力ビット数が小さいときに QC・深さがより最適となり，さらに一般の場合に QC がより最適であることを示すことができた．よって，提案方式と既存方式 [1, 8] から，ゴミラインは QC・深さに対してトレードオフ関係であり，ゴミ浄化法と既存方式 [1, 8] から，$|0\rangle$ に初期化されたラインは QC・深さに対してトレードオフ関係である．また，既存方式を単体で用いるより，ある制約のもと提案方式と組み合わせることでより最適化された回路を設計できることも示せた．

今後の課題として，制約に応じた最適な回路の一般的方法の提案，他の演算回路への応用，及び入力ビット数の小さい場合のコストをさらに解析することが挙げられる．

参考文献

[1] Draper, T.G., Kutin, S.A., Rains, E.M., et al.: A Logarithmic-Depth Quantum Carry-Lookahead Adder, *Quantum Info. Comput.*, Vol.6, No.4&5, pp.351–369 (2006).

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

[3] Golubitsky, O. and Maslov, D.: A Study of Optimal 4-Bit Reversible Toffoli Circuits and Their Synthesis, *IEEE Trans. Comput.*, Vol.61, No.9, pp.1341–1353 (2012).

[4] Hung, W., Song, X., Yang, G., et al.: Optimal Synthesis of Multiple Output Boolean Functions Using a Set of Quantum Gates by Symbolic Reachability Analysis, *IEEE Trans. on CAD*, Vol.25, No.9, pp.1652–1663 (2006).

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

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

[7] Van Rentergem, Y. and De Vos, V.: Optimal Design of A Reversible Full Adder, *Int. J. Unconv. Comput.*, Vol.1, pp.339–355 (2005).

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