量子桁上げ伝播加算器回路の深さの効率化について

柴田 心太郎*，横山哲郎（南山大学）

On a Quantum In-Place Ripple-Carry Addition with Lower Depth

Shintaro Shibata*, Tetsuo Yokoyama (Nanzan University)

1 はじめに

近年，量子計算機の分野の研究は活発であり，その中でも有名な量子アルゴリズムの一つである Shor のアルゴリズムのための，効率的な量子回路の実現は重要な課題である．本稿では in-place な量子加算器回路のみを考える．現在，ゴミラインがなく深さが $O(\log n)$ の桁上げ先見方式 [1] や $O(n)$ の桁上げ伝播方式 [2]，ゴミラインがある深さ $O(n)$ の桁上げ伝播方式のもの [4] が知られている．これらの回路はゲート数や深さ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，ゲート数や深さなどの制約に応じて効率的な回路を得る一般的方法は明らかにされていない．

本稿では，入力ビット数 4 のゴミラインがある桁上げ伝播方式の量子加算器回路の設計をし，既存手法 [1, 2, 4] に対して，入力ビット数が小さいときに量子コスト・ゲート数・深さが効率的なことを示し，さらに一般の場合に量子コスト・ゲート数が効率的であることを示す．提案方式は既存方式とトレードオフ関係にある新たな方式であり，本稿のアイデアは他の算術・論理演算の量子回路に応用されることが期待される．

本稿では，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 ($i \in \mathbb{Z}, i \geq 0, c_0 = 0$)．

2 関連研究

Draper 他の方式 [1] では古典的な桁上げ先見加算器の考え方を量子回路に応用した．各 i に関して a_i と b_i の和 s_i と桁上げ c_i を半加算器（Half Adder）で得て，桁上げ情報を二分木状に伝播させたり，桁上げ情報の伝播の逆計算をしたりして，不要な情報を含むラインを 0 にする．

Vedral 他 [2] は桁上げ伝播加算器の考え方を量子回路に応用した．

3 量子ゲート

本稿で用いる量子ゲート Not, Feynman, Toffoli を図 2(a-b) 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．ここでライン上の $\bullet$ は制御，$\oplus$ は目標のラインであることを，式の中の $\oplus$ は排他的論理和を表す．Toffoli と Feynman のゲートを並べて図 2(c) のような半加算器が構成できる．量子ゲートの量子コストは，その量子ゲートの構成に使われた NOT, 制御-V, 制御-$V^\dagger$, Feynman のゲートの数である．Not, Feynman, Toffoli のゲートの量子コストはそれぞれ 1, 1, 5 である．

4 提案方式

我々はゴミラインを使って桁上げ伝播加算器の深さを減少させることを試みる．本稿では，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すべて記憶しておくというアプローチをとる．これは古典的な加算器の “埋込み” といえる．

提案方式では，$n = 1$ のとき半加算器，$n \geq 2$ のとき半加算器の右側に Carry と Sum からなる全加算器が $n - 1$ 個置いた回路になる．ここで，それぞれの半/全加算器の桁上げビットが入力となるように次の全加算器が置かれる．

5 比較

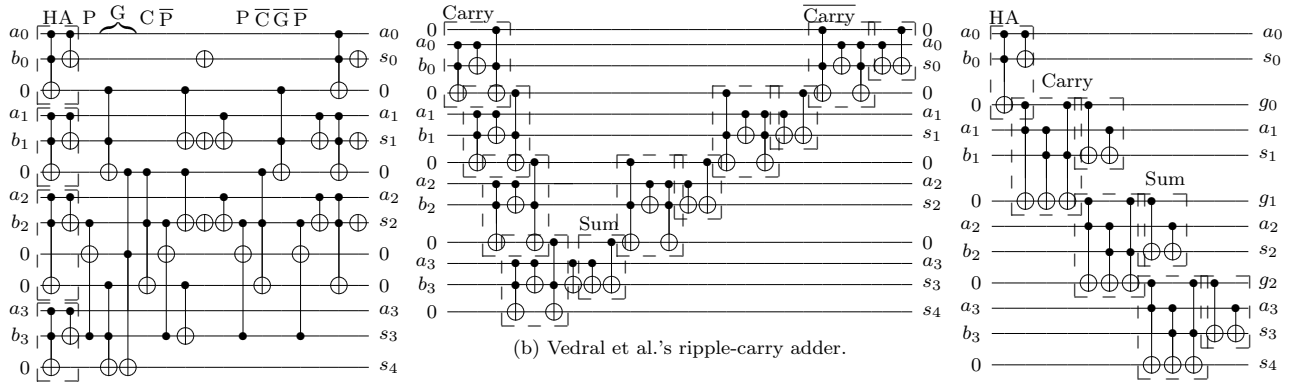
提案手法と既存手法 [1, 2] の量子コスト，ゲート数，深さ，ancillae 数，及びゴミライン数は表 1 の通りである．入力数が大きい場合に提案手法は，量子コストに関しては [1] より約 70%，[2] より約 30% 減少し，ゲート数に関しては [1] より約 50%，[2] より約 30% 減少した．一方，深さに関しては [2] から n の係数が減少したが，[1] よりも増加した．これは古典的にも桁上げ先見方式の深さが桁上げ伝播方式の深さよりも漸近的に優れていることによる．入力が 1–4 ビットの場合に提案手法は，ゴミライン数以外のすべての指標で既存手法 [1, 2] を上回ることはなかった．したがって入力ビット数が小さいときにも本手法が有効な場合があるといえる．

6 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効率が良いことがある．既存方式と提案方式を組み合わせてより多くのトレードオフ関係にある方式を探すこと，本アプローチを用いた効率的な剰余演算や乗算の回路の実装，およ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は今後の課題である．(本研究は JSPS 科研費 18K11250 の助成を受けた．)

文 献

[1] T.G.Draper, et al.: Quant. Inf. Comput., Vol.6, No.4&5, pp.351-369, 2006.
[2] V.Vendral, et al.: Phys. Rev. A, Vol.54, No.1, pp.147-153, 1996.
[3] H.Thapliyal, et al.: Trans. Comput. Sci. XVII, LNCS, Vol.7420, pp.73–97, 2013.
[4] Y.V.Rentergem.: Int. J. Unconv. Comput., Vol.1, pp.339-355, 2004.
[5] T.Æ.Mogensen: RC 2019, LNCS, Vol.11497, pp.224–237, 2019.



(a) Draper et al.'s carry-lookahead adder.

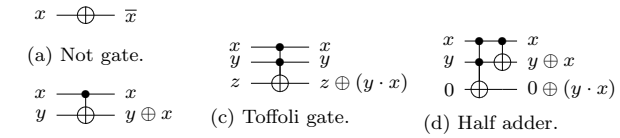
(b) Vedral et al.'s ripple-carry adder.

(c) The proposed adder.

Fig. 1: Quantum addition circuits with width four.

Table 1: Comparison of circuits.

ビット数	Draper 他 [1] ($n \geq 7$)					Vedral 他 [2] ($n \geq 3$)					提案手法 ($n \geq 2$)				
	量子コスト	ゲート数	深さ	ancillae	ゴミライン	量子コスト	ゲート数	深さ	ancillae	ゴミライン	量子コスト	ゲート数	深さ	ancillae	ゴミライン
1	6	2	2	0	0	14	6	6	1	0	6	2	2	0	0
2	23	8	6	1	0	38	14	13	2	0	23	7	6	0	1
3	46	18	10	2	0	62	22	20	3	0	40	12	9	0	2
4	102	34	18	4	0	86	30	24	4	0	57	17	12	0	3
n	$56n - o(\log n)$	$10n - o(\log n)$	$O(\log n)$	$2n - o(\log n)$	0	$24n - 10$	$8n - 2$	$4n + 8$	n	0	$17n - 11$	$5n - 3$	$3n$	0	$n - 1$



(a) Not gate.

(b) Feynman gate.

(c) Toffoli gate.

(d) Half adder.

Fig. 2: Basic gates and a half adder.