量子桁上げ伝播加算器回路における混合方式の解析

2018SE036　黒川　誠史
指導教員：横山　哲郎

1　はじめに

近年，量子コンピュータ，量子計算の分野の研究が活発である．量子コンピュータは，現代のコンピュータでは処理できない複雑な計算を処理できると考えられており，Google や IBM，Microsoft といった企業が研究開発し，注目を集めている．量子計算は，古典計算に量子力学を組み合わせたもので，古典計算よりも高性能となる．

本研究では，量子桁上げ伝播加算器回路における混合方式の解析を目的とする．混合方式とは，柴田の提案方式 [4] に既存方式の一部を組み込む方式である．混合方式を用いることによって既存方式よりも最適化された回路を設計できることが柴田の研究 [4] により明らかになっている．本研究では，既存方式を Vedral 他の方式 [3] とする．研究課題として 2 つ挙げる．1 つ目は，4 ビットと 8 ビットにおける混合方式の量子回路を構成することである．これは，2^n ビットの量子回路を小さい方から構成することによって，一般の場合を類推するためである．2 つ目は，4 ビットと 8 ビットのトレードオフ関係にあるコストを解析することである．コストの解析を行うことによって各コストの一般化の見通しを立てる．本研究で解析するコストは量子コスト・深さ・トランジスタ・遅延・ゴミライン数である．正確に見積もられたコストのトレードオフ関係にある量子回路を取りそろえることによって，量子回路設計の最適化につながることが期待される．

2　関連研究

2.1　量子ビット

量子ビットとは，量子計算機で利用される基本単位である．これは，古典計算機で利用される古典ビットとは異なる性質がある．古典ビットは 0 か 1 のどちらか一方しか用いることができないが，量子ビットは 0 と 1 の両方の状態であるような重ね合わせた状態で用いることができる．量子ビットの 0 と 1 はそれぞれ $|0\rangle$，$|1\rangle$ と書く．

2.2　量子回路

量子回路とは，量子演算を実行するために必要ないくつかの量子ゲートを組み合わせてできる量子計算のモデルである．量子回路は単射である計算のみ扱う性質があるため，可逆性が存在する．量子回路は，それぞれの量子状態とを対応させる量子演算を実行するための量子ゲートを組み合わせる．それによって入力した量子の状態を変化させた量子の状態を出力するという仕組みである．

2.3　量子ゲートと量子コスト

量子ゲートとは，量子演算を実行するために必要なものである．入出力は量子ビットを使用し，入力された値によって量子状態を変化させる．

量子コストとは，量子回路を作成するときに必要なコストで，量子回路の構成に含まれるプリミティブ量子ゲートの数である．プリミティブ量子ゲートとは，量子回路の入出力数が 1 または 2 となる量子ゲートのことである．

2.4　トランジスタと遅延

トランジスタと遅延は dual-line pass-transistor CMOS technology による評価を行う [1, 2]．トランジスタを対象とする理由は，dual-line pass-transistor CMOS technology で回路をリアルサイズ化することによって，より正確なコスト見積もりを行うことができること [2]，トランジスタ数が削減すると，それに伴い消費エネルギーが削減されるという恩恵が得られること [1] が挙げられる．本研究で扱う量子ゲートのトランジスタは CNOT ゲートが 8，Toffoli ゲートが 16 である．遅延は，本研究では NOT ゲートが存在しない量子回路図であるため深さと同様の結果を得ることができる．

2.5　柴田の提案方式

柴田の提案方式 [4] は，量子桁上げ伝播方式で，不要なビットをゴミラインですべて記憶している．この方式は CNOT ゲートと Toffoli ゲートのみを使用している．構成方法は，まず入力として，A_i，B_i を用意する．それに対して，桁上がりの値 $C_i = A_i \cdot B_i$ と和 $S_i = A_i \oplus B_i$ を計算し，それぞれ初期化された $|0\rangle$ と B_i のラインに更新する．次に，$i \geq 1$ のとき，C_{i-1} と S_i から桁上がりの値を計算する．最上位まで達したら，その値を最初に計算した桁上がりのラインに更新する．最後に，一つ前で計算した桁上がりの値から和を計算し，B_i のラインに更新する．桁上がりの値を保存するために初期化された $|0\rangle$ のラインの出力は変数となるので，ゴミラインである．これは，入力が常に変化しているためである．

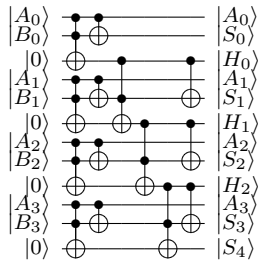
2.6　Vedral 他の方式

Vedral 他の方式 [3] は，量子桁上げ伝播方式である．この方式は CNOT ゲートと Toffoli ゲートのみを使用し，ゴミラインを持たない．また，最上位以外のラインで逆回路を計算することによって，ancilla ラインを作成している．この構成方法は，まず入力として，A_i，B_i を用意する．前の桁の桁上がりの値 C_{i-1} から桁上がりの値 C_i を最上位

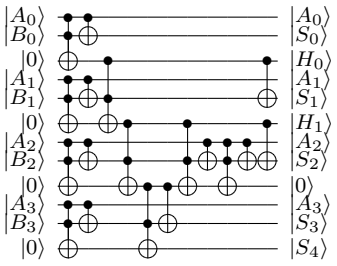
ビットまで計算する．その値を初期化されたライン $|0\rangle$ に更新する．ただし，$i \in \mathbb{Z}$, $i \geq 0$, $C_{-1} = 0$ とする．次に，最上位のビットにおいて CNOT ゲート通過後に最初の段階の逆回路を計算する．それにより，更新したラインを ancilla ラインに変換する．最後に，最初の段階で計算された桁上がりの値から和 S_i を計算し，B_i のラインに更新する．

3 混合方式

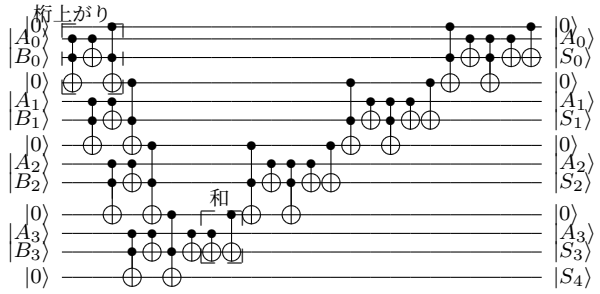
混合方式とは，柴田の提案方式 [4] に Vedral 他の方式 [3] の一部を組み込むことで構成した量子回路である．混合方式を用いることにより既存方式よりも最適化された回路を設計できることが柴田の研究で明らかになっている．Vedral 他の方式 [3] の一部とは，図 1(c) の桁上がりと和の部分である．柴田の提案方式 [4] には，桁上がりの回路があり，これの逆回路と和の回路を通すことでゴミラインをなくすことができる．これにより構成した混合方式の回路が図 1(b) となる．図 1(b) はゴミライン数を 2 まで許したときの混合方式である．



(a) 柴田の提案方式 [4](ゴミライン数 3)



(b) 混合方式 (ゴミライン数 2)[4]



(c) Vedral 他の方式 [3](ゴミライン数 0)

図 1: 4 ビットの既存方式と混合方式

4 結果

4 ビット入力の全ての場合の混合方式をまとめると表 1のようになる．ただし，ゴミライン数 3 の混合方式は柴田の提案方式 [4] と同様なので [4] の方式と表し，ゴミライン数 0 の混合方式は Vedral 他の方式 [3] と同様なので [3] の方式と表す．また，ゴミライン数 2 の混合方式のとき，表では $g = 2$ と書き，他の混合方式の場合も同様に書く．4 ビット入力のとき，混合方式による量子回路 (例：図 1(b)) をゴミライン数 0 の場合を除き，構成することができた．また，表 1より，トレードオフ関係にあるコスト (量子コスト・深さ・トランジスタ・遅延) は減少するが，ゴミライン数は増加していることがわかった．このことから，ゴミライン数を制約とした場合，量子コスト・深さ・トランジスタ・遅延は最適化されていると言える．

表 1: 4 ビット入力の比較

方式	量子コスト	深さ	ゴミライン	$\|0\rangle$ ライン	トランジスタ	遅延
[4] の方式	22	6	3	4	168	6
$g = 2$	32	11	2	4	216	11
$g = 1$	42	16	1	4	264	16
[3] の方式	72	24	0	5	352	24

5 考察

ゴミライン数を増減させることによって 4 ビットと 8 ビットの混合方式 no 量子回路をゴミライン数 0 の場合を除き，構成することができた．また，トレードオフ関係にあるコストを解析し，量子コスト・深さ・トランジスタ・遅延において減少し，ゴミライン数は増加していることが分かった．結果で述べた混合方式が最適化されている点は柴田の研究でも明らかになっている．ここから，ゴミライン数 0 の場合を除いた混合方式の各コストの一般化は，量子コストが $6n + 10m - 12$，深さと遅延が $n + 5m - 3$，トランジスタが $24(2n + 2m - 3)$ と予測できる．n はビット数，m は減らしたゴミライン数とし，$m = n - g$ とする (g = ゴミライン数)．今回はゴミライン数を増減させることで混合方式を構成したが，別の方法でも構成できると考えられる．トレードオフ関係にあるコストも解析できると考えられる．また，ゴミライン数 0 の量子回路は，最上位のラインを増やさずに構成できると考えられる．

6 おわりに

本研究では，4 ビットと 8 ビットの混合方式の量子回路をゴミライン数 0 の場合を除き，構成できた．また，トレードオフ関係にあるコストを解析することによって，量子コストと深さ・遅延，トランジスタの一般化の見通しを立てることができた．ゴミライン数 0 の場合の混合方式の構成や，それを含めた混合方式の各コストの一般化が今後の課題として挙げられる．

参考文献

[1] Thomsen, M. K. and Axelsen, H. B.: Parallel Optimization of Reversible Ripple-Carry Adders, *Parallel Processing Letters*, Vol. 19, No. 2, pp. 205–222 (2009).

[2] Van Rentergem, Y. and De Vos, A.: Optimal design of a reversible full adder, Vol. 1, pp. 339–355 (2005).

[3] Vedral, V., Barenco, A. and Ekert, A.: Quantum networks for elementary arithmetic operations, *Physical Review A*, Vol. 54, pp. 147–153 (1996).

[4] 柴田心太郎：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 2019 年度修士卒業論文 (2020).