数理解析研究所講究録
第1148巻 2000年 58-63



# Phase-Shift と Controlled-Not で構成される量子回路について

安倍 秀明 (Hideaki ABE) *　　宋 少秋 (Shao Chin SUNG) *

## 1 はじめに

量子計算機は計算原理として量子力学を取り込んだ新しい計算機である．量子計算機のモデルとして，Deutsch [4, 5] は量子チューリング機械と量子回路を提案した．また，量子回路は量子チューリング機械と同じ計算能力をもつことが知られている [7].

本論文では補助ビットを用いた量子回路の並列化に関する結果を示す．従来研究として Moore と Nilsson [6] は Controlled-Not ゲートで構成される任意の $n$ 入力量子回路について，$O(n^2)$ 補助ビットを用いることで，深さを $O(\log n)$ にできることを示した，また，$t$ 個の $s$ 入力 Phase-Shift ゲートと Controlled-Not ゲートで構成される任意の $n$ 入力量子回路について，$O(stn+n^2)$ 補助ビットを使用することで，深さ $O(\log n+\log t)$ にできることも示した．

本論文の結果として，Moore と Nilsson [6] の結果を拡張し，使用できる補助ビットの数が任意に固定された場合，上の二種類の量子回路について並列化手法を示した．その特殊な場合として，Moore と Nilsson [6] の結果で使用する補助ビットの数を $1/\log n$ 倍にしても，同じ深さに並列化できることも示した．

## 2 諸定義

この節では，量子回路に関する諸定義を行う（詳しくは [5, 7] を参照）．量子計算機では，一ビットを二状態の物理系を用いて表現し，それを**量子ビット**と呼ぶ．量子力学では，二状態の物理系の状態は二次元ヒルベルト空間のベクトルに対応する．ここで，量子力学で用いられるケットベクトル表現 $|\cdot\rangle$ を用いて

$$|0\rangle=\begin{pmatrix}1\\0\end{pmatrix},\quad |1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$$

とする．また，任意の正整数 $k$ と任意の $X=(x_1,x_2,\ldots,x_k)\in\{0,1\}^k$ に対し，

$$|X\rangle=|x_1\rangle\otimes|x_2\rangle\otimes\cdots\otimes|x_k\rangle$$

とすると，集合 $\{|X\rangle \mid X\in\{0,1\}^k\}$ は $2^k$ 次元ヒルベルト空間の基底となる[1]．ここで，$\otimes$ はテンソル積を表す．$k$ 量子ビットの状態 $|\psi\rangle$ は基底 $\{|X\rangle \mid X\in\{0,1\}^k\}$ の線形重合わせ

$$|\psi\rangle=\sum_{X\in\{0,1\}^k}\alpha_X|X\rangle$$

と表現できる．ただし，$\sum_{X\in\{0,1\}^k}|\alpha_X|^2=1$ である．また，$\alpha_X$ は状態 $|\psi\rangle$ における $|X\rangle$ の**振幅**と呼ばれ，$\alpha_X=|\alpha_X|e^{i\beta_X}$ となる $\beta_X$ は状態 $|\psi\rangle$ における $|X\rangle$ の**位相**と呼ばれる．そして，任意の $X\in\{0,1\}^k$ に対し，$k$ 量子ビットの状態が $|X\rangle$ であるとき，その $k$ 量子ビットが値 $X$ であると解釈する．

また，量子力学の制約から，量子ビットの任意の状態推移は量子ビットの状態のユニタリ変換となり，また，任意のユニタリ変換による量子ビットの状態推移が可能であることが知られている [3]．ここで，ユニタリ変換とはユニタリ行列で定義される変換である．また，行列 $\mathcal{U}$ がユニタリとは，その共役転置行列 $\mathcal{U}^\dagger$ がその逆行列 $\mathcal{U}^{-1}$ となる．任意の正整数 $k$ に対し，$2^k\times 2^k$ ユニタリ行列で定義される任意のユニタリ変換を $k$ **ビット変換**と呼ぶ．以降，$k$ ビット変換をその変換を定義するユニタリ行列で表す．

以下では，本論文で用いる変換の定義を行う．まず，二ビット変換

$$\mathcal{U}_{CN}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

は **Controlled-Not** と呼ばれ，任意の二量子ビットの状態 $|\psi\rangle=\sum_{(x_1,x_2)\in\{0,1\}^2}\alpha_{(x_1,x_2)}|x_1,x_2\rangle$ に対し，

$$\mathcal{U}_{CN}|\psi\rangle=\sum_{(x_1,x_2)\in\{0,1\}^2}\alpha_{(x_1,x_2)}|x_1,x_1\oplus x_2\rangle \quad (1)$$

となる．ここで，第一ビットは**制御ビット**と呼ばれ，第二ビットは**目標ビット**と呼ばれる．

また，任意の正整数 $k$ に対し，ある $k$ ビット変換 $\mathcal{U}$ が **Phase-Shift 変換**（以下では，略して $PS$ 変換）であるとは，$2^k$ 個のある実数 $\gamma_{0^k},\gamma_{0^{k-1}1},\ldots,\gamma_{1^k}$ が存在し，$\mathcal{U}$ が以下のように

*北陸先端科学技術大学院大学情報科学研究科，〒 923-1292 辰口町旭台 1-1，Email：{h_abe, son}@jaist.ac.jp

[1]本論文では，便宜のため，$X\in\{0,1\}^k$ に対し，$X$ をベクトル $X=(x_1,x_2,\ldots,x_k)$，および，$X$ を文字列 $X=x_1x_2\cdots x_k$ とする二つの表記法を用いている．

定義されるときである．

$$\mathcal{U} = \begin{pmatrix} e^{i\gamma_{0^k}} & & & 0 \\ & e^{i\gamma_{0^{k-1}1}} & & \\ & & \ddots & \\ 0 & & & e^{i\gamma_{1^k}} \end{pmatrix}.$$

このとき，任意の $k$ 量子ビットの状態 $|\psi\rangle = \sum_{X\in\{0,1\}^k} \alpha_X |X\rangle$ に対し，

$$\mathcal{U}|\psi\rangle = \sum_{X\in\{0,1\}^k} \alpha_X e^{i\gamma_X} |X\rangle$$

となる．

次に，量子回路を構成する素子である量子ゲートと補助ビットの定義を行う．任意の正整数 $k$ に対し，$k$ **ビット量子ゲート**とは，$k$ 量子ビットの入力と出力をもち，ある $k$ ビット変換 $\mathcal{U}$ が存在し，入力の状態 $|\psi\rangle$ に対して状態 $\mathcal{U}|\psi\rangle$ を出力の状態とする．このとき，この $k$ ビット量子ゲートは $k$ ビット変換 $\mathcal{U}$ を**実現**するという．本論文では，二ビット変換 $\mathcal{U}_{CN}$ を実現する二ビット量子ゲート，*CN* **ゲート**，とある $k$ ビット *PS* 変換を実現する $k$ ビット量子ゲート，$k$ ビット *PS* **ゲート**，を使用する．また，**補助ビット**とは，量子ビットであり，その状態は入力時と出力時とも $|0\rangle$ である[2]．補助ビットの役割として，量子ビットの状態の保存，並列に配置できる量子ゲートの数を増やすなどがある．

任意の正整数 $n$ に対し，$n$ **入力一層の量子回路**とは $n$ 量子ビットの入力と出力をもち，入力を共有しない量子ゲートで構成され，実現する $n$ ビット変換は各量子ゲートが実現する変換のテンソル積となる．ここで，どの量子ゲートの入力でもない量子ビットには $2\times 2$ 単位行列で定義される変換 $\mathcal{I}$ を実現する一ビット量子ゲートが配置されていると考える．そして，$n$ **入力量子回路**とは，$n$ 入力一層の量子回路の系列であり，**実現**する $n$ ビット変換は各一層の量子回路が実現する $n$ ビット変換の積となる．また，本論文では，量子回路の複雑さの尺度として**深さ**（すなわち，層の数）と**補助ビット数**を考える．

本論文では次の二種類の量子回路を扱う．

- *CN* ゲートで構成される量子回路，と
- 任意の正整数 $s$ に対し，$s$ ビット *PS* ゲートと *CN* ゲートで構成される量子回路．

この二種類の量子回路に対する補助ビットを用いた並列化に関する従来研究として Moore と Nilsson [6] の結果がある．

**命題 1** *CN* ゲートで構成され，$n$ ビット変換 $\mathcal{U}$ を実現する $n$ 入力量子回路が与えられたとき，$O(n^2)$ 補助ビットを用いて変換 $\mathcal{U}$ は深さ $O(\log n)$ の *CN* ゲートで構成される量子回路で実現できる．

**命題 2** $t$ 個の $s$ ビット *PS* ゲート $G_1, G_2, \ldots, G_t$ と *CN* ゲートで構成され，$n$ ビット変換 $\mathcal{U}$ を実現する $n$ 入力量子回路が与えられとき，$O(stn+n^2)$ 補助ビットを用いて変換 $\mathcal{U}$ は深さ $O(\log n+\log t)$ の $t$ 個の $s$ ビット *PS* ゲート $G_1, G_2, \ldots, G_t$ と *CN* ゲートで構成される量子回路で実現できる．

本論文では，この二種類の量子回路のそれぞれについて，使用できる補助ビットの数が任意に固定された場合の並列化手法を示し，その特殊な場合として，各命題で用いる補助ビットの数を $1/\log n$ 倍にしても同じ深さにできることも示す．

## 3 *CN* ゲートで構成される量子回路

この節では，*CN* ゲートで構成される量子回路の並列化に関する結果を示す．結果を示す前に，*CN* ゲートで構成される量子回路の性質について考える．

まず，*CN* ゲートで構成される量子回路が実現する変換について考える．式 (1) から，*CN* ゲートを任意の状態に適用することは，ある量子ビット（すなわち，目標ビット）を別のある量子ビット（すなわち，制御ビット）との排他的論理和にすることである．$\mathcal{U}$ を *CN* ゲートで構成される $n$ 入力量子回路が実現する任意の $n$ ビット変換とすると，$\mathcal{U}$ は次の条件を満たす．任意の $X = (x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ に対し，集合に対する排他的論理和において線形独立となる集合 $S_1, S_2, \ldots, S_n \subseteq \{1, 2, \ldots, n\}$ が存在し，

$$\mathcal{U}|X\rangle = |F_{\mathcal{U}}(X)\rangle$$

となる．ただし，

$$F_{\mathcal{U}}(X) = \left( \bigoplus_{j\in S_1} x_j, \bigoplus_{j\in S_2} x_j, \ldots, \bigoplus_{j\in S_n} x_j \right)$$

である．また，$S_1, S_2, \ldots, S_n$ が集合に対する排他的論理和において線形独立となることを示す．$n$ 量子ビットの任意の状態を一般性を失うことなく $|X\rangle$ とすると，$X = F_{\mathcal{I}}(X)$ と表現でき，このとき $S_v = \{v\}$ $(1 \le v \le n)$ となり，集合に対する排他的論理和において線形独立となる．ここで，$\mathcal{I}$ は $2^n \times 2^n$ 単位行列である．また，ある $v$ と $w$ $(1 \le w \le n)$ に対し，第 $v$ ビットを制御ビットとし，第 $w$ ビットを目標ビットとする一つの *CN* ゲートで構成される $n$ 入力一層の量子回路が実現する変換を $\mathcal{U}'$ とする．そして，この一層の量子回路の入力 $n$ 量子ビットの状態を $|F_{\mathcal{U}}(X)\rangle$ とし，このときの $S_1, \ldots, S_n$ を集合に対する排他的論理和において線形独立であるとすると，この一層の量子回路の出力の状態は $|F_{\mathcal{U}'\mathcal{U}}(X)\rangle$ となり，このとき $S_1, S_2, \ldots, S_{w-1}, S_w \oplus S_v, S_{w+1}, \ldots, S_n$ となる．これらは集合に対する排他的論理和において線形独

[2] ここで，補助ビットの入力時の状態が $|0\rangle$ と定義したが，入力時の状態を $|0\rangle$ または $|1\rangle$ と定義しても，同様に計算が行なえる．また，入力時の状態が既知でない補助ビットによる量子回路の効率化が可能であることも知られている [2]

立となる．ここで，$\oplus$ は集合に対する排他的論理和を表す．

次に，$CN$ ゲートで構成される任意の量子回路が実現する変換 $\mathcal{U}$ の逆変換 $\mathcal{U}^\dagger$ を実現する量子回路を考える．$CN$ ゲートが実現する変換 $\mathcal{U}_{CN}$ は自分自身の逆変換，すなわち，$\mathcal{U}_{CN}\mathcal{U}_{CN} = \mathcal{I}$ であることから，与えられた量子回路の入力側を左，出力側を右とすると，左右を反転させて得られた量子回路は変換 $\mathcal{U}^\dagger$ を実現する．よって，変換 $\mathcal{U}^\dagger$ は与えられた量子回路と同じ複雑さの $CN$ ゲートで構成される量子回路で実現できる．

そして，$CN$ ゲートで構成される量子回路の並列化で用いる変換を定義する．任意の正整数 $n$ と $m$ に対し，$\mathcal{CN}(n,m)$ を $(n+m)$ ビット変換の集合とし，$(n+m)$ ビット変換 $\mathcal{U}$ が次の条件を満たすとき，$\mathcal{U} \in \mathcal{CN}(n,m)$ とする．ある集合 $S_1, S_2, \ldots, S_m \subseteq \{1,2,\ldots,n\}$ が存在し，任意の $X = (x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ と $Y = (y_1, y_2, \ldots, y_m) \in \{0,1\}^m$ に対し，

$$\mathcal{U}|X,Y\rangle = |X, Y \oplus F_{\mathcal{U}}(X)\rangle$$

となる．

以下で，変換 $\mathcal{U} \in \mathcal{CN}(n,m)$ を実現する量子回路を示す．まず，補助ビットが使用できない場合について，以下の補題を示す．

**補題 3** 任意の正整数 $n$ と $m$ に対し，補助ビットを使用しないで $(n+m)$ ビット変換 $\mathcal{U} \in \mathcal{CN}(n,m)$ は深さ $\max\{n,m\}$ の $CN$ ゲートで構成される量子回路で実現できる．

**証明.** 入力 $n+m$ 量子ビットの状態を一般性を失うことなく $|X,Y\rangle$ とする．ただし，$X \in \{0,1\}^n$, $Y \in \{0,1\}^m$ である．また，$\mathcal{U}$ を $|X,Y\rangle$ に適用して得られる状態を

$$\mathcal{U}|X,Y\rangle = |X, Y \oplus F_{\mathcal{U}}(X)\rangle$$

とする．

並列に $\min\{n,m\}$ 個の $CN$ ゲートが配置することができるので，深さ $\max\{n,m\}$ で $nm$ 個の $CN$ ゲートが配置できる．ここで，各 $CN$ ゲートは可換であり，$\mathcal{U}_{CN}\mathcal{U}_{CN} = I$ となるので，$nm$ 個の異なる $CN$ ゲートが配置できる．この配置において，任意の $v$ $(1 \le v \le m)$ と $w$ $(1 \le w \le n)$ に対し，$w \in S_v$ となるときのみ，第 $w$ ビットを制御ビットとし，第 $n+v$ ビットを目標ビットとする $CN$ ゲートを配置する．すると，第 $n+v$ ビットに $\bigoplus_{j \in S_v} x_j$ が計算される． ■

次に，任意の正整数 $p$ に対し，$(p-1)n$ 補助ビットが使用できる場合について，以下の補題を示す．

**補題 4** 任意の正整数 $p$, $n$ と $m$ に対し，$(p-1)n$ 補助ビットを用いて $(n+pm)$ ビット変換 $\mathcal{U} \in \mathcal{CN}(n,pm)$ は深さ $\max\{n,m\} + 2\log p$ の $CN$ ゲートで構成される量子回路で実現できる．

**証明.** 入力 $n+pm$ 量子ビットの状態を一般性を失うことなく $|X, Y_1, Y_2, \ldots, Y_p\rangle$ とする．ただし，$X \in \{0,1\}^n$, $Y_1, Y_2, \ldots, Y_p \in \{0,1\}^m$ である．任意の $\mathcal{U} \in \mathcal{CN}(n,pm)$ に対して $\mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_p \in \mathcal{CN}(n,m)$ が存在し，

$$\begin{aligned}&\mathcal{U}|X, Y_1, Y_2, \ldots, Y_p\rangle \\ &= |X, Y_1 \oplus F_{\mathcal{V}_1}(X), Y_2 \oplus F_{\mathcal{V}_2}(X), \ldots, Y_p \oplus F_{\mathcal{V}_p}(X)\rangle\end{aligned}$$

を満たす．

まず，$(p-1)n$ 補助ビットを入力と見なし，

$$|X, 0^n, \ldots, 0^n, Y_1, Y_2, \ldots, Y_p\rangle$$

とし，$p-1$ 個 $|X\rangle$ のコピーを深さ $\log p$ で補助ビットに生成する．これは一量子ビットの状態 $\sum_{x \in \{0,1\}} |x\rangle$ に対し，$p-1$ 個 $|x\rangle$ のコピーを深さ $\log p$ で補助ビットに生成できるので，$|X\rangle$ の各量子ビットの状態を $p-1$ 個コピーすることで実現できる．すると，

$$|X, X, \ldots, X, Y_1, Y_2, \ldots, Y_p\rangle$$

となる．元の $|X\rangle$ と合せて $p$ 個の $|X\rangle$ がある．次に，並列に $|X\rangle$ の一つのコピーと $|Y_j\rangle$ $(1 \le j \le p)$ に対して $\mathcal{V}_j$ を適用して得られる状態は

$$|X, X, \ldots, X, Y_1 \oplus F_{\mathcal{V}_1}(X), Y_2 \oplus F_{\mathcal{V}_2}(X), \ldots, Y_p \oplus F_{\mathcal{V}_p}(X)\rangle$$

となる．ここで，各 $\mathcal{V}_j$ は補題 3 より深さ高々 $\max\{n,m\}$ で実現できる．$|X\rangle$ のコピーの逆変換を適用し，深さ $\log p$ で $(p-1)n$ 補助ビットを $|0\rangle$ に戻すと，

$$|X, 0^n, \ldots, 0^n, Y_1 \oplus F_{\mathcal{V}_1}(X), Y_2 \oplus F_{\mathcal{V}_2}(X), \ldots, Y_p \oplus F_{\mathcal{V}_p}(X)\rangle$$

となり，$\mathcal{U}$ を適用して得られる状態と同じになる．
■

また，任意の正整数 $q$ に対し，$(q-1)m$ 補助ビットが使用できる場合について，以下の補題を示す．

**補題 5** 任意の正整数 $q$, $n$ と $m$ に対し，$(q-1)m$ 補助ビットを用いて $(qn+m)$ ビット変換 $\mathcal{U} \in \mathcal{CN}(qn,m)$ は深さ $2\max\{n,m\} + 2\log q$ の $CN$ ゲートで構成される量子回路で実現できる．

**証明.** 入力 $qn+m$ 量子ビットの状態を一般性を失うことなく $|X_1, X_2, \ldots, X_q, Y\rangle$ とする．ただし，$X_1, X_2, \ldots, X_q \in \{0,1\}^n$, $Y \in \{0,1\}^m$ である．任意の $\mathcal{U} \in \mathcal{CN}(qn,m)$ に対して $\mathcal{W}_1, \mathcal{W}_2, \ldots, \mathcal{W}_q \in \mathcal{CN}(n,m)$ が存在し，

$$\begin{aligned}&F_{\mathcal{U}}(X_1, X_2, \ldots, X_q) \\ &= F_{\mathcal{W}_1}(X_1) \oplus F_{\mathcal{W}_2}(X_2) \oplus \cdots \oplus F_{\mathcal{W}_q}(X_q)\end{aligned}$$

を満たす．まず，$(q-1)m$ 補助ビットを入力と見なし，

$$|X_1, X_2, \ldots, X_q, Y, 0^m, \ldots, 0^m\rangle$$

とし，並列に各 $\mathcal{W}_k$ $(1 \le k \le q)$ を実現する．$|X_1\rangle$ と $|Y\rangle$ に対して $\mathcal{W}_1$ を適用し、$2 \le l \le q$ に対し，$|X_l\rangle$ と $m$ 個の補助ビットに $\mathcal{W}_l$ を適用する．すると，得られる状態は

$$|X_1, X_2, \ldots, X_q, Y \oplus F_{\mathcal{W}_1}(X_1), F_{\mathcal{W}_2}(X_2), \ldots, F_{\mathcal{W}_q}(X_q)\rangle$$

となる．ここで，各 $\mathcal{W}_k$ は補題 3 より深さ高々$\max\{n, m\}$ で実現できる．次に $|Y \oplus F_{\mathcal{W}_1}(X_1)\rangle$ に $|F_{\mathcal{W}_2}(X_2)\rangle, \ldots, |F_{\mathcal{W}_q}(X_q)\rangle$ を用いて $|Y \oplus F_{\mathcal{U}}(X_1, \ldots, X_q)\rangle$ を深さ $\log q$ で実現する．最後に使用した $(q-1)m$ 補助ビットを深さ高々 $\max\{n, m\} + \log q$ で $|0\rangle$ に戻すと，

$$|X_1, X_2, \ldots, X_q, Y \oplus F_{\mathcal{U}}(X_1, \ldots, X_q), 0^m, \ldots, 0^m\rangle$$

となり，$\mathcal{U}$ を適用して得られる状態と同じになる．■

上の三つの補題から，任意の正整数 $r$ に対し，$r$ 補助ビットが使用できる場合について，以下の補題を示す．

**補題 6** 任意の正整数 $r$，$n$ と $m$ に対し，$r$ 補助ビットを用いて $(n+m)$ ビット変換 $\mathcal{U} \in \mathcal{CN}(n, m)$ は深さ $O(nm/(r+1) + \log(r+1))$ の $CN$ ゲートで構成される量子回路で実現できる．

**証明.** $p = \lfloor r/2n \rfloor$，$q = \lfloor r/2m \rfloor$ とし，$n = (q+1)n'$，$m = (p+1)m'$ とすると，補題 4 より，$pn$ 補助ビットを用いて $\mathcal{U}$ は深さ高々 $\max\{n, m'\} + 2\log(p+1)$ で実現できる．補題 4 で用いる $p+1$ 個の $\mathcal{V}_j \in \mathcal{CN}(n, m')$ $(1 \le j \le p+1)$ に対し，補題 5 より，各 $\mathcal{V}_j$ は $qm'$ 補助ビットを用いて深さ高々$2\max\{n', m'\} + 2\log(q+1)$ で実現できる．よって，$pn + qm$ 補助ビットを用いて $\mathcal{U}$ は深さ高々 $2\max\{n', m'\} + 2\log(p+1) + 2\log(q+1) = O(nm/(r+1) + \log(r+1))$ で実現できる．■

そして，$CN$ ゲートで構成される任意の量子回路に対し，補助ビットが使用できない場合について，以下の補題を示す．

**補題 7** $CN$ ゲートで構成され，$n$ ビット変換 $\mathcal{U}$ を実現する $n$ 入力量子回路が与えられたとき，補助ビットを使用しないで変換 $\mathcal{U}$ は深さ高々 $3n+3$ の $CN$ ゲートで構成される量子回路で実現できる．

**証明.** $\mathcal{U}$ の逆変換を実現する量子回路を構成するを考える．入力 $n$ 量子ビットの状態を一般性を失うことなく $|X\rangle$ $(X \in \{0,1\}^n)$ とし，集合に対する排他的論理和において線形独立となる集合 $S_1, S_2, \ldots, S_n \subseteq \{1, 2, \ldots, n\}$ が存在し，

$$\mathcal{U}|X\rangle = |F_{\mathcal{U}}(X)\rangle$$

となるとする．また，$n$ ビット変換 $\mathcal{U}'$ を

$$\mathcal{U}'\mathcal{U}|X\rangle = |X'\rangle$$

となる変換とする．ここで，ベクトル $X'$ はベクトル $X$ の成分を置換したベクトルである．$\mathcal{U}'$ を実現する $CN$ ゲートで構成される量子回路を示す．まず，ある $v$ と $w$ $(1 \le v, w \le n)$ に対し，各 $v'$ $(1 \le v' \le n, v' \ne v)$ において $w \in S_v$ かつ $w \in S_{v'}$ となるときは $S_{v'}$ を $S_v$ との集合に対する排他的論理和にする．すなわち，第 $v$ ビットを制御ビットとし，第 $v'$ ビットを目標ビットとする $CN$ ゲートを配置する．すると，$v$ に対してのみ $w \in S_v$ となり，以降，$S_v$ を各 $S_{v'}$ との集合に対する排他的論理和にしたとしても，必ず $w \in S_v$ となる．ここで，$S_1, \ldots, S_n$ は常に集合に対する排他的論理和において線形独立であることから，$S_1, \ldots, S_n$ の要素数は常に一以上である．この操作をすべての $S_1, \ldots, S_n$ に対して実行すると，$S_1, \ldots, S_n$ の要素数は一となる．つまり，$F_{\mathcal{U}'\mathcal{U}}(X) = X'$ となる．ここで，任意の $S_v$ の操作において，最悪の場合，$n-1$ 回集合に対する排他的論理和を実行する．すなわち，$n-1$ 個の $CN$ ゲートを配置する．このとき，二回集合に対する排他的論理和を実行すると，次の操作を開始することができる．よって，各 $S_1, \ldots, S_n$ の操作で高々 $n-1$ 個の $CN$ ゲートが配置され，各操作で最初に配置される $CN$ ゲートと次の操作で最初に配置される $CN$ ゲートは深さが 2 ずれるので，$\mathcal{U}'$ は深さ高々 $3n-3$ で実現できる．

そして，量子ビットの任意の置換は補助ビットを使用しないで深さ高々 6 の $CN$ ゲートで構成される量子回路で実現できることが示されている [6]．これを用いて $|X'\rangle$ を置換すると $|X\rangle$ となる．よって，$\mathcal{U}$ の逆変換は補助ビットを使用しないで深さ高々 $3n+3$ の $CN$ ゲートで構成される量子回路で実現できる．■

最後に，$CN$ ゲートで構成される量子回路の並列化に関する結果を示す．任意の正整数 $r$ に対し，$r$ 補助ビットが使用できる場合について，以下の定理を示す．

**定理 8** $CN$ ゲートで構成され，$n$ ビット変換 $\mathcal{U}$ を実現する $n$ 入力量子回路が与えられたとき，任意の正整数 $r$ に対し，$r$ 補助ビット数を用いて変換 $\mathcal{U}$ は $r < n$ のとき深さ $O(n)$，$r \ge n$ のとき深さ $O(n^2/r + \log r)$ の $CN$ ゲートで構成される量子回路で実現できる．

**証明.** 与えられた量子回路の入力 $n$ 量子ビットの状態を一般性を失うことなく $|X\rangle$ $(X \in \{0,1\}^n)$ とする．また，集合に対する排他的論理和において線形独立となる集合 $S_1, S_2, \ldots, S_n \subseteq \{1, 2, \ldots, n\}$ が存在し，

$$\mathcal{U}|X\rangle = |F_{\mathcal{U}}(X)\rangle$$

とする．$r < n$ のとき，補題 7 より補助ビットを使用しないで深さ $O(n)$ で実現できる．

$r \ge n$ のとき，変換 $\mathcal{V}, \mathcal{V}' \in \mathcal{CN}(n, n)$ を

$$\mathcal{V}|X, Y\rangle \quad = \quad |X, Y \oplus F_{\mathcal{U}}(X)\rangle$$

$$\mathcal{V}'|F_{\mathcal{U}}(X),Y\rangle \quad = \quad |F_{\mathcal{U}}(X),Y\oplus X\rangle$$

となるとする．ただし，$Y = (y_1, y_2, \ldots, y_n) \in \{0,1\}^n$ である．まず，$n$ 補助ビットを入力と見なし，$|X, 0^n\rangle$ とし，$\mathcal{V}$ を適用して得られる状態は $|X, F_{\mathcal{U}}(X)\rangle$ となる．次に，$|X\rangle$ と $|F_{\mathcal{U}}(X)\rangle$ を深さ 3 で置換する．これは二量子ビットの状態の置換が三つの $CN$ ゲートで実現できるので，$|X\rangle$ と $|F_{\mathcal{U}}(X)\rangle$ の各量子ビット毎の状態の置換で実現できる．すると，$|F_{\mathcal{U}}(X), X\rangle$ となる．そして，$\mathcal{V}'$ を適用して得られる状態は

$$|F_{\mathcal{U}}(X), X\oplus X\rangle = |F_{\mathcal{U}}(X), 0^n\rangle$$

となり，$\mathcal{U}$ を $|X\rangle$ へ適用して得られる状態と同じになる．残りの補助ビットを $\mathcal{V}$ と $\mathcal{V}'$ の並列化のために使用すると，$\mathcal{V}$ と $\mathcal{V}'$ は補題 6 より $r-n$ 補助ビットを用いて深さ $O(n^2/(r-n+1)+\log(r-n+1))$ で実現できる．よって，$\mathcal{U}$ は深さ $O(n^2/r+\log r)$ で実現できる． ■

定理 8 より，以下の系が成り立つ．

**系 9** $CN$ ゲートで構成され，$n$ ビット変換 $\mathcal{U}$ を実現する $n$ 入力量子回路が与えられたとき，$O(n^2/\log n)$ 補助ビットを用いて変換 $\mathcal{U}$ は深さ $O(\log n)$ の $CN$ ゲートで構成される量子回路で実現できる．

## 4 $PS$ ゲートと $CN$ ゲートで構成される量子回路

この節では，$PS$ ゲートと $CN$ ゲートで構成される量子回路の並列化に関する結果を示す．

まず，任意の正整数 $t$ と $s$ に対し，$t$ 個の $s$ ビット $PS$ ゲート $G_1, G_2, \ldots, G_t$ と $CN$ ゲートで構成される $n$ 入力量子回路が実現する変換について考える．与えられた量子回路を各 $PS$ ゲートの前と後へ分割することで与えられた量子回路が実現する $n$ ビット変換は

$$\mathcal{C}_t\mathcal{P}_t\mathcal{C}_{t-1}\cdots\mathcal{P}_1\mathcal{C}_0$$

と表現できる．ただし，$\mathcal{C}_v$ $(0 \le v \le t)$ は $CN$ ゲートで構成される量子回路が実現する $n$ ビット変換であり，$\mathcal{P}_w$ $(1 \le w \le t)$ は $PS$ ゲート $G_w$ で構成される一層の量子回路が実現する $n$ ビット $PS$ 変換である．さらに，

$$\mathcal{C}_t\cdots\mathcal{C}_0\mathcal{D}_t\cdots\mathcal{D}_1$$

と変形できる．ここで，$\mathcal{D}_w = (\mathcal{C}_w\cdots\mathcal{C}_0)^\dagger\mathcal{P}_w(\mathcal{C}_w\cdots\mathcal{C}_0)$ である．この $n$ ビット変換 $\mathcal{D}_t\cdots\mathcal{D}_1$ について，以下の補題を示す．

**補題 10** $t$ 個の $n$ ビット $PS$ 変換 $\mathcal{D}_1,\ldots,\mathcal{D}_t$ が与えられたとき，ただし，$\mathcal{D}_w = (\mathcal{C}_w\cdots\mathcal{C}_0)^\dagger\mathcal{P}_w(\mathcal{C}_w\cdots\mathcal{C}_0)$ $(1 \le w \le t)$ である．$st$ 補助ビットを用いて変換 $\mathcal{D}_t\cdots\mathcal{D}_1$ は $t$ 個の $s$ ビット $PS$ ゲート $G_1, G_2, ..., G_t$ と $CN$ ゲートで構成される深さ $O(\log t)$ の量子回路で実現できる．

**証明．** 入力 $n$ 量子ビットの状態を $|\psi\rangle = \sum_{X\in\{0,1\}^n}\alpha_X|X\rangle$ とし，各 $G_w$ の入力 $s$ 量子ビットの状態を $\sum_{X\in\{0,1\}^s}\alpha_X|X\rangle$ としたとき，$G_w$ の出力の状態が

$$\sum_{X\in\{0,1\}^s}\alpha_X e^{i\delta_X}|X\rangle$$

となるとする．また，各 $\mathcal{D}_w$ の $\mathcal{C}_w\cdots\mathcal{C}_0$ を $|\psi\rangle$ へ適用して得られる状態を一般性を失うことなく

$$\sum_{X\in\{0,1\}^n}\alpha_X|Z_w(X), Z'_w(X)\rangle$$

とする．ここで，$|Z_w(X)\rangle$ $(Z_w(X) \in \{0,1\}^s)$ は $G_w$ の入力 $s$ 量子ビットの状態であり，$Z'_w(X) \in \{0,1\}^{n-s}$ である．すると，$\mathcal{P}_w$ を適用して得られる状態は

$$\sum_{X\in\{0,1\}^n}\alpha_X e^{i\delta_{Z_w(X)}}|Z_w(X), Z'_w(X)\rangle$$

となり，$(\mathcal{C}_w\cdots\mathcal{C}_1)^\dagger$ を適用して得られる状態は

$$\sum_{X\in\{0,1\}^n}\alpha_X e^{i\delta_{Z_w(X)}}|X\rangle$$

となる．そして，任意の $X\in\{0,1\}^n, Y_w\in\{0,1\}^s$ に対し，$\mathcal{U}\in\mathcal{CN}(n,st)$ を

$$\begin{aligned}&\mathcal{U}|X, Y_1, \ldots, Y_t\rangle\\ &= |X, Y_1\oplus Z_1(X), Y_2\oplus Z_2(X), \ldots, Y_t\oplus Z_t(X)\rangle\end{aligned}$$

となる変換とする．

まず，$st$ 補助ビットを入力と見なし，

$$\sum_{X\in\{0,1\}^n}\alpha_X|X, 0^s, \ldots, 0^s\rangle$$

とし，$\mathcal{U}$ を適用して得られる状態は

$$\sum_{X\in\{0,1\}^n}\alpha_X|X, Z_1(X), \ldots, Z_t(X)\rangle$$

となる．次に，各 $|Z_w(X)\rangle$ を $G_w$ へ入力し，その出力の状態に $\mathcal{U}^\dagger$ を適用して使用した補助ビットを $|0\rangle$ に戻すと，得られる状態は

$$\sum_{X\in\{0,1\}^n}\alpha_X e^{i(\delta_{Z_1(X)}+\cdots+\delta_{Z_t(X)})}|X, 0^s, \ldots, 0^s\rangle$$

となり，$\mathcal{D}_t\cdots\mathcal{D}_1$ を $|\psi\rangle$ に適用して得られる状態と同じになる． ■

そして，$PS$ ゲートと $CN$ ゲートで構成される量子回路について以下の定理を示す．

**定理 11** $t$ 個の $s$ ビット $PS$ ゲート $G_1, G_2, \ldots, G_t$ と $CN$ ゲートで構成され，$n$ ビット変換 $\mathcal{U}$ を実現する $n$ 入力量子回路が与えられとき，任意の正整数 $r$ に対し，$r$ 補助ビットを用いて変換 $\mathcal{U}$ は $r < n$ のとき深さ $O(tn)$，$r \geq n$ のとき 深さ $O((stn + n^2)/r + (st \log r)/k + \log r)$ の $t$ 個の $s$ ビット $PS$ ゲート $G_1, G_2, \ldots, G_t$ と $CN$ ゲートで構成される量子回路で実現できる．

**証明.** 上で述べたように，$\mathcal{U}$ は

$$\mathcal{U} = \mathcal{C}_t \mathcal{P}_t \mathcal{C}_{t-1} \cdots \mathcal{P}_1 \mathcal{C}_0$$

と表現できる．

$r < n$ のとき，各 $\mathcal{C}_v$ $(0 \leq v \leq t)$ の深さが $O(n)$ より大きい場合，補題 7 より，$\mathcal{C}_v$ は補助ビットを使用しないで深さ $O(n)$ で実現できる．よって，$r$ 補助ビットを用いて深さ $O(tn)$ で実現できる．

さらに，$\mathcal{U}$ は

$$\mathcal{U} = \mathcal{C}_t \cdots \mathcal{C}_0 \mathcal{D}_t \cdots \mathcal{D}_1$$

と変形できる．$r \geq n$ のとき，$\mathcal{D}_t \cdots \mathcal{D}_1$ について，$k = \lceil r/2 \rceil$ とすると，補題 10 より $k$ 補助ビットを用いて $\lfloor k/s \rfloor$ 個の $\mathcal{D}_w$ が並列化できる．よって，この操作を逐次的に $\lceil st/k \rceil$ 回繰り返すことで $\mathcal{D}_t \cdots \mathcal{D}_1$ を実現できる．ここで，残りの $r - k$ 補助ビットを補題 10 で用いる $\mathcal{CN}(n, k)$ の並列化に使用すると，補題 6 より深さ $O(kn/(r - k + 1) + \log(r - k + 1))$ で実現できるので，$\mathcal{D}_t \cdots \mathcal{D}_1$ は深さ $O(stn/r + (st \log r)/r)$ で実現できる．また，$\mathcal{C}_t \cdots \mathcal{C}_0$ について，定理 8 より深さ $O(n^2/r + \log r)$ で実現できる．以上より，$\mathcal{U}$ は $r$ 補助ビットを用いて深さ $O((stn + n^2)/r + (st \log r)/r + \log r)$ で実現できる． ■

ここで，定理 11 で構成される量子回路に含まれている $PS$ ゲートは与えられた量子回路に含まれている $t$ 個の $s$ ビット $PS$ ゲート $G_1, \ldots, G_t$ のみである．また，定理 11 より，以下の系が成り立つ．

**系 12** $t$ 個の $s$ ビット $PS$ ゲート $G_1, G_2, \ldots, G_t$ と $CN$ ゲートで構成され，$n$ ビット変換 $\mathcal{U}$ を実現する $n$ 入力量子回路が与えられとき，$O((stn + n^2)/\log n)$ 補助ビットを用いて変換 $\mathcal{U}$ は深さ $O(\log n + \log t)$ の $t$ 個の $s$ ビット $PS$ ゲート $G_1, G_2, \ldots, G_t$ と $CN$ ゲートで構成される量子回路で実現できる．

## 5 おわりに

本論文では，$CN$ ゲートで構成される $n$ 入力量子回路と $t$ 個の $s$ ビット $PS$ ゲート $G_1, G_2, \ldots, G_t$ と $CN$ ゲートで構成される $n$ 入力量子回路について，使用できる補助ビットの数が任意に固定された場合の並列化手法を示した．また，その特殊な場合として，使用する補助ビットの数が従来研究 [6] の $1/\log n$ 倍にしても，従来研究 [6] と同じ深さに並列化できることも示した．また，Walsh-Hadamard ゲートと $CN$ ゲートで構成される量子回路について，補助ビットを用いた並列化手法が知られている [1]．

また，Barenco ら [2] は任意のユニタリ変換がすべての一ビット量子ゲートと $CN$ ゲートで構成される量子回路で実現できることを示した．本論文で扱っている $CN$ ゲートと $PS$ ゲートにあと Walsh-Hadamard ゲートを一般化した一ビット量子ゲートを加えると任意のユニタリ変換を実現する量子回路が構成できる．今後の課題として，この種類の量子回路について並列化手法を示すことがある．

## References


[1] 安倍 秀明, 宋 少秋, "制約付き量子回路における補助ビットを用いた並列化について", 数理解析研究所共同研究集会「代数系, 形式言語および計算理論」, 2000 年 3 月.

[2] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, "Elementary gates for quantum computation", Phys. Rev **A** (52), pp.3457-3467, 1995.

[3] E. Bernstein and U.V. Vazirani, "Quantum complexity theory", SIAM J. Comput., vol. **26**, no. 5, pp.1411–1473, 1997.

[4] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer", Proc. Roy. Soc. London Ser. A **400**, pp.96–117, 1985.

[5] D. Deutsch, "Quantum computational networks", Proc. Roy. Soc. London Ser. A **425**, pp.73–90, 1989.

[6] C. Moore and M. Nilsson, "Parallel quantum computation and quantum codes", manuscript, 1998 (available at lanl e-print quant-ph/9808027).

[7] A. Yao, "Quantum circuit complexity", in Proc. 34th Annual IEEE Symp. on Foundations of Computer Science, pp.352–361, 1993.