修 士 論 文

補助ビットを用いた量子回路の並列化手法について

指導教官　平石邦彦 助教授

北陸先端科学技術大学院大学

情報科学研究科情報システム学専攻

安倍秀明

2000 年 2 月 15 日

目 次

図 目 次

第 1 章

はじめに

現在の計算機の計算能力に関する「現在の計算機は任意の物理現象を効率的に模倣できるか？」という疑問に対し，Feynman [14] は現在の計算機では効率的に模倣できない物理現象が存在することを示唆した．そのため，任意の物理現象を効率的に模倣できる計算機として量子力学を計算原理に組込んだ計算機，すなわち，量子計算機，が要求される．この要求に対し，Deutsch [9] は二つの量子計算機のモデル，量子チューリング機械と量子回路を提案した．

量子チューリング機械は従来のチューリング機械に量子力学を計算原理に組込んで拡張したモデルであり，量子チューリング機械において計算可能な問題のクラスは従来のチューリング機械おける計算可能な問題のクラスと同じであることが知られている [9]．また，Bernstein と Vazirani [4] によって量子チューリング機械のより数学的な形式化が行われた．その後，量子チューリング機械は従来の決定性チューリング機械や確率的チューリング機械より計算能力が高いことが示された．まず，Deutsch と Jozsa [12] によって量子チューリング機械で決定性チューリング機械よりも指数倍高速に解ける問題が示された．しかし，この問題は確率的チューリング機械でも同様に決定性チューリング機械よりも指数倍高速に解ける問題であった．そして，Simon [23] は，量子チューリング機械では多項式時間で解けるが，確率的チューリング機械では多項式時間で解けない問題を示した．さらに，Shor [22] は Simon の量子アルゴリズムを拡張し，量子チュー

リング機械で素因数分解問題と離散対数問題が多項式時間で解けることを示した．この二つの問題は現在の計算機では多項式時間で解けないと予想されている．この二つの問題の困難さが公開鍵暗号系の安全性の保証となっている．また，Shor の結果に対して様々な拡張が行われた [3, 8, 19, 25]．一方，Grover [15] は N 個の要素で構成される未整列データベースにおける検索問題に対し，現在の計算機では与えられた条件を満たす一つの要素を確率 1/2 以上で取り出すためにデータベースへのアクセスを $\Omega(N)$ 回必要とするが，量子チューリング機械ではデータベースへのアクセスを $O(\sqrt{N})$ 回で十分であることを示した．その後，データベース内の最大値，最小値，中間値をもつ要素や条件満たす要素の数を求まる問題など Grover の結果について様々の拡張および応用が考えられた [5, 6, 7]．さらに，Grover は，一般の量子アルゴリズムの高速化手法や高速な Sampling を量子計算機で実現する手法も示した [16, 17].

量子計算機のもう一つのモデルである量子回路に対して，Yao [24] は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を示した．一方，従来の論理回路において NAND ゲートが universal であるように，量子回路において universal である量子ゲートのクラスに関する多くの結果 [1, 2, 10, 11, 13, 18] が示され，その中で代表的な結果は Barenco ら [2] によるものである．Barenco らは，Controlled-Not と呼ばれる二入力の量子ゲートと一入力の量子ゲート全体からなる量子ゲートのクラスが universal であることを示した.

本研究では，いくつかの量子ゲートのクラスで構成される量子回路に対して，その並列化を補助ビットを用いて行う手法について考える．ただし，universal な量子ゲートのクラスで構成される量子回路を扱うのは依然困難のため，本研究では制約付きの量子ゲートのクラスで構成される量子回路について扱っている．なお，本研究で扱う量子ゲートのクラスと Barenco ら [2] による universal な量子ゲートのクラスの違いに関する考察は第 2 章で行う．直感的に，補助ビットとは量子回路において付加的な入力ビットであり，量子回路の出力は補助ビットの状態に依存しない．また，補助ビットを使用する効果として，補助ビットに情報を格納できることがある．そして，より本質的な効果と

して，補助ビットを用いることでより多くの量子ゲートを並列に配置することができることがある．

具体的に，本研究では以下の三種類の量子回路について考える．それは，Controlled-Not ゲートで構成される量子回路，Controlled-Not ゲートと Phase-Shift ゲートで構成される量子回路，及び， Controlled-Not ゲートと Walsh-Hadamard ゲートで構成される量子回路である．従来研究として，Moore と Nilsson [21] はこの三種類の内ある量子回路が与えられたとき，補助ビットを用いることで，その量子回路と同じ計算を行う量子回路が同じ量子ゲートのクラスを用いて対数深さで構成できることを示した．本研究では，Moore と Nilsson の結果の改良を行った．三種類の量子回路それぞれに対する本研究の並列化手法で用いる補助ビットの数は Moore と Nilsson の結果で用いる補助ビットの数の $1/\log n$ 倍である．ただし，n は並列化の対象である量子回路の入力数である．さらに，より一般な結果として，使用できる補助ビットの数が固定した場合，三種類の量子回路それぞれについての並列化手法を示す．

本論文の構成は以下の通るである．第 2 章では，量子回路に関する諸定義と扱う量子回路に関する考察を行う．第 3 章，第 4 章，と第 5 章では，Controlled-Not ゲートで構成される量子回路，Controlled-Not ゲートと Phase-Shift ゲートで構成される量子回路，及び， Controlled-Not ゲートと Walsh-Hadamard ゲートで構成される量子回路，それぞれの並列化に関する結果を示す．最後に，第 6 章では，本研究のまとめと今後の課題について述べる．

第 2 章

諸定義と従来研究

2.1 量子ビット

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し，すなわち，一量子ビットの任意の状態 $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ は二次元の複素列ベクトルであり，

$$|\alpha_0|^2 + |\alpha_1|^2 = 1$$

を満たす．言い換えれば，一量子ビットの任意の状態は複素単位ベクトルである．二次元複素ベクトル空間の基底となる

$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

に対し，一量子ビットの状態が $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ のときはその量子ビットは値 0 を表すと解釈し，一量子ビットの状態が $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ のときはその量子ビットは値 1 を表すと解釈する．ここで，量子力学で用いられるケットベクトル表現 $|\cdot\rangle$ を用いて量子ビットの状態を表現する．

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

とする．すると，任意の $x \in \{0,1\}$ に対し，一量子ビットの状態が $|x\rangle$ のときはその量子ビットが値 x を表すと解釈する．また，一量子ビットの状態 $|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ は基底 $\{|0\rangle, |1\rangle\}$ の線形重合わせ

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \alpha_0|0\rangle + \alpha_1|1\rangle$$

と表すことができる．

また，任意の正整数 k に対し，k 量子ビットの状態は 2^k 次元の複素単位ベクトルである．すなわち，k 量子ビットの任意の状態

$$|\psi\rangle = \begin{pmatrix} \alpha_{0^k} \\ \alpha_{0^{k-1}1} \\ \vdots \\ \alpha_{1^k} \end{pmatrix} \tag{2.1}$$

は 2^k 次元の複素列ベクトルであり，$\sum_{X\in\{0,1\}^k} |\alpha_X|^2 = 1$ を満たす[1]．任意の $X = (x_1, x_2, \ldots, x_k) \in \{0,1\}^k$ に対し，$|X\rangle$ は $|x_1\rangle, |x_2\rangle, \ldots, |x_k\rangle$ のテンソル積

$$\begin{aligned} |X\rangle &= |x_1, x_2, \ldots, x_k\rangle \\ &= |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_k\rangle \end{aligned}$$

とする．ただし，$n_1 \times m_1$ 行列 $A = [a_{ij}]$ と $n_2 \times m_2$ 行列 $B = [b_{ij}]$ のテンソル積 $A \otimes B$ は $n_1 n_2 \times m_1 m_2$ 行列となり，以下のように定義される．

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n_1}B \\ a_{21}B & a_{22}B & \cdots & a_{2n_1}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m_1 1}B & a_{m_1 2}B & \cdots & a_{m_1 n_1}B \end{pmatrix}$$

すると，上で定義した $|X\rangle$ の集合 $\{|X\rangle \mid X \in \{0,1\}^k\}$ は 2^k 次元複素ベクトル空間の基底となり，任意の $X \in \{0,1\}^k$ に対し，k 量子ビットの状態が $|X\rangle$ のときはその k 量子

[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 $X = x_1 x_2 \cdots x_k$，とするの二つの表記法を用いている．

ビットは値 X を表すと解釈する．また，式 (2.1) の状態 $|\psi\rangle$ は基底 $\{|X\rangle \mid X \in \{0,1\}^k\}$ の線形重合わせ

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

と表すことができる．ここで，状態 $|\psi\rangle$ において，α_X は $|X\rangle$ の**振幅** (Amplitude) と呼ばれ，$\alpha_X = |\alpha_X| e^{i\beta_X}$ となる β_X は $|X\rangle$ の**位相** (Phase) と呼ばれる．本論文では，k 量子ビットの状態を表す線形重合わせの基底として $\{|X\rangle \mid X \in \{0,1\}^k\}$ のみを用いるため，以降 k 量子ビットの状態を表す**線形重合わせ**はその状態を表す基底 $\{|X\rangle \mid X \in \{0,1\}^k\}$ の線形重合わせを指す．

また，量子計算機では計算結果を取り出すときに定められた基底に関して**観測**を行う．状態 $|\psi\rangle$ に対して基底 $\{|X\rangle \mid X \in \{0,1\}^k\}$ に関する観測を行った場合，$|X\rangle$ を得る確率は $|\alpha_X|^2$ となる．ただし，量子回路の並列化を行う上では観測は行わないため，本論文では以降観測について言及することはない．

2.2 ユニタリ変換

量子ビットの状態に関する量子力学の制約，

- 量子ビットの状態が複素単位ベクトルであり，かつ，
- 量子ビットの状態推移は可逆である，

によって，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 [4]．**ユニタリ変換**とは，線形変換でありユニタリ行列で定義される．行列 U がユニタリであるとは，$U^\dagger$ を U の共役転置行列とし，I を単位行列とすると，

$$UU^\dagger = U^\dagger U = I$$

を満たす．ここで，$(U^\dagger)^\dagger = U$ であることから，行列 $U^\dagger$ ，すなわち U の逆行列，もまたユニタリとなる．すなわち，任意のユニタリ変換に対し，その逆変換もまたユニタリ変換となる．これは，量子ビットの状態推移が可逆であることに対応する．また，複素単位列ベクトルにユニタリ変換を適用すると，その結果もまた複素単位列ベクトルとなる．以降，ユニタリ変換をその変換を定義するユニタリ行列で表す．

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変換を k **ビット変換**と呼ぶ．すなわち，任意の k ビット変換は k 量子ビットのある状態推移を表す．以下では，本論文で用いる変換の定義を行う．まず，一ビット変換

$$U_{WH} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.2}$$

は **Walsh-Hadamard 変換**と呼ばれ，任意の一量子ビットの状態

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

に対し，

$$\begin{aligned} U_{WH}|\psi\rangle &= U_{WH}(\alpha_0|0\rangle + \alpha_1|1\rangle) \\ &= \alpha_0 U_{WH}|0\rangle + \alpha_1 U_{WH}|1\rangle \\ &= \frac{\alpha_0}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{\alpha_1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{2}}(\alpha_0 + \alpha_1)|0\rangle + \frac{1}{\sqrt{2}}(\alpha_0 - \alpha_1)|1\rangle \end{aligned}$$

となる．k 量子ビットの状態 $|0^k\rangle$ に対し，各の量子ビットに Walsh-Hadamard 変換 U_{WH} を適用すると，

$$\begin{aligned} \overbrace{U_{WH} \otimes U_{WH} \otimes \cdots \otimes U_{WH}}^{k \text{ 個}} |0^k\rangle &= U_{WH}|0\rangle \otimes \cdots \otimes U_{WH}|0\rangle \\ &= \left(\frac{|0\rangle}{\sqrt{2}} + \frac{|1\rangle}{\sqrt{2}}\right) \otimes \cdots \otimes \left(\frac{|0\rangle}{\sqrt{2}} + \frac{|1\rangle}{\sqrt{2}}\right) \\ &= \sum_{X \in \{0,1\}^k} \frac{1}{2^{k/2}} |X\rangle \end{aligned}$$

すべての $X \in \{0,1\}^k$ に対して $|X\rangle$ が同じ振幅をもつ線形重合わせで表される状態が得られる．そのため，Walsh-Hadamard 変換は最も用いられる変換の一つである．

次に，二ビット変換

$$U_{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.3}$$

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，

$$\begin{aligned} U_{CN}|\psi\rangle &= U_{CN} \sum_{(x_1,x_2)\in\{0,1\}^2} \alpha_{(x_1,x_2)}|x_1, x_2\rangle \\ &= \sum_{(x_1,x_2)\in\{0,1\}^2} \alpha_{(x_1,x_2)} U_{CN}|x_1, x_2\rangle \\ &= \sum_{(x_1,x_2)\in\{0,1\}^2} \alpha_{(x_1,x_2)}|x_1, x_1 \oplus x_2\rangle \end{aligned}$$

となる．ここで，$U_{CN}|\psi\rangle$ を表す線形重合わせ

$$U_{CN}|\psi\rangle = \sum_{(x_1,x_2)\in\{0,1\}^2} \alpha_{(x_1,x_2)}|x_1, x_1 \oplus x_2\rangle \tag{2.4}$$

において，第一ビット x_1 が 1 であるときのみ第二ビット $x_1 \oplus x_2$ が $\neg x_2$ となるため，第一ビットは**制御ビット** (control bit)，第二ビットは**目標ビット** (target bit) と呼ばれる．これはまた，この変換が Controlled-Not と呼ばれる理由でもある．

最後に，任意の正整数 k に対し，ある k ビット変換 U が **Phase-Shift 変換** (以下では，略して PS 変換) であるとは，長さ 2^k のある実数の系列 $\Gamma = (\gamma_{0^k}, \gamma_{0^{k-1}1}, \ldots, \gamma_{1^k})$ が存在し，U が Γ によって以下のように定義されるときである．

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

以下では，実数の系列をギリシャ文字の大文字で表し，上のように実数の系列 Γ によって定義される PS 変換を U_Γ と表す．すると，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，

$$\begin{aligned} U_\Gamma|\psi\rangle &= U_\Gamma \sum_{X\in\{0,1\}^k} \alpha_X |X\rangle \\ &= \sum_{X\in\{0,1\}^k} \alpha_X U_\Gamma |X\rangle \\ &= \sum_{X\in\{0,1\}^k} \alpha_X e^{i\gamma_X} |X\rangle \end{aligned}$$

となる．すなわち，PS 変換 $U_\Gamma|\psi\rangle$ は $|\psi\rangle$ を表す線形重合わせ中の $|X\rangle$ の位相 (Phase) を γ_X 分変化 (Shift) させたことになる．

2.3 量子回路

量子回路の定義を行う前に，量子回路を構成する素子である量子ゲートと量子回路の効率化，本研究では並列化，を行う際に使用する補助ビットについて定義を行う．

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，入力の k 量子ビットの状態に対してある k ビット変換による状態推移を行った状態を出力の k 量子ビットの状態とする．ある k ビット量子ゲートがある k ビット変換 U を**実現**するとは，任意の k 量子ビットの状態 $|\psi\rangle$ に対し，入力の k 量子ビットの状態を $|\psi\rangle$ としたとき，出力の k 量子ビットの状態は $|\psi\rangle$ に U を適用した状態 $U|\psi\rangle$ となる．

以下では，本研究で使用する量子ゲートを定義する．まず，WH **ゲート** とは，一ビット量子ゲートであり，一ビット変換 U_{WH} を実現する (式 (2.2) を参照)．次に，CN **ゲート** とは，二ビット量子ゲートであり，二ビット変換 U_{CN} を実現する (式 (2.3) を参照)．CN ゲートを図示するときは（図 2.1 参照），制御ビットと目標ビットにはそれぞれ $\bullet$ と $\oplus$ を描き，それらを直線で結ぶ．最後に，k **ビット PS ゲート**とは，k ビット量子

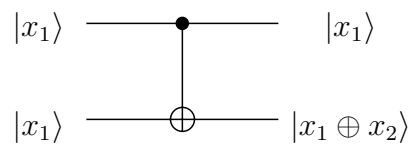

図 2.1: CN ゲート

ゲートであり，ある k ビット PS 変換を実現する．

次に，**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．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].

任意の整数 $n \geq 1$ に対し，n **入力一層の回路**とは n 量子ビットの入力と n 量子ビットの出力をもち，入力を共有しない量子ゲートによって構成される．ここで，量子ゲートの入力になっていない各量子ビットには一ビット変換 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ことができ，この一層の回路が実現する n ビット変換は各量子ゲートが実現するユニタリ変換のテンソル積となる．そして，n **入力量子回路**とは，n 入力の一層の回路の系列であり，**実現**するユニタリ変換はそれぞれの一層の回路が実現する n ビット変換の積となる．

一般に，量子回路の複雑さの尺度としてゲート数，深さ（層の数）と補助ビット数が考えられる．本研究では，量子回路の複雑さの尺度として**深さ**と**補助ビット数**についてのみを考える．ゲート数については，量子回路の深さと補助ビットを含む量子回路の量子ビット数の積で押さえられる．本研究の目的である補助ビットを用いた量子回路の並列化とは，ある量子回路が与えられ，その量子回路は変換 U を実現するとすると，補助ビットを用いて $U \otimes I$ を実現する深さの小さい量子回路を構成することである．使用する補助ビットの数が m のとき，I は $2^m \times 2^m$ の単位行列である．

2.4 Non-Cloning Theorem

量子回路固有の制約として，量子ビットの任意の状態のコピーを他の量子ビットへコピーをすることができないことである．すなわち，論理回路における fan-out，ある一つのビットを二つ以上のゲートの入力とすること，ができないことになる．量子力学では，この制約を説明する定理を Non-Cloning Theorem と呼ぶ．量子回路における fan-out に関する考察は Moore [20] によって行われた．

Non-Cloning Theorem について簡単に説明する．$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ を一量子ビットの任意の状態とする．状態 $|\psi\rangle \otimes |0\rangle$ が与えられたとき，第一ビットの状態 $|\psi\rangle$ を第二ビットにコピーすることを考える．すると，状態は $|\psi\rangle \otimes |0\rangle$ から

$$|\psi\rangle \otimes |\psi\rangle = \alpha_0^2|00\rangle + \alpha_0\alpha_1(|01\rangle + |10\rangle) + \alpha_1^2|11\rangle$$

に推移する．しかし，一般にこの状態推移を表す変換は線形ではない，すなわち，ユニタリ変換ではない．よって，一般にこの変換は実現できない．

量子回路では，状態のコピーはできないが，状態を表す線形重合わせではコピーが実現できる．それは，CN ゲートと補助ビットを用いて実現する．状態 $|\psi\rangle \otimes |0\rangle$ に対し，第一ビット (コピー元) を制御ビット，補助ビット (コピー先) を目標ビットとする CN ゲートを適用して得られる状態は

$$\begin{aligned} U_{CN}(|\psi\rangle \otimes |0\rangle) &= U_{CN}((\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes |0\rangle) \\ &= U_{CN}(\alpha_0|00\rangle + \alpha_1|10\rangle) \\ &= \alpha_0|00\rangle + \alpha_1|11\rangle \end{aligned}$$

となり，線形重合わせで $|0\rangle$ のコピーと $|1\rangle$ のコピーがそれぞれ実現できる．以下では，量子回路においてコピーを行うことは上で述べた CN ゲートと補助ビットを用いたコピーのことを指す．

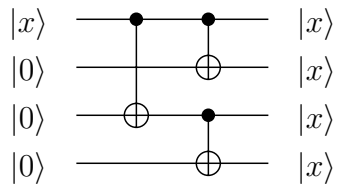

図 2.2: 一量子ビットの状態 $\sum_{x\in\{0,1\}} \alpha_x|x\rangle$ における $|x\rangle$ のコピー（3 個コピーする場合）

次に，任意の正整数 l に対し，一量子ビットの状態

$$|\psi\rangle = \sum_{x\in\{0,1\}} \alpha_x|x\rangle$$

における $|x\rangle$ を l 補助ビットへ l 個コピーすることを考える．l 補助ビットを入力と見なし，

$$\sum_{x\in\{0,1\}} \alpha_x|x,0,0,...,0\rangle$$

とし，$|x\rangle$ である量子ビットを制御ビットとし，$|0\rangle$ である量子ビットを目標ビットとする U_{CN} を適用して得られる状態は

$$\sum_{x\in\{0,1\}} \alpha_x|x,x,0,...,0\rangle$$

となり，一つの U_{CN} の適用で $|x\rangle$ が一つコピーされる．同様に 各 $|x\rangle$ に対して，$|x\rangle$ である量子ビットを制御ビットとし，$|0\rangle$ である量子ビットを目標ビットとする U_{CN} を並列に適用することを繰り返せば，深さ $\log l$ で $|x\rangle$ を l 個コピーできる（図 2.2 参照）．また，任意の正整数 k と l に対し，k 量子ビットの状態

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

における $|X\rangle$ を kl 補助ビットへ l 個 コピーすることを考える．ここで，$X = (x_1, x_2, ..., x_k)$ とすると，各 x_j $(1 \leq j \leq k)$ に対して，並列に $|x_j\rangle$ を l 補助ビットへ l 個コピーすれば，深さは $\log l$ で $|X\rangle$ を l 個コピーできる．

2.5 本研究で扱う量子回路

本研究では，以下の三種類の量子回路を扱う．それは，

- CN ゲートで構成される量子回路，
- 任意の正整数 l に対し，l ビット PS ゲートと CN ゲートで構成される量子回路，及び，
- WH ゲートと CN ゲートで構成される量子回路

である．この三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 [21] の結果がある．Moore と Nilsson は以下の三つの結果を示した．

命題 2.1 CN ゲートで構成され，n ビット変換 U を実現する n 入力量子回路が与えられたとき，変換 U は補助ビット数 $O(n^2)$ 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 2.2 s 個の l ビット PS ゲート $G_1, G_2, ..., G_s$ と CN ゲートで構成され，n ビット変換 U を実現する n 入力量子回路が与えられとき，変換 U は補助ビット数 $O(lsn+n^2)$ 深さ $O(\log n + \log s)$ の s 個の l ビット PS ゲート $G_1, G_2, ..., G_s$ と CN ゲートで構成される量子回路で実現できる．

命題 2.3 WH ゲートと CN ゲートで構成され，n ビット変換 U を実現する n 入力量子回路が与えられたとき，変換 U は補助ビット数 $O(n^2)$ 深さ $O(\log n)$ の WH ゲートと CN ゲートで構成される量子回路で実現できる．

本研究では，この三つの命題で用いる補助ビットの数を改良した．三種類の量子回路それぞれに対する本研究の並列化手法で用いる補助ビットの数はこの三つの命題で用い

る補助ビットの数の $1/\log n$ 倍である．さらに，より一般な結果として，使用できる補助ビットの数が固定した場合，三種類の量子回路それぞれについての並列化手法を示した．

次に，本研究で扱う三種類の量子回路に関する性質について考える．

ある量子ゲートのクラスが universal とは，そのクラスに含まれる量子ゲートを用いて量子回路を構成すれば，任意のユニタリ変換を実現する量子回路が構成できる．Universal な量子ゲートのクラスに関する代表的な結果として，Barenco ら [2] によってすべての一ビット量子ゲートと CN ゲートからなる量子ゲートのクラスは universal であることが示された．また，任意の一ビット量子ゲートが実現する一ビット変換は以下の形で表現できる．

$$\begin{pmatrix} e^{i\sigma} & 0 \\ 0 & e^{i\sigma} \end{pmatrix} \begin{pmatrix} e^{i\lambda} & 0 \\ 0 & e^{-i\lambda} \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} \begin{pmatrix} e^{i\mu} & 0 \\ 0 & e^{-i\mu} \end{pmatrix}$$

ここで，σ，λ，θ，μ は実数である．

本研究では，上で示した一ビット量子ゲートが実現する四つの一ビット変換の積において，一番目，二番目，及び，四番目の変換を実現する一ビット PS ゲートを含む l ビット PS ゲートと三番目の変換で $\theta = \pi/4$ の場合を実現する WH ゲートを扱っている．本研究で扱っている CN ゲートと PS ゲートにあと三番目の任意の変換を実現する一ビット量子ゲートを加えた量子ゲートのクラスは universal となる．

第 3 章

CN ゲート
で構成される量子回路

3.1 CN ゲートで構成される量子回路の性質

この章では，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，まず 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ある量子回路が与えられれば，その量子回路が実現する変換の逆変換を実現する CN ゲートで構成される量子回路が容易に得られる．U を CN ゲートで構成される量子回路で実現される任意の変換とする．CN ゲートが実現する変換 U_{CN} は自分自身の逆変換，すなわち，

$$U_{CN}U_{CN} = I$$

であることから，U を実現する CN ゲートで構成された量子回路が与えられたとき，この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 U の逆変換 $U^\dagger$ を実現する（図 3.1 と 3.2 参照）．よって，変換 $U^\dagger$ を実現する CN ゲートで構成される量子回路は U を実現する CN ゲートで構成される量子回路と同じ複雑さで実現できる．

次に，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 (2.4) か

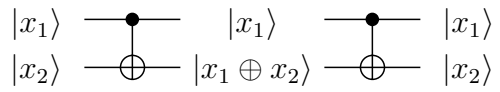

図 3.1: 二つの同じ CN ゲートが実現する変換

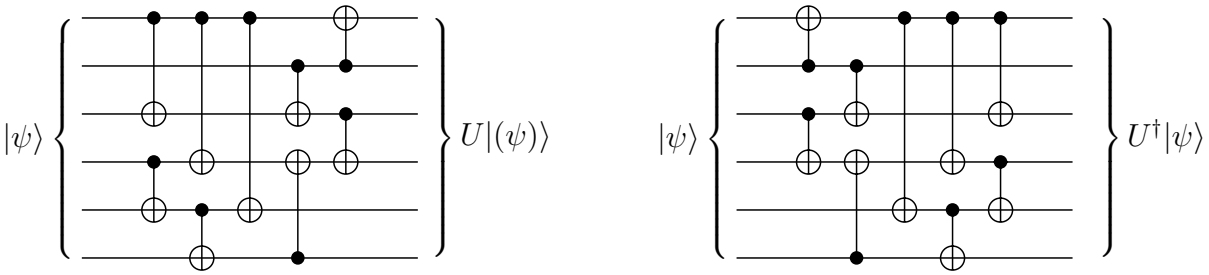

図 3.2: 逆変換を実現する CN ゲートで構成される量子回路

ら，CN ゲートを任意の状態に適用することは，その状態を表す線形重合わせにおいて，あるビット (すなわち，目標ビット) があるもう一つのビット (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．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．すると，n ビット変換 U は次の条件を満たす．ある集合 $S_1, S_2, \ldots, S_m \subseteq \{1, 2, \ldots, n\}$ が存在し，任意の $X = (x_1, x_2, \ldots, x_n) \in \{0, 1\}^n$ に対し，

$$U|X\rangle = |F_U(X)\rangle$$

となる．ただし，

$$F_U(X) = \left(\bigoplus_{k \in S_1} x_k, \bigoplus_{k \in S_2} x_k, \ldots, \bigoplus_{k \in S_m} x_k \right)$$

である．

3.2 CN ゲートで構成される量子回路の並列化

まず，補助ビットが使用できないとき，CN ゲートで構成される量子回路について以下の補題が成り立つことを示す．

補題 3.1 CN ゲートで構成され，n ビット変換 U を実現する n 入力量子回路が与えられたとき，変換 U 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．

証明． 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．ある集合 $S_1, S_2, \ldots, S_n \subseteq \{1,2,\ldots,n\}$ が存在し，

$$U|X\rangle = |F_U(X)\rangle$$

となるとする．ただし，

$$F_U(X) = \left(\bigoplus_{k\in S_1} x_k, \bigoplus_{k\in S_2} x_k, \ldots, \bigoplus_{k\in S_n} x_k \right)$$

である．まず，$X' \in \{0,1\}^n$ に対し，n ビット変換 U' を

$$U'U|X\rangle = |X'\rangle$$

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．U' を実現する CN ゲートで構成される量子回路を示す．

Begin
  Set $B := \emptyset$;
  Repeat for $j = 1,2,\ldots,n$ do
    Find $b_j \in S_j \setminus B$;
    Set $B := B \cup \{b_j\}$;
    Repeat for $k = 1,2,\ldots,n-1$ do
      Set $t := (j+k-1) \bmod n + 1$;
      If $b_j \in S_t$ Then
        Set $S_t := S_t \oplus S_j$;
        Put CN gate with control bit at j-th bit
            and target bit at t-th bit ;

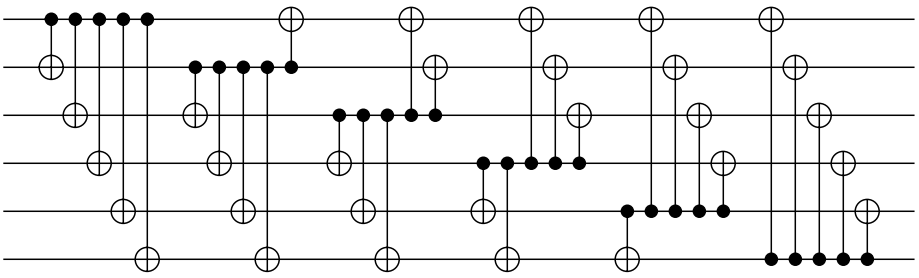

図 3.3: 各制御ビットに対する CN ゲートの順序（$k = 6$ の場合）

End

End

End

End

ここでの $\oplus$ は集合に対する排他的論理和である．以上より，$S_1, S_2, ..., S_n$ はそれぞれ一つの要素だけになる．また，配置された CN ゲートの順序は第一ビットを制御ビットとする CN ゲートの目標ビットの順序は $2 \prec 3 \prec \cdots \prec n$ となる．また，第二ビットを制御ビットとする CN ゲートの目標ビットの順序は $3 \prec 4 \prec \cdots \prec n \prec 1$ となる．以下同様に，第 k ビットを制御ビットとする CN ゲートの目標ビットの順序は $(k \bmod n) + 1 \prec (k + 1 \bmod n) + 1 \prec \cdots \prec (k + n - 1 \bmod n) + 1$ となる（図 3.3 参照）．各制御ビットに対する順序を変えずに入力を共有しない CN ゲートを同じ層に配置すると深さ高々 $3n - 3$ となる（図 3.4 参照）．よって，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．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 [21]．これを用いて $|X'\rangle$ を置換すると $|X\rangle$ となる．よって，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．以上より，U 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．

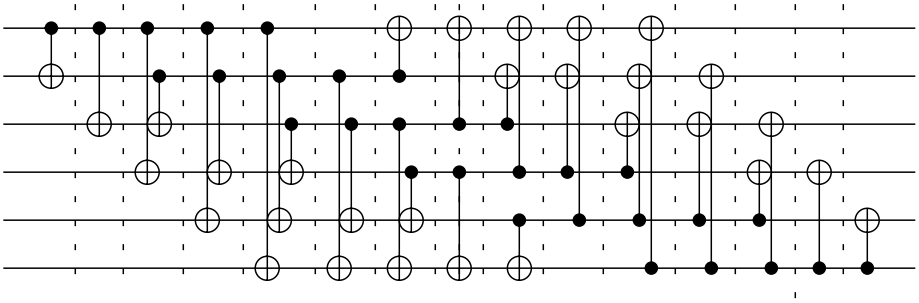

図 3.4: $k = 6$ の場合，CN ゲートで構成される量子回路（図中の点線は層の区切りを表現している）

よって，変換 U は補助ビットを使用しないで深さ $O(n)$ の CN ゲートで構成される量子回路で実現できる．■

また，本研究で使用する変換を次のように定義する．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 U が次の条件を満たすとき、$U \in \mathcal{CN}(n,m)$ 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，

$$U|X,Y\rangle = |X, Y \oplus F_U(X)\rangle$$

となる．ただし，

$$F_U(X) = \left(\bigoplus_{k \in S_1} x_k, \bigoplus_{k \in S_2} x_k, \ldots, \bigoplus_{k \in S_m} x_k \right)$$

である．図では第 j $(1 \leq j \leq n)$ ビットに $\diamond$ を書き，第 j' $(n+1 \leq j' \leq n+m)$ ビットに長方形を書く．そして，$\diamond$ と長方形を実線で結び，$\diamond$ の上に変換 U を書く（図 3.5 参照）．

次に，変換 $U \in CN(n,m)$ が補助ビットを使用しないで CN ゲートで構成される量子回路で実現できることを以下の補題で示す．

補題 3.2 任意の正整数 n と m に対し，$(n+m)$ ビット変換 $U \in \mathcal{CN}(n,m)$ は補助ビットを使用しないで深さ $\max\{n,m\}$ の CN ゲートで構成される量子回路で実現できる．

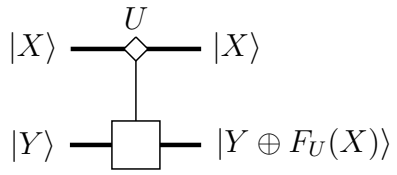

図 3.5: $U \in \mathcal{CN}(n,m)$ を実現する量子ゲートの表記法

証明. 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．ある集合 $S_1, S_2, \ldots, S_m \subseteq \{1,2,\ldots,n\}$ が存在し，任意の $Y = (y_1, y_2, \ldots, y_m) \in \{0,1\}^m$ に対し，

$$U|X,Y\rangle = |X, Y \oplus F_U(X)\rangle$$

となるとする．ただし，

$$F_U(X) = \left(\bigoplus_{k \in S_1} x_k, \bigoplus_{k \in S_2} x_k, \ldots, \bigoplus_{k \in S_m} x_k \right)$$

である．U を実現する CN ゲートで構成される量子回路を示す.

Begin
  Repeat for $v = 1, 2, \ldots, mn$ do
    Set $k := (v-1) \bmod n + 1$;
    Set $j := (v-1) \bmod m + 1$;
    If $x_k \in S_j$ Then
      Put CN gate with control bit at k-th bit
        and target bit at $n+j$-th bit at Level v ;
    End
  End
End

以上より，第 $n+j$ $(1 \leq j \leq m)$ ビットには $\bigoplus_{k \in S_j} x_k$ が計算される．よって，任意の $U \in \mathcal{CN}(n,m)$ は深さ高々 $\max\{n,m\}$ で実現できる（図 3.6 参照）.

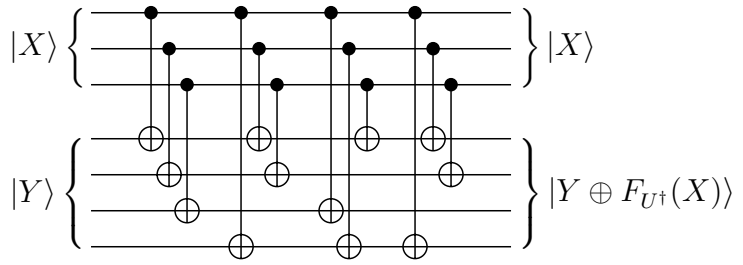

図 3.6: $U \in \mathcal{CN}(3,4)$ を実現する深さ $\max\{3,4\}$ の量子回路

■

$(k-1)n$ 個の補助ビットが使用できる場合，以下の補題が成り立つ．

補題 3.3 任意の正整数 k，n と m に対し，$(n+km)$ ビット変換 $U \in \mathcal{CN}(n,km)$ は補助ビット数 $(k-1)n$ 深さ $\max\{n,m\}+2\log k)$ 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 $n+km$ 量子ビットの状態を一般性を失うことなく

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

とする．ただし，$X \in \{0,1\}^n$，$Y_1, Y_2, \ldots, Y_k \in \{0,1\}^m$ である．任意の $U \in \mathcal{CN}(n,km)$ に対して $V_1, V_2, \ldots, V_k \in \mathcal{CN}(n,m)$ が存在し，$F_U = (F_{V_1}, F_{V_2}, \ldots, F_{V_k})$ を満たす．すなわち，

$$U|X, Y_1, Y_2, \ldots, Y_k\rangle = |X, Y_1 \oplus F_{V_1}(X), Y_2 \oplus F_{V_2}(X), \ldots, Y_k \oplus F_{V_k}(X)\rangle$$

を満たす（図 3.7 参照）．

まず，$(k-1)n$ 補助ビットを入力と見なし，

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

とし，$k-1$ 個 $|X\rangle$ のコピーを深さ $\log k$ で補助ビットに生成すると，

$$|X, X, ..., X, Y_1, Y_2, \ldots, Y_k\rangle$$

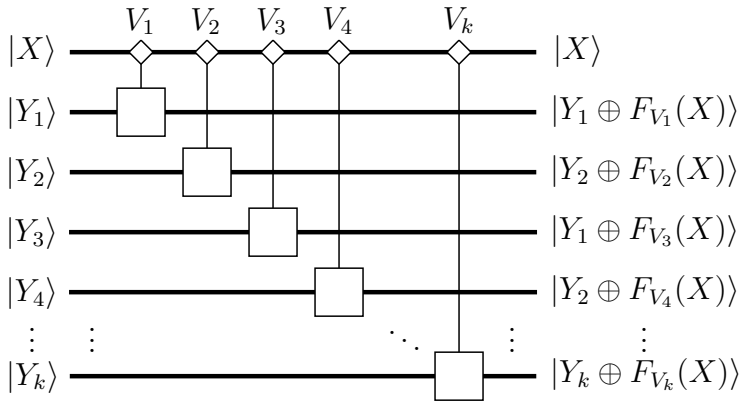

図 3.7: $U \in \mathcal{CN}(n, km)$ を実現する量子回路

となる．元の $|X\rangle$ と合せて k 個の X がある．次に，並列に $|X\rangle$ の一つのコピーと $|Y_j\rangle$ に対して変換 V_j を適用して得られる状態は

$$|X, X, ..., X, Y_1 \oplus F_{V_1}(X), Y_2 \oplus F_{V_2}(X), \ldots, Y_k \oplus F_{V_k}(X)\rangle$$

となる．ここで，変換 V_j は補題 3.2 より深さ高々 $\max\{n, m\}$ で実現できる．X のコピーの逆変換を適用し，深さ $\log k$ ですべて補助ビットを $|0\rangle$ に戻すと，

$$|X, 0^n, ..., 0^n, Y_1 \oplus F_{V_1}(X), Y_2 \oplus F_{V_2}(X), \ldots, Y_k \oplus F_{V_k}(X)\rangle$$

となり，U を適用して得られる状態と同じになる（図 3.8 参照）.

よって，変換 $U \in CN(n, km)$ は補助ビット数 $(k-1)n$ 深さ高々 $\max\{n, m\} + 2\log k$ の CN ゲートで構成される量子回路で実現できる． ■

$(k-1)m$ 個の補助ビットが使用できる場合，以下の補題が成り立つ.

補題 3.4 任意の正整数 k，n と m に対し，$(kn+m)$ ビット変換 $U \in \mathcal{CN}(kn, m)$ は補助ビット数 $(k-1)m$ 深さ $2\max\{n, m\} + 2\log k$ 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 $kn+m$ 量子ビットの状態を一般性を失うことなく

$$|X_1, X_2, \ldots, X_k, Y\rangle$$

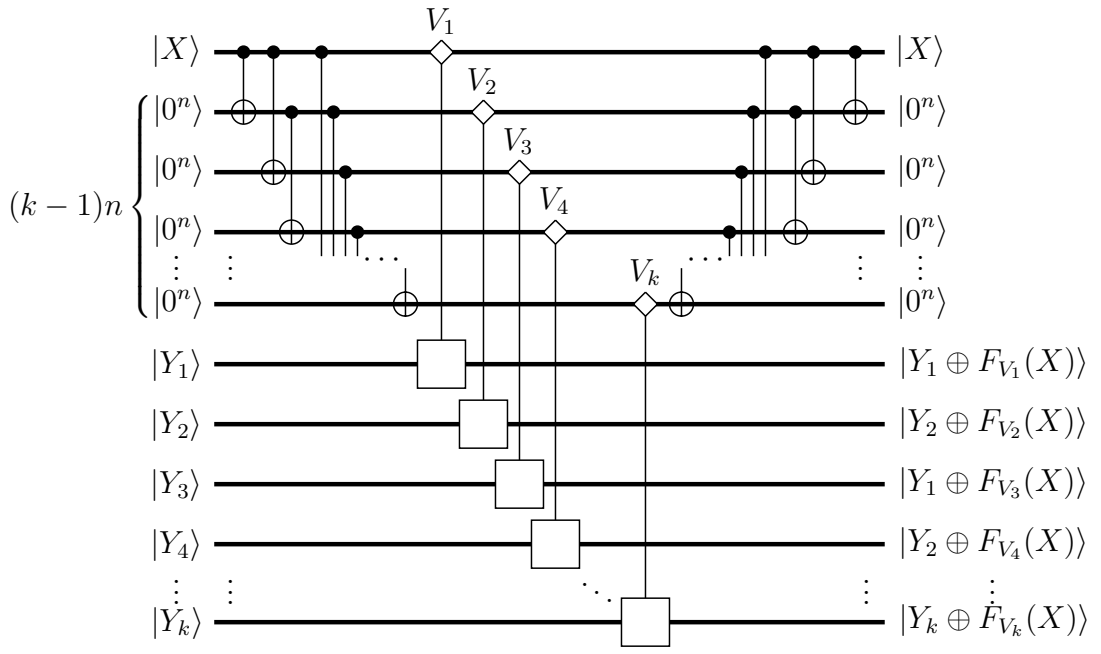

図 3.8: $U \in \mathcal{CN}(n, km)$ の並列化

とする．ただし，$X_1, X_2, \ldots, X_k \in \{0,1\}^n$，$Y \in \{0,1\}^m$ である．任意の $U \in \mathcal{CN}(kn, m)$ に対して $W_1, W_2, \ldots, W_k \in \mathcal{CN}(n, m)$ が存在し，

$$F_U(X_1, X_2, \ldots, X_k) = F_{W_1}(X_1) \oplus F_{W_2}(X_2) \oplus \cdots \oplus F_{W_k}(X_k)$$

を満たす（図 3.9 参照）．まず，$(k-1)m$ 補助ビットを入力と見なし，

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

とし，並列に各 W_j を実現する．$|X_1\rangle$ と $|Y\rangle$ に対して W_1 を適用し、$2 \leq j \leq k$ に対し，$|X_j\rangle$ と m 個の補助ビットに W_j を適用する．すると，得られる状態は

$$|X_1, X_2, \ldots, X_k, Y \oplus F_{W_1}(X_1), F_{W_2}(X_2), ..., F_{W_k}(X_k)\rangle$$

となる．ここで，変換 W_j $(1 \leq j \leq k)$ は補題 3.2 より深さ高々 $\max\{n, m\}$ で実現できる．次に $|Y \oplus F_{W_1}(X_1)\rangle$ に $|F_{W_2}(X_2)\rangle, |F_{W_3}(X_3)\rangle, \ldots, |F_{W_k}(X_k)\rangle$ を用いて $|Y \oplus F_U(X_1, \ldots, X_k)\rangle$ を深さ $\log k$ で実現する．最後に使用した $(k-1)m$ 個の補助ビットを

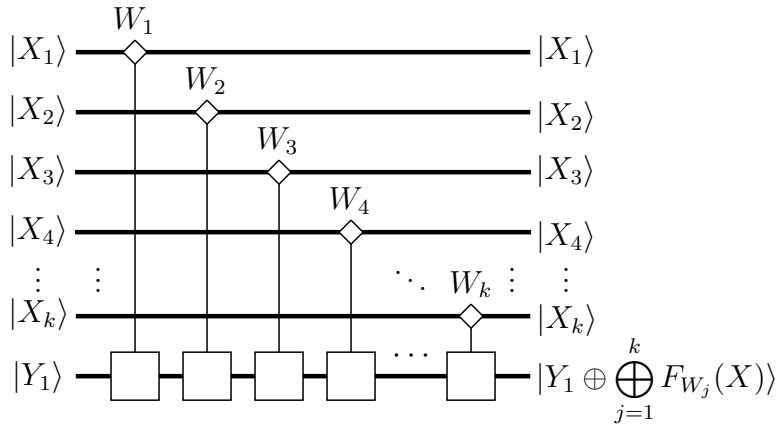

図 3.9: $U \in \mathcal{CN}(kn, m)$ を実現する量子回路

深さ高々 $\max\{n, m\} + \log k$ で $|0\rangle$ に戻すと，

$$|X_1, X_2, \ldots, X_k, Y \oplus F_U(X_1, \ldots, X_k), 0^m, ..., 0^m\rangle$$

となり，U を適用して得られる状態と同じになる（図 3.10 参照）.

よって，変換 U は補助ビット数 $(k-1)m$ 深さ高々 $2\max\{n, m\} + 2\log k$ の CN ゲートで構成される量子回路で実現できる. ■

最後に，任意の $U \in \mathcal{CN}(n, m)$ に対して，τn 補助ビットが使用できる場合，以下の補題が成り立つ.

補題 3.5 任意の正整数 τ，n と m に対し，$(n+m)$ ビット変換 $U \in \mathcal{CN}(n, m)$ は補助ビット数 τn 深さ $O((n+m)/(\tau+1) + \log(\tau+1))$ の CN ゲートで構成される量子回路で実現できる.

証明. 補題 3.3 と補題 3.4 より，U は補助ビット数 $(k_1-1)n + (k_2-1)m$ 深さ高々 $2\max\{n/k_2, m/k_1\} + 2\log k_1 + 2\log k_2$ で実現できる．ここで，$k_1 = (\tau n + n + m)/2n$, $k_2 = (\tau n + n + m)/2m$ とすると，深さ $2\max\{2nm/(\tau n + n + m), 2nm/(\tau + n + m)\} + 2\log((\tau n + n + m)/2n) + 2\log((\tau n + n + m)/2m) = O((n+m)/(\tau+1) + \log(\tau+1))$ となる.

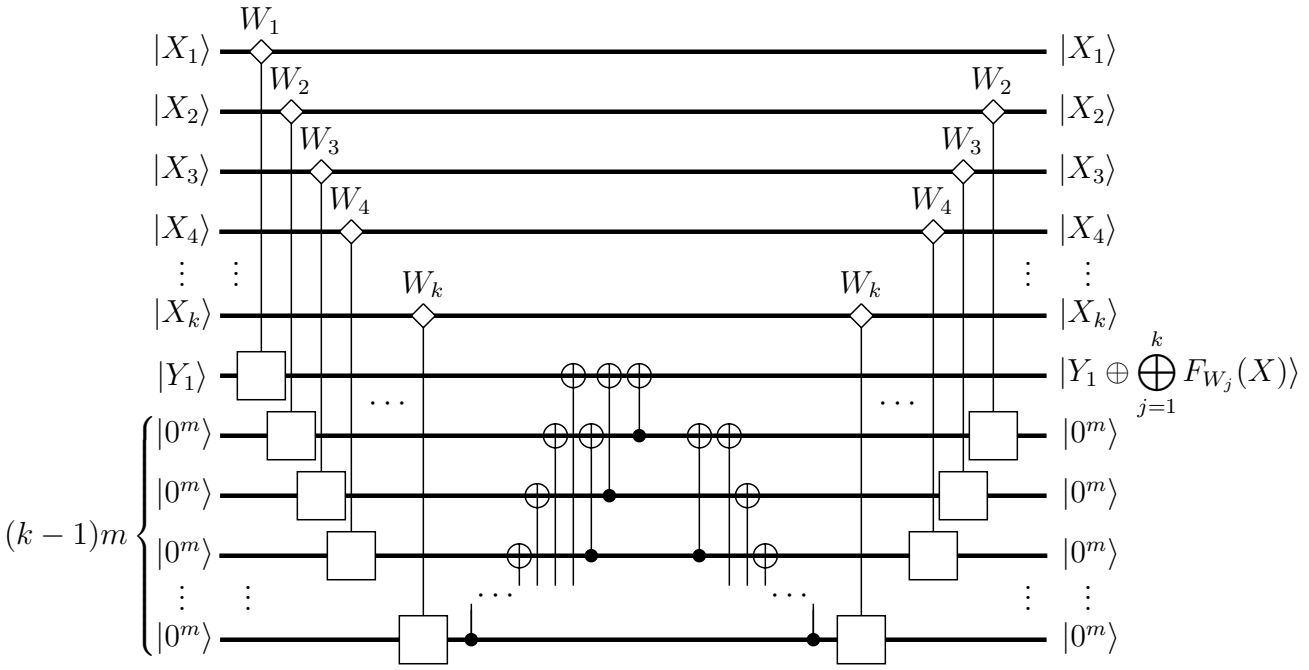

図 3.10: $U \in \mathcal{CN}(kn, m)$ の並列化

よって，変換 $U \in \mathcal{CN}(n, m)$ は補助ビット数 τn 深さ $O((n+m)/(\tau+1) + \log(\tau+1))$ の CN ゲートで構成される量子回路で実現できる． ■

そして，本研究では 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 3.6 CN ゲートで構成され，n ビット変換 U を実現する n 入力量子回路が与えられたとき，任意の整数 $\tau \geq 0$ に対し，変換 U は補助ビット数 τn 深さ $O(n/(\tau+1) + \log(\tau+1))$ の CN ゲートで構成される量子回路で実現できる．

証明． $\tau = 0$ のとき，補題 3.1 より補助ビットを使用しないで深さ $O(n)$ の CN ゲートで構成される量子回路で実現できる．

$\tau \geq 1$ のとき，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．ある集合 $S_1, S_2, \ldots, S_n \subseteq \{1, 2, \ldots, n\}$ が存在し，任意の

$Y = (y_1, y_2, \ldots, y_n) \in \{0,1\}^n$ に対し，

$$U|X, Y\rangle = |X, Y \oplus F_U(X)\rangle$$

となるとする．ただし，

$$F_U(X) = \left(\bigoplus_{k \in S_1} x_k, \bigoplus_{k \in S_2} x_k, \ldots, \bigoplus_{k \in S_n} x_k \right)$$

である．また，変換 $V, V' \in \mathcal{CN}(n, n)$ を

$$\begin{aligned} V|X, Y\rangle &= |X, Y \oplus F_U(X)\rangle \\ V'|F_U(X), Y\rangle &= |F_U(X), Y \oplus X\rangle \end{aligned}$$

とおく．n 補助ビットを入力と見なし，

$$|X, 0^n\rangle$$

V を適用して得られる状態は

$$|X, F_U(X)\rangle$$

となる．そして，$|X\rangle$ と $|F_U(X)\rangle$ を入れ替える．これは深さ 3 の CN ゲートで構成される量子回路で実現できる（図 3.11 参照）．すると，

$$|F_U(X), X\rangle$$

となる．次に，V' を適用して得られる状態は

$$|F_U(X), X \oplus X\rangle = |F_U(X), 0^n\rangle$$

となり，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 V と V' の並列化のために使用すると，V と V' は補題 3.5 より補助ビット数 $(\tau - 1)n$ 深さ $O(n/\tau + \log \tau)$ の CN ゲートで実現できる．

よって，U は補助ビット数 τn 深さ $O(n/(\tau + 1) + \log(\tau + 1))$ の CN ゲートで構成される量子回路で実現できる．

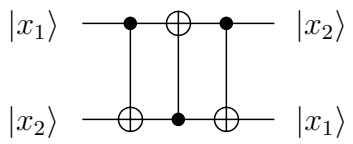

図 3.11: 二量子ビットの基底 $|x_1, x_2\rangle$ に対する $|x_1\rangle$ と $|x_2\rangle$ の入れ替え

■

この定理より，以下の系が成り立つ.

系 3.7 CN ゲートで構成され，n ビット変換 U を実現する n 入力量子回路が与えられたとき，変換 U は補助ビット数 $O(n^2/\log n)$ 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.

第 4 章

PS ゲートと CN ゲートで構成される量子回路

4.1 PS 変換の積の並列化

PS ゲートと CN ゲートで構成される量子回路について，与えられた量子回路が実現する変換を PS 変換で実現される部分と CN ゲートで構成される量子回路で実現される部分へ分け，それぞれの部分を補助ビットを用いて並列化することを考える．

s 個の l ビット PS ゲート $G_1, G_2, ..., G_s$ と CN ゲートで構成される n 入力量子回路が与えられとき，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

$$C_s P_s C_{s-1} \cdots P_1 C_0$$

と表現できる．ただし，C_k $(0 \leq k \leq s)$ 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，P_j $(1 \leq j \leq s)$ は PS ゲート G_j のみで構成される一層の回路が実現する n ビット PS 変換である．さらに，

$$C_s \cdots C_0 D_s \cdots D_1$$

と変形できる．ここで，$D_j = (C_j \cdots C_0)^\dagger P_j (C_j \cdots C_0)$ である．

$D_s \cdots D_1$ について，以下の補題が成り立つ．

補題 4.1 s 個の n ビット PS 変換 $D_1, ..., D_s$ が与えられたとき，$D_s \cdots D_1$ は補助ビット数 sn 深さ $O(\log s)$ の s 個の n ビット PS 変換 $D_1, ..., D_s$ と 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 量子ビットの任意の状態を

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

とし，各 D_j $(1 \leq j \leq s)$ を $|\psi\rangle$ へ適用して得られる状態が

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

となるとする．そして，sn 補助ビットを入力と見なし，

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

とする．まず， s 個 X のコピーを深さ $\log s$ で補助ビットに生成し，並列に X の一つのコピーに対し変換 D_j を適用して得られる状態は

$$\sum_{X \in \{0,1\}^n} \alpha_X e^{i(\gamma_1(X)+\cdots+\gamma_s(X))} |X, X, ..., X\rangle$$

となる．X のコピーの逆操作を行い深さ $\log s$ で使用した補助ビットを $|0\rangle$ に戻すと，

$$\sum_{X \in \{0,1\}^n} \alpha_X e^{i(\gamma_1(X)+\cdots+\gamma_s(X))} |X, 0^n, ..., 0^n\rangle$$

となり，$D_s \cdots D_1$ を $|\psi\rangle$ に適用して得られた状態と同じになる（図 4.1 参照）．

よって，$D_s \cdots D_1$ は補助ビット数 sn 深さ $O(\log s)$ の s 個の n ビット PS 変換 D_j と CN ゲートで構成される量子回路で実現できる． ■

ここで，各 D_j をより厳密に，つまり一つの n ビット PS 変換としてではなく，$(C_j \cdots C_0)^\dagger P_j (C_j \cdots C_0)$ として扱うと，以下の補題が成り立つ．

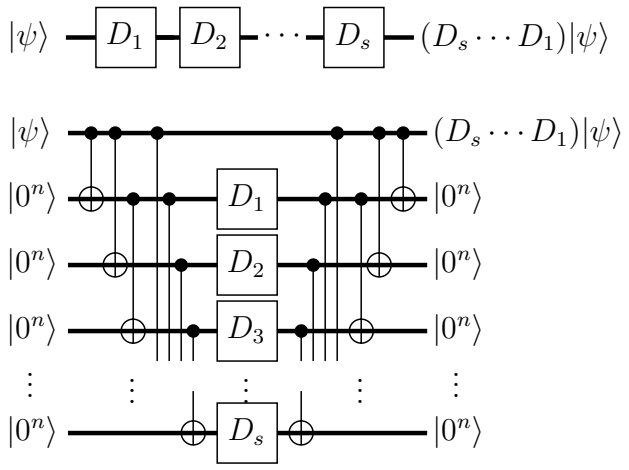

図 4.1: PS 変換の系列 $D_s \cdots D_1$ の並列化

補題 4.2 s 個の l ビット PS ゲート $G_1, ..., G_s$ と CN ゲートで構成される n ビット PS 変換 $D_j = (C_j \cdots C_0)^\dagger P_j (C_j \cdots C_0)$ $(1 \leq j \leq s)$ が与えられたとき，ここで，P_j は l $(l \geq 1)$ ビット PS ゲート G_j で構成される一層の回路が実現する n ビット変換である．$D_s \cdots D_1$ は補助ビット数 ln 深さ $O(\log s)$ の s 個の l ビット PS ゲート $G_1, ..., G_s$ と CN ゲートで構成される量子回路で実現できる．

証明．

各 D_j の $C_j \cdots C_0$ は $|\psi\rangle$ から G_j の入力 l 量子ビットの状態を計算する変換であり，$C_j \cdots C_0$ を $\sum_{X \in \{0,1\}^n} \alpha_X |X\rangle$ へ適用して得られた状態は一般性を失うことなく

$$\sum_{X \in \{0,1\}^n} \alpha_X |\rho_j(X), \rho'_j(X)\rangle$$

となるとする．ここで，$\rho_j(X) \in \{0,1\}^l, \rho'_j(X) \in \{0,1\}^{n-l}$ であり，$|\rho_j(X)\rangle$ は G_j の入力 l 量子ビットの状態である．また，$U \in \mathcal{CN}(n, ls)$ を 任意の $X \in \{0,1\}^n, Y_j \in \{0,1\}^l$ に対し，

$$U|X, Y_1, ..., Y_s\rangle = |X, Y_1 \oplus \rho_1(X), ..., Y_s \oplus \rho_s(X)\rangle$$

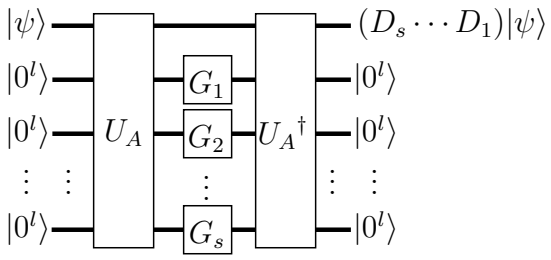

図 4.2: PS ゲートの並列化

となる変換とする．まず，ls 補助ビットを入力と見なし，

$$\sum_{X\in\{0,1\}^n} \alpha_X |X, 0^l, ..., 0^l\rangle$$

とする．U を適用して得られる状態は

$$\sum_{X\in\{0,1\}^n} \alpha_X |X, \rho_1(X), ..., \rho_s(X)\rangle$$

となり，各 $|\rho_j(X)\rangle$ に G_j を並列に適用し，$U^\dagger$ 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

$$\sum_{X\in\{0,1\}^n} \alpha_X e^{i(\theta_1(\rho_1(X))+\cdots+\theta_s(\rho_s(X)))} |X, 0^l, ..., 0^l\rangle$$

となり，$D_s \cdots D_1$ を $|\psi\rangle$ に適用して得られた状態と同じになる．

よって，$D_s \cdots D_1$ は補助ビット数 ls 深さ $O(\log s)$ の s 個の l ビット PS ゲート $G_1, ..., G_s$ と CN ゲートで構成される量子回路で実現できる． ■

4.2 PS ゲートと CN ゲートで構成される量子回路の並列化

PS ゲートの並列化を利用して 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 4.3 s 個の l ビット PS ゲート $G_1, G_2, ..., G_s$ と CN ゲートで構成され，n ビット変換 U を実現する n 入力量子回路が与えられとき，変換 U は補助ビットを使用しないで深さ $O(sn)$，そして，任意の整数 $\tau \geq 1$ に対し，補助ビット数 τn 深さ $O((ls+n)/\tau + (ls\log\tau)/\tau n + \log\tau)$ の s 個の l ビット PS ゲート $G_1, G_2, ..., G_s$ と 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 $|\psi\rangle = \sum_{X\in\{0,1\}^n} \alpha_X |X\rangle$ とする．前節で述べたように，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

$$U = C_s P_s C_{s-1} \cdots P_1 C_0$$

と表現できる．ただし，C_k $(0 \leq k \leq s)$ 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，P_j $(1 \leq j \leq s)$ は PS ゲート G_j のみで構成される一層の回路が実現する n ビット PS 変換である．

$\tau = 0$ のとき，各 C_k の深さが $O(n)$ より大きい場合，補題 3.1 より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，U は補助ビットを使用しないで深さ $O(sn)$ の CN ゲートで構成される量子回路で実現できる．

さらに，U は

$$U = C_s \cdots C_0 D_s \cdots D_1$$

と変形できる．ここで，$D_j = (C_j \cdots C_0)^\dagger P_j (C_j \cdots C_0)$ である．$\tau \geq 1$ のとき，$D_s \cdots D_1$ について，$r = \lceil \tau/2 \rceil$ とすると，rn 補助ビットと $U_A, {U_A}^\dagger \in \mathcal{CN}(n, rn)$ を用いて $\lfloor rn/l \rfloor$ 個の G_j を並列化する．$\lceil ls/rn \rceil$ 回分けて $\lfloor rn/l \rfloor$ 個の G_j 並列に適用することで $D_s \cdots D_1$ が実現できる．ここで，残りの $(\tau - r)n$ 補助ビットを U_A と ${U_A}^\dagger$ の並列化のために使用すると，補題 3.5 より U_A と ${U_A}^\dagger$ は深さ $O((n+rn)/(\tau - r + 1) + \log(\tau - r + 1))$ で実現できるので，$D_s \cdots D_1$ は深さ $O(ls/\tau + ls\log\tau/\tau n)$ で実現できる．また，$C_s \cdots C_0$ について，定理 3.6 より $C_s \cdots C_0$ は深さ $O(n/\tau + \log\tau)$ で実現できる．

以上より，U は補助ビットが使用しないで深さ $O(sn)$，そして，$\tau \geq 1$ に対し，補助ビット数 τn 深さ $O((ls+n)/\tau + (ls\log\tau)/\tau n + \log\tau)$ の s 個の l ビット PS ゲート $G_1, ..., G_s$ と CN ゲートで構成される量子回路で実現できる．■

ここで，定理 4.3 で構成される量子回路に含まれている s 個の l ビット PS ゲート $G_1, ..., G_s$ のみである．それは与えられた量子回路に含まれている l ビット PS ゲートである．また，定理 4.3 より，以下の系が成り立つ．

系 4.4 s 個の l ビット PS ゲート $G_1, G_2, ..., G_s$ と CN ゲートで構成され，n ビット変換 U を実現する n 入力量子回路が与えられとき，変換 U は補助ビット数 $O((lsn+n^2)/\log n)$ 深さ $O(\log n + \log s)$ の s 個の l ビット PS ゲート $G_1, G_2, ..., G_s$ と CN ゲートで構成される量子回路で実現できる．

第 5 章

WH ゲートと CN ゲートで構成される量子回路

5.1 量子ゲートの定義

この章で使用する量子ゲートの定義を行う．まず，**π-Shift ゲート**とは二ビット量子ゲートであり，4×4 ユニタリ行列

$$U_\pi = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

で定義されるユニタリ変換 U_π を実現する（図 5.1 参照）．そして，**wiggle ゲート**とは二ビット量子ゲートであり，4×4 ユニタリ行列

$$U_w = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix}$$

で定義されるユニタリ変換 U_w を実現する（図 5.2 参照）．また，2×2 ユニタリ行列 G_X, G_Z を

$$G_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, G_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

とする．

5.2　各量子ゲートの関係を用いた量子回路の分解

この章で示す WH ゲートと CN ゲートで構成される量子回路の並列化手法は，まず各量子ゲートの関係を用いて量子ゲートを入れ替え，与えられた量子回路を並列化に適した量子回路へ分解する．そして，分解されたそれぞれの量子回路について並列化を行う．WH ゲートと CN ゲートで構成される量子回路について，以下の補題が成り立つ．

補題 5.1 WH ゲートと CN ゲートで構成される量子回路が与えられたとき，状態が $|1\rangle$ である一補助ビットを使用して CN ゲートで構成される量子回路，π-*Shift* ゲートと *wiggle* ゲートで構成される量子回路，そして，WH ゲートで構成される一層の量子回路の三つの量子回路へこの順序で分解できる．

証明． まず，すべての WH ゲートを出力側へ移動する（図 5.3 参照）．すると，$U_{WH}^2 = I$ となるので，与えられた量子回路は CN ゲート，π-Shift ゲート，wiggle ゲートで構成される量子回路とその出力側に WH ゲートで構成される一層の回路となる．

次に分解された CN ゲート，π-Shift ゲート，wiggle ゲートで構成される量子回路について，CN ゲートを入力側へ移動する（図 5.4 参照）．ここで，G_Z と G_X で定義される一ビット量子ゲートが生成されるが，状態が $|1\rangle$ である補助ビットを制御ビットとする π-Shift ゲートと CN ゲートへそれぞれ置き換えることができる．すると，CN ゲートで構成される量子回路とその出力側に π-Shift ゲートと wiggle ゲートで構成される量子回路となる．

よって，状態が $|1\rangle$ である一補助ビット を使用して WH ゲートと CN ゲートで構成される量子回路は CN ゲートで構成される量子回路，π-Shift ゲートと wiggle ゲートで構成される量子回路，そして，WH ゲートで構成される一層の量子回路の三つの量子回路へこの順序で分解できる． ■

また，π-Shigt ゲートと wiggle ゲートで構成される量子回路について，以下の補題が成り立つ．

補題 5.2 *π-Shigt* ゲートと *wiggle* ゲートで構成される任意量子回路が与えられたとき，補助ビットを使用しないで CN ゲートで構成される量子回路，*π-Shift* ゲートで構成される量子回路，*wiggle* ゲートで構成される量子回路，そして，もう一つの *π-Shift* ゲートで構成される量子回路へこの順序で分解できる．

証明． π-Shigt ゲートと wiggle ゲートで構成される量子回路について，$U_\pi^2 = U_w^2 = I$ であり，$U_w U_\pi U_w = U_\pi U_w U_\pi$ であるので，任意の二量子ビットに対し，π-Shift ゲートと wiggle ゲートが取り得る組合わせは

$$\{I, U_\pi, U_w, U_\pi U_w, U_w U_\pi, U_\pi U_w U_\pi\}$$

となる．このことから，任意の π-Shift ゲートと wiggle ゲートで構成される量子回路が実現するユニタリ変換は π-Shift ゲートで構成される量子回路，wiggle ゲートで構成される量子回路，そして，もう一つの π-Shift ゲートで構成される量子回路の順序となる三つの量子回路で実現できる．

π-Shigt ゲートと wiggle ゲートの順序を入れ替えて π-Shift ゲートで構成される量子回路，wiggle ゲートで構成される量子回路，そして，もう一つの π-Shift ゲートで構成される量子回路という順序の三つの量子回路へ分解する（図 5.5 参照）．ここで，π-Shift ゲートと wiggle ゲートの順序を入れ替えるとき，CN ゲートを生成する場合があり，このような場合は生成された CN ゲートを入力側へ移動する (図 5.4 参照)．この CN ゲートの移動によって π-Shift ゲートと wiggle ゲートの順序は変化しない．

よって，CN ゲートで構成される量子回路，π-Shift ゲートで構成される量子回路，wiggle ゲートで構成される量子回路，そして，もう一つの π-Shift ゲートで構成される量子回路へこの順序で分解できる． ■

π-Shift ゲートで構成される量子回路について，以下の補題が成り立つ．

補題 5.3 *π-Shift* ゲートで構成され，n ビット変換 U を実現する n 入力量子回路が与えられたとき，任意の整数 $\tau \geq 0$ に対し，変換 U は補助ビット数 τn 深さ $O(n/(\tau +$

$1) + \log(\tau + 1))$ の CN ゲートと π-*Shift* ゲートで構成される量子回路で実現できる．

証明． 各 π-Shifit ゲートは可換であり，$U_\pi^2 = I$ となることから，各量子ビットは高々 $n-1$ 個の π-Shift ゲートの入力になっている．よって，補助ビットを使用しないで深さ $O(n)$ にできる．このときの各層は n ビット PS 変換となるので，補題 4.1 より，任意の整数 $\tau \geq 0$ に対し，補助ビット数 τn 深さ $O(n/(\tau+1) + \log(\tau+1))$ の CN ゲートと π-Shift ゲートで構成される量子回路で実現できる． ■

5.3 WH ゲートと CN ゲートで構成される量子回路の並列化

WH 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 5.4 WH ゲートと CN ゲートで構成され，n ビット変換 U を実現する n 入力量子回路が与えられたとき，任意の整数 $\tau \geq 0$ に対し，変換 U は補助ビット数 τn 深さ $O(n/(\tau+1) + \log(\tau+1))$ の WH ゲートと CN ゲートで構成される量子回路で実現できる．

証明． まず，補題 5.1 と 補題 5.2 より，状態が $|1\rangle$ である一補助ビットを使用して．CN ゲートで構成される量子回路，π-Shift ゲートで構成される量子回路，wiggle ゲートで構成される量子回路，もう一つの π-Shift ゲートで構成される量子回路，そして，WH ゲートで構成される一層の回路へこの順序で分解できる．

次に wiggle ゲートを WH ゲートと π-Shift ゲートへ置き換える（図 5.2 参照）．すると，wiggle ゲートで構成される量子回路は WH ゲートで構成される一層の回路，π-Shift ゲートで構成される量子回路，そして，もう一つの WH ゲートで構成される一層の回路へこの順序で分解できる．以上より，CN ゲートで構成される量子回路，π-Shift ゲートで構成される量子回路と WH ゲートで構成される一層の回路の順序の組が三つとなる．

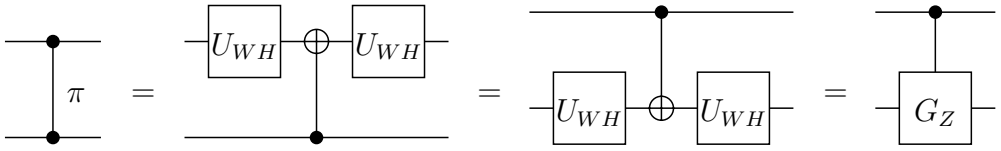

図 5.1: π-Shift ゲートと CN ゲート，WH ゲートとの関係

CN ゲートで構成される量子回路について，定理 3.6 より任意の整数 $\tau \geq 0$ に対し，補助ビット数 τn 深さ $O(n/(\tau+1)+\log(\tau+1))$ の CN ゲートで構成される量子回路で実現できる．π-Shift ゲートで構成される各量子回路について，補題 5.3 より，任意の整数 $\tau \geq 0$ に対し，補助ビット数 τn 深さ $O(n/(\tau+1)+\log(\tau+1))$ の CN ゲートと π-Shift ゲートで構成される量子回路で実現できる．ここで，π-Shift ゲートは二つの WH ゲートと一つの CN ゲートへ置き換えることができるので（図 5.1 参照），補助ビット数 τn 深さ $O(n/(\tau+1)+\log(\tau+1))$ の WH ゲートと CN ゲートで構成される量子回路で実現できる．

よって，WH ゲートと CN ゲートで構成され，ユニタリ変換 U を実現する n 入力量子回路が与えられたとき，任意の整数 $\tau \geq 0$ に対し，補助ビット数 τn 深さ $O(n/(\tau+1)+\log(\tau+1))$ の WH ゲートと CN ゲートで構成される量子回路で実現できる． ■

定理 5.4 より，以下の系が成り立つ．

系 5.5 WH ゲートと CN ゲートとで構成され，n ビット変換 U を実現する n 入力量子回路が与えられたとき，変換 U は補助ビット数 $O(n^2/\log n)$ 深さ $O(\log n)$ の WH ゲートと CN ゲートで構成される量子回路で実現できる．

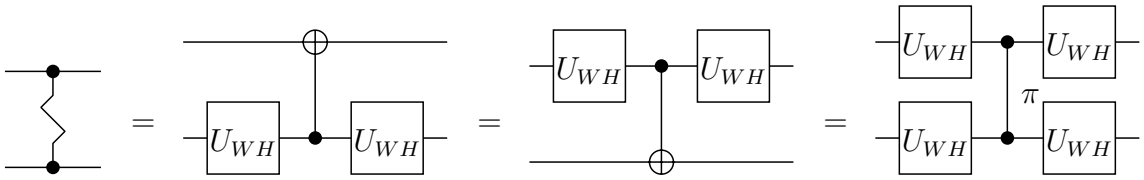

図 5.2: wiggle ゲートと CN ゲート，π-Shift ゲート及び WH ゲートとの関係

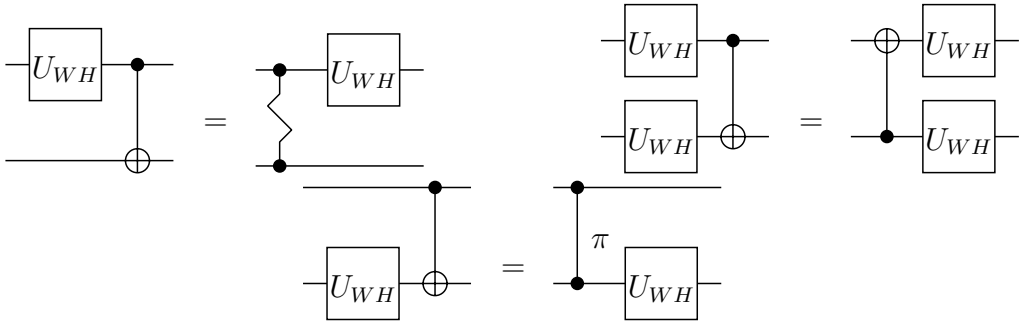

図 5.3: 出力側への WH ゲートの移動

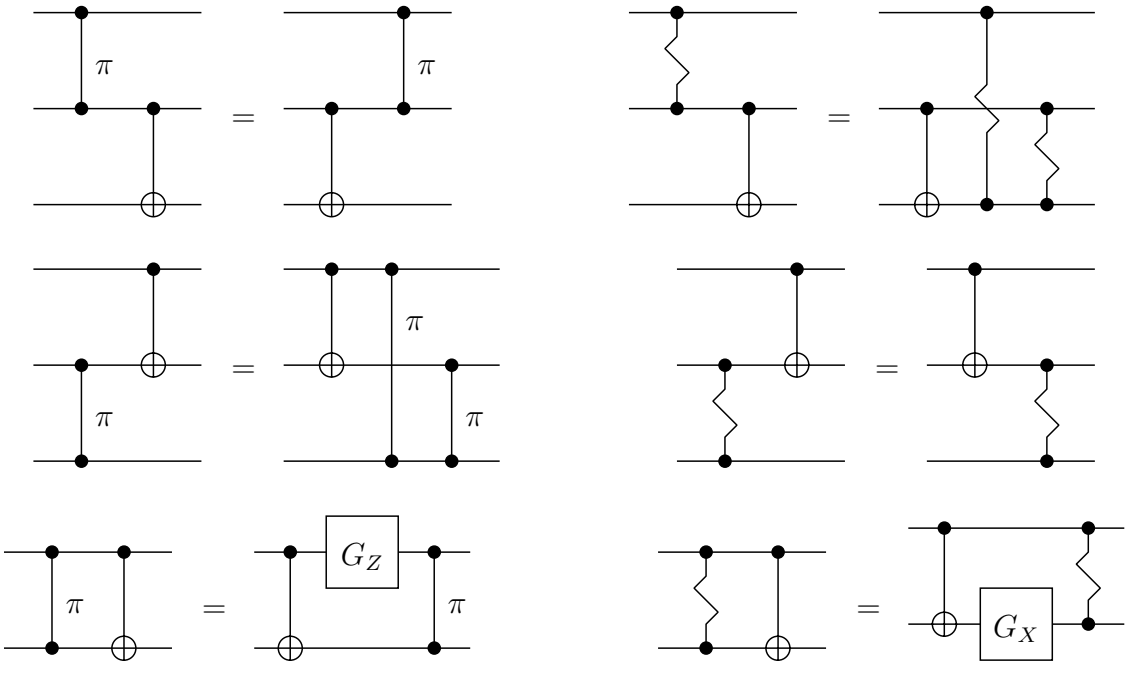

図 5.4: 入力側への CN ゲートの移動

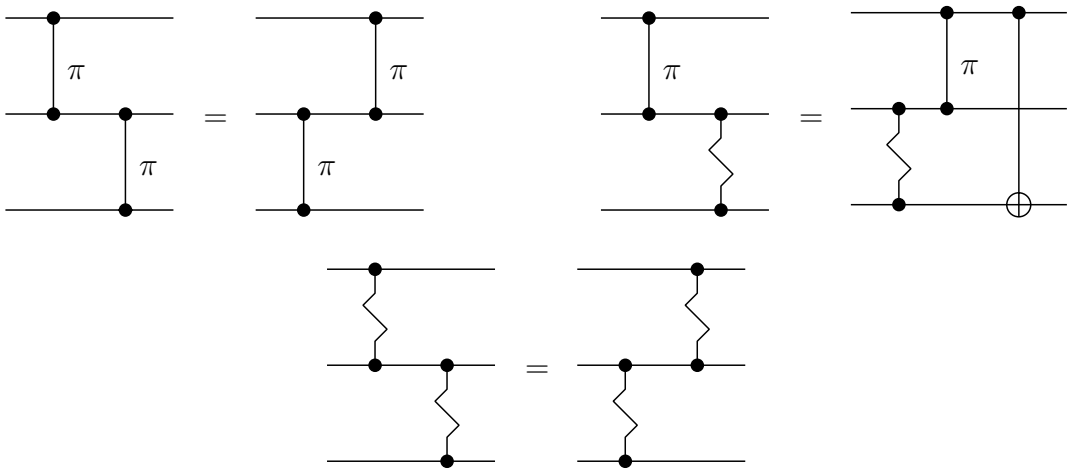

図 5.5: π-Shift ゲートと wiggle ゲートの関係

第 6 章

おわりに

本研究では，CN ゲートで構成される n 入力量子回路，s 個の l ビット PS ゲート $G_1, G_2, ..., G_s$ と CN ゲートで構成される n 入力量子回路，及び，WH ゲートと 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固定された場合の並列化手法を示した．また，この三種類の量子回路について，補助ビットを用いた並列化に関する従来研究である Moore と Nilsson [21] の結果に比べ使用する補助ビットの数を $1/\log n$ 倍に改良した．

さらに，第 4 章の定理 4.3 と系 4.4 について，各 PS ゲートの入力数について拡張することができる．定理 4.3 において，すべて PS ゲートの入力数が任意の同じ数 l に固定されていたが，各 PS ゲートの入力数はそれぞれ任意の数とする拡張を行うことができ，すべての PS ゲートの入力数の合計を L とすると，以下の定理が成り立つ．

定理 6.1 s 個の PS ゲート $G_1, G_2, ..., G_s$ と CN ゲートで構成され，n ビット変換 U を実現する n 入力量子回路が与えられたとき，すべての PS ゲートの入力数の合計を L とすると，変換 U は補助ビットを使用しないで深さ $O(sn)$，そして任意の整数 $\tau \geq 1$ に対し，補助ビット数 τn 深さ $O((L+n)/\tau + (L\log\tau)/\tau n + \log\tau)$ の s 個の PS ゲート $G_1, G_2, ..., G_s$ と CN ゲートで構成される量子回路で実現できる．

この定理より以下の系が成り立つ．

系 6.2 s 個の PS ゲート $G_1, G_2, ..., G_s$ と CN ゲートで構成され，n ビット変換 U を実現する n 入力量子回路が与えられたとき，すべての PS ゲートの入力数の合計を L とすると，変換 U は補助ビット数 $O((Ln + n^2)/\log n)$ 深さ $O(\log n + \log s)$ の s 個の PS ゲート $G_1, G_2, ..., G_s$ と CN ゲートで構成される量子回路で実現できる．

今後の課題として，本研究では各量子回路について，補助ビットを固定した場合の深さの上界を示しただけであるので下界を示すことがある．また，CN ゲートで構成される n 入力量子回路について，補助ビットを含めた入力数と深さの積が $\Theta(n^2)$ となると予想しているので，この予想が正しいことを示すことがある．そして，扱う一ビット量子ゲートの種類を増やし，扱える量子ゲートのクラスを universal にすることがある．

謝辞

本研究を行なうに当たり, 終始御指導を賜わった平石 邦彦助教授に深謝致します.

また, 日頃から有益な御助言をいただき, 多面に渡って励ましていただいたブラッハ・平石研究室 助手 宋 少秋博士に感謝致します.

最後に, 本論文をまとめるに当たって御協力いただいたブラッハ・平石研究室の諸兄に厚く御礼申し上げます.

参考文献

[1] A. Barenco, "A universal two-bit gate for quantum computation", preprint, 1994.

[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] D. Beckman, A.N. Chari, A. Devabhaktuni, and J. Preskill "Efficient networks for quantum factoring", lanl e-print quant-ph/9602016, 1996.

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

[5] D. Biron, O. Biham, E. Biham, M. Grassl, and D. Lidar, "Generalized Grover Search algorithm for arbitrary initial amplitude distribution", Proc. of the 1st NASA International Conference on Quantum Computing and Quantum Communications, 1998 (available at lanl e-print quant-ph/9801066).

[6] M. Boyer, G. Brassard, P. Hoyer, and A. Tapp, "Tight bounds on quantum searching", Proc. Phys. Comp. 1996 (available at lanl e-print quant-ph/9605034).

[7] G. Brassard, R. Hoyer, and A. Tapp, "Quantum counting", lanl e-print quant-ph/9805082, 1998.

[8] I. Chuang, R. Laflamme, P. Shor, and W. Zurek, "Quantum computers, factoring, and decoherence", lanl e-print quant-ph/9503007, 1995.

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

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

[11] D. Deutsch, A. Barenco, and A. Ekert, "Universality in quantum computation", submitted to Proc. Roy. Soc. London Ser. 1995.

[12] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation", Proc. Roy. Soc. London Ser. A **439**, pp.553–558, 1992.

[13] D.P. DiVincenzo, "Two-bit gates are universal", Phys. Rev. A **50**, pp.1015, 1995.

[14] R.P. Feynman, "Simulating physics with computers", Int. J. Theor. Phys. ,wol. 21,nos. 6/7, pp.467–488, 1982.

[15] L.K. Grover, "Quantum mechanics helps in searching for a needle in a haystack", Phys. Rev. Lett. **78** (2), pp.325–328, 1997 (available at lanl e-print quant-ph/9605043).

[16] L.K. Grover, "A framework for fast quantum mechanical algorithms", Proc. 30th ACM Symp. on Theory of Computing, pp. 53–63, 1998.

[17] L.K. Grover, "Rapid sampling through quantum computing", lanl e-print quant-ph/9912001, 1999.

[18] S. Lloyed, "Almost any quantum logic gate is universal", preprint, 1994.

[19] Y.I. Manin, "Classical computing, quantum computing, and Shor's factoring algorithm", lanl e-print quant-ph/9903008, 1999.

[20] C. Moore, "Quantum circuits : fanout, parity, and counting", manuscript, 1999 (available at lanl e-print quant-ph/9903046).

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

[22] P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum camputer", SIAM J. comput. **26** (5), pp.1484–1509, 1997.

[23] D.R. Simon, "On the power of quantum computation", SIAM J. Comput., **26** (5), pp. 1474–1483, Oct. 1997.

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

[25] C. Zalka, "Fast versions of Shor's quantum factoring algorithm", Proc. 34th Annual IEEE Symp. on Foundations of Computer Science, pp.352–361, 1993.

本研究に関する発表論文

[1] 安倍 秀明, 宋 少秋, ”2-Toffoli 量子回路の深さと補助ビットについて”, 電子情報通信学会 第 2 回量子情報技術研究会資料, 大阪大学, pp. 39–43, November, 1999.

[2] 安倍 秀明, 宋 少秋, ”Phase-Shift と Controlled-Not で構成される量子回路について”, In 情報基礎理論ワークショップ論文集, 京大数解研, January, 2000. 2000 年冬の LA シンポジウム.

[3] 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」, March, 2000. (発表予定)