備忘録：量子コンピュータ入門（第2版）
宮野健次郎・古澤　明　共著

伊藤榮信

2020年2月27日

第4章　量子論理ゲート

練習問題

4.1　　制御 NOT ゲートの行列表現

制御ビット $|\psi_1\rangle$ と標的ビット $|\psi_2\rangle$ の直積状態を $|\psi_1\rangle \otimes |\psi_1\rangle = |\psi_1\psi_2\rangle$ と書くとして $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ を基底とする制御 NOT ゲートの表現を書け.

（解答）

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

とする．制御 NOT ゲートは

$$|00\rangle \to |00\rangle, |01\rangle \to |01\rangle, \ \ |10\rangle \to |11\rangle, \ \ |11\rangle \to |10\rangle$$

と状態を変化させるので，このように変化させる行列は

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

である．この行列と状態を表す 4 つの縦ベクトルとの積を計算し制御 NOT ゲートの状態変化を確認すればよい.

4.2　　制御ユニタリーゲートの行列表現

前問と同じ基底をとったときの制御ユニタリーゲートの表現を作れ.

（解答）　制御ユニタリゲートは制御ビットが 0 の場合，標的ビットはそのまま通過し，制御ビットが 1 の場合，標的ビットはユニタリー変換を受ける．この条件を満たす行列は

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{21} \\ 0 & 0 & U_{12} & U_{22} \end{pmatrix}$$

テキストでの解答は行で書いて $U_{11}\ \ U_{12}$, 次の行 $U_{21}\ \ U_{22}$ であるがユニタリー変換行列のサフィックスを表現するには上記の方が良いと思う．$|10\rangle$ のユニタリー変換は

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{21} \\ 0 & 0 & U_{12} & U_{22} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ U_{11} \\ U_{12} \end{pmatrix} = U_{11} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + U_{12} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

となるので，標的ビットだけを取り出すと

$$|0\rangle' = U_{11}|0\rangle + U_{12}|1\rangle$$

同様にこの行列と $|11\rangle$ との積を計算することで

$$|1\rangle' = U_{21}|0\rangle + U_{22}|1\rangle$$

を得るから，制御ユニタリーゲートの表現を得た．

4.3 スワップゲート

量子ビットを入替える操作 $|\psi_1\psi_2\rangle \to |\psi_2\psi_1\rangle$ の表現を書け．
スワップゲートを表す図 4.7 の制御 NOT ゲートを順次作用させることは問題 4.1 で得た制御 NOT ゲートの行列表現の積により得られることを確かめよ．
（解答）

$$|00\rangle \to |00\rangle,\ \ |01\rangle \to |10\rangle,\quad |10\rangle \to |01\rangle,\quad |11\rangle \to |11\rangle$$

と状態を変化させるので，このように変化させる行列は

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

となる．

次に，制御 NOT ゲート行列の積により得られることの確認を行う．まず図 4.7 の中央の逆さまの制御 NOT ゲートは以下のような変換を表している．

$$|00\rangle \to |00\rangle,\ \ |10\rangle \to |10\rangle,\quad |01\rangle \to |11\rangle,\quad |11\rangle \to |01\rangle$$

これを表現する行列は

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

よって図 4.7 の制御 NOT ゲート行列の積は

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

4.3 図 4.15 の量子回路の等値性の確認

（解答）(b) の 2 量子ビットのアダマールゲートの行列表現を考える．このアダマール変換行列を H とすると

$$H|00\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{2}\Big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\Big)$$

$$H|01\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{2}\Big(|00\rangle - |01\rangle + |10\rangle - |11\rangle\Big)$$

$$H|10\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{2}\Big(|00\rangle + |01\rangle - |10\rangle - |11\rangle\Big)$$

$$H|11\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{2}\Big(|00\rangle - |01\rangle - |10\rangle + |11\rangle\Big)$$

となるから H は

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

で表現される．よって，図の回路の行列の積による表現は

$$\frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$= \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

第5章　ショアのアルゴリズム

5.1　公開鍵暗号

$$\begin{aligned} P &= 10011001001111110101101000101_{(2)} \\ &= 160688965_{(10)}, \qquad (5.1) \\ C &= P^e \mod M \\ &= 160688965^e \mod M, \qquad (5.2) \end{aligned}$$

フェルマーの小定理：

g が素数 p の倍数でないとき, $g^{p-1} \mod p = 1$ が成り立つ.

証明（Web 上にはあちらこちらにあるが念のため）:
本題の証明の準備のために

$$g^p \mod p = g, \qquad (5.2.1)$$

であることを帰納法により証明しておく.
g は整数であるので帰納法の第 1 である $g = 1$ の場合を考える. 明らかに

$$1^p \mod p = 1, \qquad (5.2.2)$$

となるので $g = 1$ の場合成立する. 次に $g = n$ の場合成立すると仮定する :

$$n^p \mod p = n, \qquad (5.2.3)$$

$g = n + 1$ の場合を考える. 2 項定理より

$$(n+1)^p = n^p + 1 + \sum_{j=1}^{p-1} {}_pC_j n^j$$

と展開できるから

$$(n+1)^p \mod p = (n^p + 1) \mod p \equiv n + 1, \qquad (5.2.4)$$

となる．ここで

$$ {}_pC_j = p\frac{(p-1)\cdots(p-j+1)}{j!} $$

であることと (5.2.3) を使った．よって帰納法のルール (5.2.2)-(5.2.4) により (5.2.1) が成立することが分かる．

次に，g が p の倍数でないとき，(5.2.1) の両辺を g で割るとフェルマーの小定理が証明された．ここで注意すべきは g が p の倍数でないことである．実際，自明ではあるが $g = kp$ とすると $g^{p-1} = (kp)^{p-1}$ は p の倍数となるから余りはゼロである：$(kp)^{p-1} \mod p = 0$ となる． □

$$
\begin{aligned}
C^d \mod M &= (P^e)^d \mod M \\
&= P^{ed} \mod M \\
&= P^{k(p-1)(q-1)+1} \mod M, \\
&= P \cdot P^{k(p-1)(q-1)} \mod M = pq, \qquad (5.3.1) \\
&= P \mod M, \qquad (5.3)
\end{aligned}
$$

となる．

//

伊藤注：(5.3.1) から (5.3) を導出する．まず mod 計算の基本的な性質を以下に記しておく．

性質 1：

$$ (A \cdot B) \mod p = [(A \mod p) \cdot (B \mod p)] \mod p $$

確認：$A = kp+i, B = hp+j$ とすると $(A\cdot B) \mod p = [(kp+i)(hp+j)] \mod p = [khp^2 + (k+h)p + ij] \mod p = ij \mod p$ である．一方 $[(A \mod p)\cdot(B \mod p)] \mod p = (ij) \mod p$ となり等号が成立する．

性質 2：

$$ A \mod q = A \mod kq $$

確認：$A = kq+i$ とすると $A \mod q \equiv i$ であり，$A \mod (kq) = [s(kq)+j] \mod q = (skq+j) \mod kq \equiv j$ となるが，明らかに $i = j$ であるので上記等号が成立する．

(5.3.1) 式のように上の式を 2 つの積に書き換え，さらに上記性質 1 により，まずは $P^{k(p-1)(q-1)} \mod M$ を考える．$P^{(p-1)} = B$ とする（B は M の倍数ではないとする）．よって $P^{k(p-1)(q-1)} \mod M = (B^{q-1})^k \mod M$ と書き換えられる．$(B^{q-1})^k$ については B^{q-1} の k 個の積と考え上記性質 1 を使う．$M = pq$ なので上記性質 2 より $B^{q-1} \mod M = B^{q-1} \mod q \equiv 1$ となり，よって $P\cdot 1^k \mod M = P\cdot 1 \mod M = P \mod M$ を得る．□

//

5.2 量子離散的フーリエ変換

5.2.1 量子離散的フーリエ変換の定義

時間Tごとに離散的に，物理量xを測定し，そのjT; $(j = 0, 1, \cdots, N-1)$での測定値をx_jとする．このとき意味のある周波数は$k/(NT)$となる．ただし$k = 0, 1, \cdots, N-1$とする．
物理空間x_jから周波数空間y_kへの離散的フーリエ変換の定義

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \mathrm{e}^{\mathrm{i}2\pi jk/N}, \tag{5.8}$$

正規直交基底（状態）ベクトルの変換

$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \mathrm{e}^{\mathrm{i}2\pi jk/N} |k\rangle, \tag{5.9}$$

を定義する[1]．

5.2.2 量子離散的フーリエ変換の量子回路

10進数表現状態$|j\rangle (j = 0, 1, 2, \cdots, N-1)$を量子ビットで表すため，10進数表現の$j$を2進数$j_1 \cdot 2^{n-1} + j_2 \cdot 2^{n-2} + \cdots + j_n \cdot 2^0 (j_m = 0, 1, N = 2^n)$を用いると，

$$|j\rangle = |j_1 j_2 \cdots j_n\rangle = |j_1\rangle \otimes |j_2\rangle \otimes \cdots |j_n\rangle$$

2進数で少数を表す方法の定義：

$$0.j_1 j_2 \cdots j_m = \frac{j_1}{2^1} + \frac{j_2}{2^2} + \cdots + \frac{j_m}{2^m}, \tag{5.15}$$

以下

$$j = j_1 \cdot 2^{n-1} + j_2 \cdot 2^{n-2} + \cdots + j_n \cdot 2^0,$$
$$k = k_1 \cdot 2^{n-1} + k_2 \cdot 2^{n-2} + \cdots + k_n \cdot 2^0$$

である．

//
(5.16) 式の確認；量子離散的フーリエ変換

$$|j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \mathrm{e}^{\mathrm{i}2\pi jk/2^n} |k\rangle$$

[1]伊藤注：量子コンピュータでは必ずこの離散的フーリエ変換を定義した後にこの状態の変換を定義するが，量子力学的にはストレートに状態の変換をこの形で定義すればよいのではないかと思われる．離散フーリエ変換を持ち出すのは変換式に$\exp(\mathrm{i}2\pi jk/N)$が現れるからだけの理由である．

で

$$\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}\mathrm{e}^{\mathrm{i}2\pi jk/2^n}|k\rangle = \frac{1}{\sqrt{2^n}}\Big(\,|0\rangle+\mathrm{e}^{\mathrm{i}2\pi j2^{n-1}/2^n}|1\rangle\Big)$$
$$\otimes\Big(\,|0\rangle+\mathrm{e}^{\mathrm{i}2\pi j2^{n-1}/2^n}|1\rangle\Big)\otimes\cdots\otimes\Big(\,|0\rangle+\mathrm{e}^{\mathrm{i}2\pi j2^{0}/2^n}|1\rangle\Big) \qquad (*)$$

と積の形で書けることを $n=3$ の場合に確かめる．
(*) 式の最左辺は $1/\sqrt{2^3}$ を外して

$$\sum_{k=0}^{7}\mathrm{e}^{\mathrm{i}2\pi jk/2^3}|k\rangle = \mathrm{e}^{\mathrm{i}2\pi j0/8}|0\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot1/8}|1\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot2/8}|2\rangle$$
$$+\mathrm{e}^{\mathrm{i}2\pi j\cdot3/8}|3\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot4/8}|4\rangle+\cdots+\mathrm{e}^{\mathrm{i}2\pi j\cdot7/8}|7\rangle \qquad (**)$$

である．一方，(*) 式右辺は

$$\Big(\,|0\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot2^2/2^3}|1\rangle\Big)\otimes\Big(\,|0\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot2^1/2^3}|1\rangle\Big)\otimes\Big(\,|0\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot2^0/2^3}|1\rangle\Big)$$
$$=\Big(\,|0\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot4/8}|1\rangle\Big)\otimes\Big(\,|0\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot2/8}|1\rangle\Big)\otimes\Big(\,|0\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot1/8}|1\rangle\Big)$$
$$=\Big(\,|0\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot4/8}|1\rangle\Big)$$
$$\otimes\Big(\,|00\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot1/8}|01\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot2/8}|10\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot(1/8+2/8)}|11\rangle\Big)$$
$$=|000\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot1/8}|001\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot2/8}|010\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot3/8}|011\rangle$$
$$+\mathrm{e}^{\mathrm{i}2\pi j\cdot4/8}|100\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot5/8}|101\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot6/8}|110\rangle+\mathrm{e}^{\mathrm{i}2\pi j\cdot7/8}|111\rangle \qquad (***)$$

となり，(**) 式と (***) は同じである．
また，例えば (***) 式の最後の項

$$\mathrm{e}^{\mathrm{i}2\pi j\cdot7/8}|111\rangle=\mathrm{e}^{\mathrm{i}2\pi j\cdot(1/2+1/2^2+1/2^3)}|111\rangle$$

であるから，(5.16) 式の 2 行目の成立も確認できる．
//

$$|j\rangle\to\frac{1}{\sqrt{2^n}}\sum_{k=0}^{N-1}\mathrm{e}^{\mathrm{i}2\pi jk/2^n}|k\rangle$$
$$=\frac{1}{\sqrt{2^n}}\sum_{k_1=0}^{1}\sum_{k_2=0}^{1}\cdots\sum_{k_n=0}^{1}\mathrm{e}^{\mathrm{i}2\pi j(k_1\cdot2^{n-1}+k_2\cdot2^{n-2}+\cdots+k_n\cdot2^0)/2^n}|k_1k_2\cdots k_n\rangle$$
$$=\frac{1}{\sqrt{2^n}}\sum_{k_1=0}^{1}\sum_{k_2=0}^{1}\cdots\sum_{k_n=0}^{1}\mathrm{e}^{\mathrm{i}2\pi j\left(\frac{k_1}{2}+\frac{k_2}{2^2}+\cdots+\frac{k_n}{2^n}\right)}|k_1k_2\cdots k_n\rangle$$

注：//////////指数部計算////////////////////////////////

$$
\begin{aligned}
&j\left(\frac{k_1}{2}+\frac{k_2}{2^2}+\cdots+\frac{k_n}{2^n}\right)\\
&=(j_1\cdot 2^{n-1}+j_2\cdot 2^{n-2}+\cdots+j_n\cdot 2^0)\left(\frac{k_1}{2}+\frac{k_2}{2^2}+\cdots+\frac{k_n}{2^n}\right)\\
&=j_1k_1\cdot 2^{n-2}+j_2k_1\cdot 2^{n-3}+\cdots+j_{n-1}k_1+j_nk_1\cdot\frac{1}{2}\\
&+j_1k_2\cdot 2^{n-3}+j_2k_2\cdot 2^{n-4}+\cdots+j_{n-1}k_2\cdot\frac{1}{2}+j_nk_2\cdot\frac{1}{2^2}\\
&+\cdots\\
&+j_1k_n\cdot\frac{1}{2}+j_2k_n\cdot\frac{1}{2^2}+\cdots+j_{n-1}k_n\cdot\frac{1}{2^{n-1}}+j_nk_n\cdot\frac{1}{2^n}
\end{aligned}
$$

ここで $\mathrm{e}^{\mathrm{i}2\pi n}=1$ であることを使うと，上記指数が整数となる項は全て 1 となるのでそれらを取り除くと指数部は以下のようになる：

$$
\begin{aligned}
&=0.j_n\cdot k_1+0.j_{n-1}j_n\cdot k_2+\cdots+0.j_1j_2\cdots j_n\cdot k_n\\
&=\frac{1}{\sqrt{2^n}}\sum_{k_1=0}^{1}\sum_{k_2=0}^{1}\cdots\sum_{k_n=0}^{1}\mathrm{e}^{\mathrm{i}2\pi 0.j_n\cdot k_1}|k_1\rangle\otimes\mathrm{e}^{\mathrm{i}2\pi 0.j_{n-1}j_n\cdot k_2}|k_2\rangle\otimes\cdots\otimes\mathrm{e}^{\mathrm{i}2\pi 0.j_1j_2\cdots j_n\cdot k_n}|k_n\rangle\\
&=\frac{1}{\sqrt{2^n}}\Big(|0\rangle+\mathrm{e}^{\mathrm{i}2\pi 0.j_n}|1\rangle\Big)\otimes\Big(|0\rangle+\mathrm{e}^{\mathrm{i}2\pi 0.j_{n-1}j_n}|1\rangle\Big)\otimes\cdots\\
&\qquad\otimes\Big(|0\rangle+\mathrm{e}^{\mathrm{i}2\pi 0.j_1j_2\cdots j_n}|1\rangle\Big),
\end{aligned}
\tag{5.16}
$$

図 5.2 の量子離散的フーリエ変換の量子回路で最後のスワップ器を通過する直前の状態は

$$
\frac{1}{\sqrt{2^n}}\Big(|0\rangle+\mathrm{e}^{\mathrm{i}2\pi 0.j_1j_2\cdots j_n}|1\rangle\Big)\otimes\Big(|0\rangle+\mathrm{e}^{\mathrm{i}2\pi 0.j_2\cdots j_n}|1\rangle\Big)\otimes\cdots\Big(|0\rangle+\mathrm{e}^{\mathrm{i}2\pi 0.j_n}|1\rangle\Big),
\tag{5.29}
$$

(5.16) と (5.29) 式では左から第 1 量子ビット，第 2 量子ビットという順序で第 n 量子ビットまで並んでいる．量子離散的フーリエ変換後の (5.16) は図 5.2 の量子離散的フーリエ変換の量子回路を通過後の (5.29) とは逆となっているので最後にスワップ器を通過させる必要がある．

5.3 位相推定問題

位相推定問題とは以下で定義される．

U をユニタリー演算子として

$$
U|u\rangle=\mathrm{e}^{\mathrm{i}2\pi\phi}|u\rangle,
\tag{5.39}
$$

のとき，$\phi(0 \leq \phi < 1)$ を求める．ここで ϕ を 2 進数で表すと $0.\phi_1\phi_2\cdots\phi_n$ であるとする．

制御 U^{2^k} ゲートは制御ビットが 1 のとき，以下のように $|u\rangle$ を変換する：

$$|u\rangle \longrightarrow U^{2^k}|u\rangle = \mathrm{e}^{\mathrm{i}2\pi 2^k\phi}|u\rangle, \tag{5.41}$$

したがって，制御 U^{2^k} ゲートを各量子ビットを通過した後の全体の状態は

$$\frac{1}{\sqrt{2^n}}\Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi 2^{n-1}\phi}|1\rangle\Big)\otimes\Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi 2^{n-2}\phi}|1\rangle\Big)\otimes\cdots\otimes\Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi 2^{0}\phi}|1\rangle\Big)\,|u\rangle, \tag{5.42}$$

となる．

式 (5.42) は以下のように書くことができる：

$$\frac{1}{\sqrt{2^n}}\Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi 0.\phi_n}|1\rangle\Big)\otimes\Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi 0.\phi_{n-1}\phi_n}|1\rangle\Big)\otimes\cdots$$

$$\cdots\otimes\Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi 0.\phi_1\phi_2\cdots\phi_n}|1\rangle\Big)\,|u\rangle, \tag{5.43}$$

//

(5.42) 式と (5.43) 式の一致確認

$$\phi = \frac{\phi_1}{2} + \frac{\phi_2}{2^2} + \cdots + \frac{\phi_n}{2^n} = 0.\phi_1\phi_2\cdots\phi_n$$

とする．ここで $\phi_i = 0$ または 1 の整数である．

$n = 3$ の場合の (5.42) 式：（$|u\rangle$ と規格化係数は外す）
よって

$$\phi = \frac{\phi_1}{2} + \frac{\phi_2}{2^2} + \frac{\phi_3}{2^3} = 0.\phi_1\phi_2\phi_3$$

$$\Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi 2^2\phi}|1\rangle\Big)\otimes\Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi 2^1\phi}|1\rangle\Big)\otimes\Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi 2^0\phi}|1\rangle\Big)$$

$$= \Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi(2\phi_1+\phi_2+\phi_3/2)}|1\rangle\Big)\otimes\Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi(\phi_1+\phi_2/2+\phi_3/2^2)}|1\rangle\Big)$$

$$\otimes\Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi(\phi_1/2+\phi_2/2^2+\phi_3/2^3)}|1\rangle\Big)$$

ここで $2\phi_1, \phi_1, \phi_2$ は全て整数であり，$\mathrm{e}^{\mathrm{i}2\pi m} = 1$ であるから，上の式の第 1 と第 2 因子を書き換えると

$$= \Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi\phi_3/2}|1\rangle\Big)\otimes\Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi(\phi_2/2+\phi_3/2^2)}|1\rangle\Big)$$

$$\otimes\Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi(\phi_1/2+\phi_2/2^2+\phi_3/2^3)}|1\rangle\Big)$$

$$= \Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi 0.\phi_3}|1\rangle \Big) \otimes \Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi 0.\phi_2\phi_3}|1\rangle \Big) \otimes \Big(|0\rangle + \mathrm{e}^{\mathrm{i}2\pi 0.\phi_1\phi_2\phi_3}|1\rangle \Big)$$

となり，これは (5.43) 式で $n = 3$ とした場合になっている．
//

5.4 位数計算

(5.54) 式で使われた計算式の確認

$$\frac{1}{r}\sum_{j=0}^{r-1}\left(\sum_{s=0}^{r-1}\mathrm{e}^{-\mathrm{i}2\pi j\cdot s/r}\right)|x^j \mod M\rangle = \frac{1}{r}\sum_{j=0}^{r-1}\Big(r\delta_{j0}\Big)|x^j \mod M\rangle$$

上の式での s に関する和について念のため確認しておく．$j \neq 0$ の場合，s に関する和を具体的に書くと (その和を S と書く)

$$S = \sum_{s=0}^{r-1}\mathrm{e}^{-\mathrm{i}2\pi j\cdot s/r} = 1 + \mathrm{e}^{-\mathrm{i}2\pi j\cdot 1/r} + \mathrm{e}^{-\mathrm{i}2\pi j\cdot 2/r} + \cdots + \mathrm{e}^{-\mathrm{i}2\pi j\cdot (r-1)/r} \quad (*)$$

これは初項が 1 で公比が $\mathrm{e}^{-\mathrm{i}2\pi j\cdot 1/r} \neq 1$ の等比数列である．よってその和の公式より

$$S = \frac{\mathrm{e}^{-\mathrm{i}2\pi j\cdot r/r} - 1}{\mathrm{e}^{-\mathrm{i}2\pi j\cdot 1/r} - 1} = \frac{\mathrm{e}^{-\mathrm{i}2\pi j} - 1}{\mathrm{e}^{-\mathrm{i}2\pi j\cdot 1/r} - 1} = \frac{1-1}{\mathrm{e}^{-\mathrm{i}2\pi j\cdot 1/r} - 1} = 0$$

ここで j は整数であるから，分子の $\mathrm{e}^{-\mathrm{i}2\pi j} = 1$ となるから全体でゼロとなる．一方，$j = 0$ の場合，(*) 式からもわかるように s に関する和で，すべての項が 1 となるので $S = r$ となる．これを式の形で書くと $S = r\delta_{j0}$ と書くことができる．

5.5 ショアのアルゴリズムの実際

追記：整数 M の因数分解の一方法

I) 整数 M の約数でないある整数 x を選択する．約数かそうでないかの判定にははユークリッドの互除法を使用する．
II) x^r を計算し，これを M で割った余りが 1 となる r を決定する．
III) 探し出された x^r から 1 をひいた数 $x^r - 1$ は M の倍数である．例えば M は素数 p, q の積であったとすると

$$x^r - 1 = (x^{r/2} - 1)(x^{r/2} + 1) = nM(= npq)$$

と書くことができる．ここで n は整数とする．
IV) この式から $x^{r/2}-1$ と M の公約数には p もしくは q が含まれている可能性がある．この公約数の求める方法としてはユークリッドの互除法を使う．同様に $x^{r/2}+1$ に対しても M との公約数を求める．
V) 以上の IV) で因数分解 $M=pq$ を決定する．

以上では手順の II) における r 探索に計算量が増大となることが分かっている．

第7章　量子テレポーテーション

7.1　光を用いた量子テレポーテーション実験の意義

$$|\Psi_2\rangle = c_0 \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}} + c_1 \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|10\rangle + |01\rangle}{\sqrt{2}}, \quad (7.1)$$

上の式の c_0 項で第 1 量子ビットは

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

で，更に

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

の中の，$0,0$ が第 2，第 3 量子ビットであり，同じく $1,1$ が第 2，第 3 量子ビットである．

練習問題

7.1　(7.1) 式で制御 X ゲートを通過すると

$$c_0 \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle + c_1 \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |1\rangle, \quad (A.36)$$

となる．

テキストでは制御ビットと標的ビットとしての制御 X ゲート（パウリゲート）の働きが明確に定義されていないと思う．その手掛かりとして 61 頁の M_1, M_2 の測定結果と状態変化との表を参考とし，以下のように判断する．

制御 X ゲート

制御ビットが 0 の場合，標的ビットは変化しない．

制御ビットが 1 の場合，標的ビットが 0 なら 1 へと変化して，標的ビットが 1 ならば 0 へと変化する．

c_0 項の場合，制御 X ゲートの制御ビットが第 2 量子ビットであり，標的ビットが第 3 量子ビットであり

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \xrightarrow{X} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle$$

と変化する．状態 $|00\rangle$ では第 2 量子ビットの制御ビットが　0　だから，第 3 量子ビットの　0　は変化しないので $|00\rangle \to |0\rangle\otimes|0\rangle$ と変化した．次に状態 $|11\rangle$ では第 2 量子ビットの制御ビットが　1　だから，第 3 量子ビットの　1　は制御 X ゲートの作用により $1 \to 0$ と変化し $|11\rangle \to |1\rangle\otimes|0\rangle$ と変化する．

念のために c_1 の項も確認する．c_1 の項は

$$\frac{|10\rangle+|01\rangle}{\sqrt{2}} \quad \xrightarrow{X} \quad \frac{|1\rangle+|0\rangle}{\sqrt{2}}\otimes|1\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes|1\rangle$$

となる．状態 $|10\rangle$ では第 2 量子ビットの制御ビットが　1　だから，制御 X ゲートの作用により $0 \to 1$ と変化し $|10\rangle \to |1\rangle\otimes|1\rangle$ と変化した．次に状態 $|01\rangle$ では第 2 量子ビットの制御ビットが　0　だから，第 3 量子ビットの　1　に制御 X ゲートは作用せず $1 \to 1$ のままで，よって $|01\rangle \to |0\rangle\otimes|1\rangle$ となる．これらから (A.36) 式を得る．

以上で制御 X ゲートを通過させた．次に Z ゲートの通過を考える．図 7.2 より今度は第 1 量子ビットが制御ビットになる．最終結果は (A.36) 式が

$$\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes(c_0|0\rangle+c_1|1\rangle), \tag{A.37}$$

と変化する．これについて考える．制御 Z ゲートの定義は 54 ページのパウリゲートの定義より

$$|0\rangle \to |0\rangle, \quad |1\rangle \to -|1\rangle$$

である．c_0 の項は明らかであるから c_1 の項だけを確認する．c_1 項は以下のように書くことができる．ただし，第 2 量子ビットには関係しないので，S と記しておく．

$$c_1\left(\frac{|0\rangle}{\sqrt{2}}\otimes S\otimes|1\rangle - \frac{|1\rangle}{\sqrt{2}}\otimes S\otimes|1\rangle\right)$$

この状態に制御 Z ゲートを作用させると

$$\xrightarrow{Z} c_1\left(\frac{|0\rangle}{\sqrt{2}}\otimes S\otimes|1\rangle - \frac{|1\rangle}{\sqrt{2}}\otimes S\otimes(-|1\rangle)\right) = c_1\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes S\otimes|1\rangle$$

が得られる．よって，全体では (A.37) 式となる．

7.2　図 7.3 で二つ目のアダマールまでは図 7.1 と同じであるので，そこまでの状態は (7.1) 式と同じである．

次に制御 NOT ゲート（制御 X ゲートと同じ）を通過すると，全体の状態は前問と同様に (A.36) すなわち

$$c_0\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes|0\rangle + c_1\frac{|0\rangle-|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes|1\rangle, \tag{A.38}$$

となり，次のアダマールゲートを通過すると，

$$c_0\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}+c_1\frac{|0\rangle-|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}, \tag{A.39}$$

となる．すなわち，第 3 量子ビットが

$$|0\rangle\to\frac{|0\rangle+|1\rangle}{\sqrt{2}},\quad |1\rangle\to\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

と変化した．更に制御 NOT ゲートを通過すると

$$\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\left(c_0\frac{|0\rangle+|1\rangle}{\sqrt{2}}+c_1\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right), \tag{A.40}$$

となる．制御 NOT ゲートは制御 X ゲートと同じ働きで，以下となる：

制御 NOT ゲート

制御ビットが 0 の場合，標的ビットは変化しない．

制御ビットが 1 の場合，標的ビットが 0 なら 1 へと変化して，標的ビットが 1 ならば 0 へと変化する．

以下 (A.39) 式の c_1 の項のみについて確かめる．ただし，図 7.3 で制御ビットは第 1 量子ビットで標的ビットは第 3 量子ビットなので，第 2 量子ビットを単に S と記しておく．制御 Z ゲート通過前の状態は以下のように書くことができる：

$$c_1\frac{|0\rangle-|1\rangle}{\sqrt{2}}\otimes S\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}=c_1\left(\frac{|0\rangle}{\sqrt{2}}\otimes S\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}-\frac{|1\rangle}{\sqrt{2}}\otimes S\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

この状態に制御 Z ゲートを作用させると

$$\xrightarrow{Z}c_1\left(\frac{|0\rangle}{\sqrt{2}}\otimes S\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}-\frac{|1\rangle}{\sqrt{2}}\otimes S\otimes\frac{|1\rangle-|0\rangle}{\sqrt{2}}\right)$$

$$=c_1\left(\frac{|0\rangle}{\sqrt{2}}\otimes S\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}+\frac{|1\rangle}{\sqrt{2}}\otimes S\otimes\frac{|0\rangle-|i\rangle}{\sqrt{2}}\right)=c_1\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes S\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

となり (A.40) が得られる．次に (A.40) 式の第 3 量子ビットにアダマールゲートを作用させると，

$$c_0\frac{1}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}+\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)+c_1\frac{1}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}-\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$=\frac{1}{2}\left(2c_0|0\rangle+2c_1|1\rangle\right)=c_0|0\rangle+c_1|1\rangle$$

従って， 図 7.3 の量子回路の出力は

$$\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes(c_0|0\rangle+c_1|1\rangle), \tag{A.37}$$

となる．