量子コンピュータと情報セキュリティ

中部大学工学部情報工学科

授業科目「卒業研究」教科書

只木孝太郎

中部大学工学部情報工学科

E-mail: tadaki@cs.chubu.ac.jp

http://www2.odn.ne.jp/tadaki/

2018 年 4 月 11 日版

目 次

第1章　量子計算のための量子力学入門 1
— 量子状態と量子測定 —

1.1　量子状態

$\mathbb{C}$ を**複素数**の集合とする。$\mathbb{C}^d$ を複素数を成分に持つ d 次元**列ベクトル**の集合とする。即ち、

$$\mathbb{C}^d = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} \middle| \, x_1, \dots, x_d \in \mathbb{C} \right\} \qquad (d = 1, 2, 3, \dots) \tag{1.1}$$

である。$\mathbb{C}^d$ は、次式で定義される和とスカラー倍により、複素ベクトル空間を成す。

$$\begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_d + y_d \end{pmatrix}, \qquad \alpha \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} = \begin{pmatrix} \alpha x_1 \\ \vdots \\ \alpha x_d \end{pmatrix} \quad (\alpha \in \mathbb{C}). \tag{1.2}$$

量子力学の公理 1 (状態空間と量子状態)**.** 任意の（有限次元の）**量子力学的系**には、複素ベクトル空間 $\mathbb{C}^d$ が対応し、その量子力学的系の**状態空間**と呼ばれる。その量子力学的系の任意の状態（**量子状態**）は、$x \neq 0$ なる或るベクトル $x \in \mathbb{C}^d$ によって表される。逆に、$x \neq 0$ なる任意のベクトル $x \in \mathbb{C}^d$ は、その量子力学的系の或る量子状態を表す。但し、0 でない二つのベクトル x と y が線型従属のとき（即ち、或る複素数 α が存在し $\alpha x = y$ となるとき）、x と y は同じ量子状態を表す。状態空間 $\mathbb{C}^d$ のベクトルを**状態ベクトル**と言うことがある。 □

以下で、**量子系**とは、量子力学的系のことである。また、量子状態のことを、単に**状態**と言うことがある。なお、量子力学では、状態ベクトルを表記するのに $|\psi\rangle, |0\rangle, |1\rangle, |+\rangle, |-\rangle$ などの記号を用いることが多い。このように表記された $\mathbb{C}^d$ のベクトル（列ベクトル）は、量子力学の習慣として、**ケットベクトル** (ket vector) と呼ばれる。

例 1.1.1 (1 qubit の量子系)**.** 1 *qubit* の量子系[1] には、状態空間として、複素ベクトル空間 $\mathbb{C}^2$ が対応する。1 *qubit* の量子系の例としては、電子のスピンについての量子系、原子核のスピンについての量子系、光の偏向についての量子系などがある。例えば、外部の一様磁場中に置かれた原子核のスピンの場合、外部磁場の向きに対し平行になっているスピン、および反平行[2] になっているスピンは、それぞれ、次式で定義される状態ベクトル $|0\rangle$、および $|1\rangle$ によって表される。

$$\text{外部磁場}\downarrow\text{に平行なスピン}\downarrow \qquad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad \text{外部磁場}\downarrow\text{に反平行なスピン}\uparrow \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1.3}$$

このとき、$|0\rangle$ と $|1\rangle$ は、（古典的な）通常の 1 ビットが取り得る *2* つの状態 0 と 1 に、それぞれ対応する。$|\theta\rangle \in \mathbb{C}^2$ を任意の状態ベクトルとすると、その成分 $x_1, x_2 \in \mathbb{C}$ を用いて、

$$|\theta\rangle = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = x_1|0\rangle + x_2|1\rangle \tag{1.4}$$

[1] qubit は “キュービット” と読む。quantum bit の略である。
[2] 外部の一様磁場の向きに対し、反対向きになっているとき、反平行であると言う。

と表され。任意の状態ベクトルは、$|0\rangle$ と $|1\rangle$ の線形結合で表現できる事がわかる。一般に、幾つかの量子状態 $|\psi_1\rangle, \ldots, |\psi_n\rangle$ の線形結合 $\alpha_1|\psi_1\rangle + \cdots + \alpha_n|\psi_n\rangle$ $(\alpha_1, \ldots, \alpha_n \in \mathbb{C})$ で表される状態を、$|\psi_1\rangle, \ldots, |\psi_n\rangle$ の重ね合わせの状態と呼ぶ。従って、1 *qubit* の量子系では、任意の状態は、$|0\rangle$ と $|1\rangle$ の重ね合わせの状態になっている。 □

A を $m \times n$ 行列（m 行 n 列行列）、B を $p \times q$ 行列（p 行 q 列行列）とする。行列 A と B の**テンソル積** $A \otimes B$ は、$mp \times nq$ 行列であり、次式で定義される。

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \ldots & a_{1n}B \\ a_{21}B & a_{22}B & \ldots & a_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \ldots & a_{mn}B \end{pmatrix}. \tag{1.5}$$

ここで、a_{ij} は行列 A の第 (i,j)-要素であり、$a_{ij}B$ は行列 B の複素数 a_{ij} によるスカラー倍を表す。例えば、例 1.1.1 の 1 qubit の量子系の場合で考察すると、

$$|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ \\ 0\begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 1 \times 0 \\ 1 \times 1 \end{pmatrix} \\ \\ \begin{pmatrix} 0 \times 0 \\ 0 \times 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ \\ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{1.6}$$

となる。

量子力学の公理 2 (量子系の合成)**.** n 個の量子系 $\mathcal{Q}_1, \mathcal{Q}_2, \ldots, \mathcal{Q}_n$ を考える。これらは全体として *1* つの量子系を構成しているとみなすことができる。この量子系は**全系**または**合成系**と呼ばれる。一方、全系を構成する個々の量子系 $\mathcal{Q}_i$ $(i = 1, \ldots, n)$ は**部分系**と呼ばれる。各 $i = 1, \ldots, n$ に対し、部分系 $\mathcal{Q}_i$ の状態空間が $\mathbb{C}^{d_i}$ であるとすると、全系の状態空間は $\mathbb{C}^{d_1 d_2 \cdots d_n}$ となる。そして、各 $i = 1, \ldots, n$ について、部分系 $\mathcal{Q}_i$ の量子状態が状態ベクトル $|\psi_i\rangle$ で表されている場合、全系の量子状態は状態ベクトル $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ で表される。逆に、全系の量子状態が状態ベクトル $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ で表されており、かつ各 $i = 1, \ldots, n$ について、$|\psi_i\rangle \in \mathbb{C}^{d_i}$ となっている場合、各 $i = 1, \ldots, n$ について、部分系 $\mathcal{Q}_i$ の量子状態は状態ベクトル $|\psi_i\rangle$ で表される。 □

例 1.1.2 (n qubit の量子系)**.** n *qubit* の量子系とは、n 個の 1 *qubit* の量子系から成る量子系のことである。1 *qubit* の量子系の状態空間は $\mathbb{C}^2$ なので、量子力学の公理 *2* より、n *qubit* の量子系には、状態空間として、複素ベクトル空間 $\mathbb{C}^{2^n}$ が対応する [3]。そして、n *qubit* の量子系で、それを構成する n 個の 1 *qubit* の量子系の量子状態が、それぞれ状態ベクトル $|b_1\rangle, |b_2\rangle, \ldots, |b_n\rangle$ $(b_1, b_2 \ldots, b_n = 0, 1)$ で表されている場合、この n *qubit* の量子系の量子状態は、量子力学の公理 *2* より、状態ベクトル

$$|b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle \tag{1.7}$$

で表される。この状態は、（古典的な）通常のビット列 $b_1 b_2 \ldots b_n$ に対応し、これを特に $|b_1 b_2 \ldots b_n\rangle$ と表す。従って、

$$|b_1 b_2 \ldots b_n\rangle = |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle \quad (b_1, b_2 \ldots, b_n = 0, 1) \tag{1.8}$$

となる。例えば 2 *qubit* の場合（$n = 2$ の場合）、このような状態ベクトルは次の具体形を持つ。

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{1.9}$$

[3] n qubit の量子系の状態空間は $\mathbb{C}^{2^n}$ であり、$\mathbb{C}^n$ ではないことに注意。

一般に、ベクトルの系列 $\{|b_1b_2\dots b_n\rangle\}_{b_1,b_2\dots,b_n=0,1}$ は線型独立であり、全部で 2^n 個のベクトルからなるので、この系列は $\mathbb{C}^{2^n}$ の基底を成す。従って、n *qubit* の量子系の任意の量子状態は、2^n 個の状態ベクトル $|b_1b_2\dots b_n\rangle$ $(b_1,b_2\dots,b_n=0,1)$ の重ね合わせの状態になっている。即ち、$|\psi\rangle$ を n *qubit* の量子系の任意の量子状態とすると、ある複素数の系列 $\{\alpha_{b_1,b_2,\dots,b_n}\}_{b_1,b_2\dots,b_n=0,1}$ が存在し、$|\psi\rangle$ は次の形に表現することが出来る。

$$|\psi\rangle = \sum_{b_1,b_2\dots,b_n=0,1} \alpha_{b_1,b_2,\dots,b_n}|b_1b_2\dots b_n\rangle. \tag{1.10}$$

これは、式 (1.4) の一般化になっている。 □

問 1. 式 (1.9) が成り立つことを、テンソル積の定義に基づいて確認せよ。 □

1.2 量子測定: 全系に対する測定

複素数を要素として持つ任意の $m\times n$ 行列

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \tag{1.11}$$

に対し、A の**随伴行列** $A^\dagger$ は、$n\times m$ 行列であり、次式で定義される：

$$A^\dagger = \begin{pmatrix} \overline{a}_{11} & \dots & \overline{a}_{m1} \\ \vdots & & \vdots \\ \overline{a}_{1n} & \dots & \overline{a}_{mn} \end{pmatrix}. \tag{1.12}$$

但しここで、複素数 α の共役複素数を $\overline{\alpha}$ で表している。なお、随伴行列 (adjoint matrix) は共役転置行列とも呼ばれる [4]。例えば、

$$|\psi\rangle = \begin{pmatrix} i \\ 2 \end{pmatrix} \in \mathbb{C}^2 \tag{1.13}$$

のとき、$|\psi\rangle^\dagger = (-i, 2)$ となり、$|\psi\rangle^\dagger$ は行ベクトルになる。

問 2. 次が成り立つことを確認せよ。

$$(A^\dagger)^\dagger = A, \quad (A+B)^\dagger = A^\dagger + B^\dagger, \quad (\alpha A)^\dagger = \overline{\alpha}A^\dagger \ \ (\text{ここで } \alpha \text{ は任意の複素数}),$$
$$(BA)^\dagger = A^\dagger B^\dagger, \quad I^\dagger = I \ \ (\text{ここで } I \text{ は恒等行列（単位行列）}).$$

□

量子力学の習慣として、列ベクトルがケットベクトルの表記法で $|\phi\rangle$ と表されているときには、行ベクトル $|\phi\rangle^\dagger$ を $\langle\phi|$ と書き表す。逆に、行ベクトルが $\langle\phi|$ と表されているときには、列ベクトル $\langle\phi|^\dagger$ をケットベクトルの表記法で $|\phi\rangle$ と書き表す。このように、量子力学では、行ベクトルを表記するのに $\langle\psi|, \langle 0|, \langle 1|, \langle +|, \langle -|$ などの記号を用いることが多く、このように表記された行ベクトルは、習慣として、**ブラベクトル** (bra vector) と呼ばれる。従って、次が成り立つ。

$$\langle\phi| = |\phi\rangle^\dagger, \qquad |\phi\rangle = \langle\phi|^\dagger. \tag{1.14}$$

[4] 記号 † は “ダガー” (dagger) と読む。

問 3. 問 *2* の関係式を用い、次の同値性を証明せよ。

$$|\theta\rangle = \alpha|\psi\rangle + \beta|\phi\rangle \Longleftrightarrow \langle\theta| = \overline{\alpha}\langle\psi| + \overline{\beta}\langle\phi|. \tag{1.15}$$

□

複素ベクトル空間 $\mathbb{C}^d$ は、次式で定義される**内積** (x, y) を導入することにより、**内積空間**（**計量線型空間**、**ユークリッド線型空間**、**前ヒルベルト空間**）となる [5]。

$$(x, y) = x^\dagger y \qquad (x, y \in \mathbb{C}^d). \tag{1.16}$$

問 4. 任意の $x, y, z \in \mathbb{C}^d$ と複素数 α に対して、次が成り立つことを証明せよ。

(i) $(x, x) \geq 0$, かつ $(x, x) = 0 \Longleftrightarrow x = 0$,

(ii) $(x, \alpha y) = \alpha(x, y)$, かつ $(\alpha x, y) = \overline{\alpha}(x, y)$,

(iii) $(x, y + z) = (x, y) + (x, z)$, かつ $(x + y, z) = (x, z) + (y, z)$,

(iv) $\overline{(x, y)} = (y, x)$. □

ベクトル $v \in \mathbb{C}^d$ が**規格化されている**とは、$(v, v) = 1$ が成り立つことである。$v_1, \ldots, v_d$ が $\mathbb{C}^d$ の**正規直交基底**であるとは、$v_1, \ldots, v_d$ が $\mathbb{C}^d$ の基底であり、かつ任意の $j, k = 1, \ldots, d$ に対し $(v_j, v_k) = \delta_{jk}$ が成り立つことを言う。ここで、δ_{jk} はクローネッカーの δ であり、次のように定義される：数 j, k が等しい場合（$j = k$ の場合）には $\delta_{jk} = 1$ であるが、数 j, k が異なっている場合（$j \neq k$ の場合）には $\delta_{jk} = 0$ となる。

なお、量子力学の習慣として、$\mathbb{C}^d$ のベクトルが、ケットベクトルの表記法で $|\phi\rangle, |\psi\rangle$ と表されているときには、$(|\phi\rangle, |\psi\rangle)$ を $\langle\phi|\psi\rangle$ と書く。従って、

$$\langle\phi|\psi\rangle = (|\phi\rangle, |\psi\rangle) = |\phi\rangle^\dagger|\psi\rangle = \langle\phi| \cdot |\psi\rangle \tag{1.17}$$

が成立する。ここで最後の 2 つは行列の積（d 次元行ベクトルと d 次元列ベクトルの積）である。従って、ケットベクトルとブラベクトルを用いる、この量子力学特有の記号法には、一貫性があることがわかる [6]。ゆえに例えば、ケットベクトル $|\psi\rangle \in \mathbb{C}^d$ が規格化されているとは、$\langle\psi|\psi\rangle = 1$ が成り立つことである。また、ケットベクトル $|r_1\rangle, \ldots, |r_d\rangle \in \mathbb{C}^d$ が正規直交基底であるとは、$|r_1\rangle, \ldots, |r_d\rangle$ が $\mathbb{C}^d$ の基底であり、かつ任意の $j, k = 1, \ldots, d$ に対し $\langle r_j|r_k\rangle = \delta_{jk}$ が成り立つことである。

問 5. 式 (1.17) を確認せよ。 □

問 6. 次が成り立つことを確認せよ。

(i) $\langle\psi|\psi\rangle \geq 0$, かつ $\langle\psi|\psi\rangle = 0 \Longleftrightarrow |\psi\rangle = 0$,

(ii) $\langle\phi|\{\alpha|\psi\rangle\} = \alpha\langle\phi|\psi\rangle$, かつ $\{\alpha\langle\phi|\}|\psi\rangle = \alpha\langle\phi|\psi\rangle$,

(iii) $\langle\theta|\{|\psi\rangle + |\phi\rangle\} = \langle\theta|\psi\rangle + \langle\theta|\phi\rangle$, かつ $\{\langle\psi| + \langle\phi|\}|\theta\rangle = \langle\psi|\theta\rangle + \langle\phi|\theta\rangle$,

(iv) $\overline{\langle\phi|\psi\rangle} = \langle\psi|\phi\rangle$. □

---

[5] なお、量子力学では、式 (1.16) を内積の定義とするが、数学では、式 (1.16) の代わりに、その複素共役をとり、$(x, y) = \overline{x^\dagger y}$ で内積を定義することが多いので、注意が必要である。しかし、量子力学では、内積の絶対値の二乗 $|(x, y)|^2$ の計算が主な関心事となるので（量子力学の公理 3 参照）、その場合、両者の定義の違いは問題とならない。

[6] ケットベクトル、ブラベクトルの名称は、表式 $\langle\phi|\psi\rangle$ で、bracket $\langle\cdots\rangle$ の左側の記号 '$\langle$' を bra、右側の記号 '$\rangle$' を ket と解釈することに由来する。

例 1.2.1 ($\mathbb{C}^2$ の正規直交基底)**.** 1 *qubit* の量子系の状態空間、即ち、$\mathbb{C}^2$ では、$|0\rangle$ と $|1\rangle$ が正規直交基底となっている。これは、式 (1.3) より、$(|j\rangle, |k\rangle) = |j\rangle^\dagger |k\rangle = \delta_{jk}$ $(j, k = 0, 1)$ が成り立ち（従って $\langle j|k\rangle = \delta_{jk}$ となる）、かつ $|0\rangle$ と $|1\rangle$ は明らかに線型独立であり、ゆえに $\mathbb{C}^2$ の基底となっているからである。

一方、次の *2* つのベクトルもまた、$\mathbb{C}^2$ の正規直交基底となっている。

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{1.18}$$

これは、$\langle j|k\rangle = \delta_{jk}$ から確認することが出来る。従って、

$$\langle +|+\rangle = \langle -|-\rangle = 1, \qquad \langle +|-\rangle = \langle -|+\rangle = 0 \tag{1.19}$$

となる。 □

問 7. ベクトル $|+\rangle, |-\rangle$ が $\mathbb{C}^2$ の正規直交基底となっていることを確認せよ。 □

量子力学の公理 3 (量子測定 I)**.** $\mathcal{Q}$ を状態空間が $\mathbb{C}^d$ で与えられる任意の量子系とする。そして、$|r_1\rangle, \ldots, |r_d\rangle$ を $\mathbb{C}^d$ の任意の正規直交基底とする。このとき、量子系 $\mathcal{Q}$ に対し、次の性質を持つ**量子測定**を行うことが出来る。

(i) 測定結果として、$r_1, \ldots, r_d$ のうちの、どれか一つが得られる。

(ii) 測定の直前に、量子系 $\mathcal{Q}$ の状態が、規格化されたベクトル $|\psi\rangle$ で表されていたものとする。このとき、各 $i = 1, \ldots, d$ に対し、確率 $|\langle r_i|\psi\rangle|^2$ で測定結果 r_i が得られ、その場合、測定直後の量子系 $\mathcal{Q}$ の状態は $|r_i\rangle$ で表される。 □

例 1.2.2 (1 qubit の量子系での測定)**.** 1 *qubit* の量子系に対する量子測定について考察しよう。

***(a)* 正規直交基底 $\{|0\rangle, |1\rangle\}$ についての測定**

例 1.2.1 より、$|0\rangle$ と $|1\rangle$ は正規直交基底である。1 *qubit* の量子系に対し、この基底 $|0\rangle, |1\rangle$ に関して測定を行う場合を考える。

測定直前に系の状態が $|0\rangle$ で表されていた場合、$\langle 0|0\rangle = 1, \langle 1|0\rangle = 0$ なので、$|\langle 0|0\rangle|^2 = 1, |\langle 1|0\rangle|^2 = 0$ となる。従って、量子力学の公理 *3* より、測定結果は確率 1 で 0 が得られ、測定直後の状態は $|0\rangle$ で表されることになる。これは極めて当然の結果であり、測定の前後で状態に変化は起こらない。同様に、測定直前に系の状態が $|1\rangle$ で表されていた場合、確率 1 で測定結果 1 が得られ、測定直後の状態は $|1\rangle$ で表される。従って特に、系の状態が $|0\rangle$ か $|1\rangle$ のどちらかである場合には、基底 $|0\rangle, |1\rangle$ に関して測定を行うことにより、その状態を決定できる。その上、測定によって状態に変化は生じない。

一方、測定直前に系の状態が $|+\rangle$ で表されていた場合を考えよう。この場合、

$$\langle 0|+\rangle = \langle 0| \left\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right\} = \frac{1}{\sqrt{2}} \langle 0| \{|0\rangle + |1\rangle\} = \frac{1}{\sqrt{2}}(\langle 0|0\rangle + \langle 0|1\rangle) = \frac{1}{\sqrt{2}}(1 + 0) = \frac{1}{\sqrt{2}} \tag{1.20}$$

となるので、量子力学の公理 *3* から、測定結果 0 が得られる確率は $|\langle 0|+\rangle|^2 = 1/2$ となり、この測定結果が得られたときには、測定直後の状態は $|0\rangle$ で表される。また、同様の計算から $\langle 1|+\rangle = 1/\sqrt{2}$ となるので、量子力学の公理 *3* から、測定結果 1 が得られる確率は $|\langle 1|+\rangle|^2 = 1/2$ となり、この測定結果が得られたときには、測定直後の状態は $|1\rangle$ で表される。

従って、まとめると、測定直前に系の状態が $|+\rangle$ で表されていた場合、正規直交基底 $|0\rangle, |1\rangle$ に関する測定を行うと、測定結果としては確率 1/2 で 0 か 1 が得られ、測定直後の状態は、測定結果にそのまま依存し、$|0\rangle$ か $|1\rangle$ で表されることになる。同様の計算を行うと、測定直前に系の状態が $|-\rangle$ で表されていた場合も全く同じで、正規直交基底 $|0\rangle, |1\rangle$ に関する測定を行うと、測定結果としては確率 1/2 で 0 か 1 が得られ、測

定直後の状態は、測定結果に依存し、$|0\rangle$ か $|1\rangle$ で表されることがわかる。

***(b)* 正規直交基底 $\{|+\rangle, |-\rangle\}$ についての測定**

例 *1.2.1* より、$|+\rangle$ と $|-\rangle$ は正規直交基底である。1 *qubit* の量子系に対し、この基底 $|+\rangle, |-\rangle$ に関して測定を行う場合を考える。

(a) で測定直前の状態が $|0\rangle$ か $|1\rangle$ で表されていた場合と同様に、測定直前に系の状態が $|+\rangle$ で表されていた場合には、測定結果は確率 1 で $+$ が得られ、測定直後の状態は $|+\rangle$ で表される。また、測定直前に系の状態が $|-\rangle$ で表されていた場合には、確率 1 で測定結果 $-$ が得られ、測定直後の状態は $|-\rangle$ で表される。従って特に、系の状態が $|+\rangle$ か $|-\rangle$ のどちらかである場合には、基底 $|+\rangle, |-\rangle$ に関して測定を行うことにより、その状態を決定できる。その上、測定によって状態に変化は生じない。

一方、関係式

$$|\langle +|0\rangle|^2 = |\overline{\langle 0|+\rangle}|^2 = |\langle 0|+\rangle|^2 = \frac{1}{2} \tag{1.21}$$

などが成り立つことに気を付け、*(a)* の結果を利用すると、次が成り立つことがわかる：

測定直前に系の状態が $|0\rangle$ で表されていた場合、正規直交基底 $|+\rangle, |-\rangle$ に関する測定を行うと、測定結果としては確率 1/2 で $+$ か $-$ が得られ、測定直後の状態は、測定結果にそのまま依存し、$|+\rangle$ か $|-\rangle$ で表される。また、測定直前に系の状態が $|1\rangle$ で表されていた場合も全く同じで、正規直交基底 $|+\rangle, |-\rangle$ に関する測定を行うと、測定結果としては確率 1/2 で $+$ か $-$ が得られ、測定直後の状態は、測定結果に依存し、$|+\rangle$ か $|-\rangle$ で表される。 □

問 8. 例 *1.2.2* の諸結果（特に、計算の多くを省略した *(b)* の場合）を確認せよ。 □

1.3 量子鍵共有プロトコル BB84

本節では、これまでに学んだ事柄に基づいて、量子鍵共有プロトコル BB84 について学ぶ [7]。BB84 は盗聴検知機能が付いた鍵共有プロトコルである。空間的に離れた場所にいる Alice と Bob が、ランダムなビット列 [8] を、盗聴はなされていないという保証付きで、共有するためのプロトコルであり、これまでに学んだ量子力学の原理に基づいている。共有したビット列は、通常の共通鍵暗号の秘密鍵などに利用される。

Alice と Bob は n ビットのランダム列を共有したいとしよう。BB84 プロトコルの実行に際しては、Alice は Bob に順次 1 qubit を送り、Bob はそのつど送られてきた 1 qubit を測定する。また、Alice と Bob の間には、通常の電話のような双方向の公衆回線が確保されているものとする。この公衆回線は常時盗聴されていても構わないとする。自然数 m は安全性パラメータであり、プロトコルにおける盗聴検知能力の高さを表す。以下では、状態 $|0\rangle, |1\rangle$ をあわせて 01 系状態、状態 $|+\rangle, |-\rangle$ をあわせて $+-$ 系状態と呼ぶことにする。また、正規直交基底 $\{|0\rangle, |1\rangle\}$ についての測定を 01 系測定、正規直交基底 $\{|+\rangle, |-\rangle\}$ についての測定を $+-$ 系測定と呼ぶことにする。そしてプロトコル中では、Alice は状態 $|0\rangle, |+\rangle$ にビット 0 を、状態 $|1\rangle, |-\rangle$ にビット 1 を、それぞれ対応させて記録する。一方、Bob は測定結果 $0, +$ にビット 0 を、測定結果 $1, -$ にビット 1 を、それぞれ対応させて記録する。BB84 プロトコルは次のように与えられる。

BB84 鍵共有プロトコル

(i) Alice と Bob の間で、次の (a), (b), (c) を $n + m$ ビット分の記録が得られるまで繰り返す。

(a) Alice は 4 つベクトル $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ の中からランダムに 1 つを選び、1 qubit を、そのベクトルが表す状態に設定した上で Bob に送信する。その際、Alice は、1 qubit をどの状態にして送ったのかということと、その状態に対応するビット（即ち、0 か 1）を記録する。

[7] この量子暗号プロトコルは、C. H. Bennett と G. Brassard が 1984 年に考案したものなので、BB84 と呼ばれる。
[8] qubit 列ではなく、古典的な通常のビット列。

(b) Bob は 01 系測定と $+-$ 系測定のうち 1 つをランダムに選び、その測定を Alice から送られてきた 1 qubit に対して行う。そして、行った測定の種類（即ち、01 系測定と $+-$ 系測定のどちらかか）と、測定結果に対応するビットを記録する。

(c) 公衆回線を用い、Alice は、送信した状態が 01 系状態と $+-$ 系状態のうちどちらであったのかを、Bob に告げる。このとき、$|1\rangle$ や $|+\rangle$ など、具体的な個々の状態についてまでは開示しない。また、Bob は、Alice から送信された qubit を 01 系測定と $+-$ 系測定のどちらで測定したのかを、Alice に告げる。このとき、1 や + など、測定結果についてまでは開示しない。そして、Alice は 01 系状態を送信したのに Bob は $+-$ 系測定をしてしまった場合、および Alice は $+-$ 系状態を送信したのに Bob は 01 系測定をしてしまった場合の二つの場合については、Alice、Bob 共に記録を破棄する。

(ii) Alice と Bob は以上の手続きで記録されたビット列の中から、ランダムに m ビット選び、公衆回線を使って一致しているかどうかをチェックする。全て一致していた場合、盗聴は無かったとして、残りの n ビットを共有鍵として採用する。1 ビットでも違っていた場合、盗聴があったとして、鍵共有は失敗に終わったとする。（鍵共有は失敗に終わった場合には、Alice と Bob は、この鍵共有プロトコルを最初からやり直すか、またはその前に、qubit を配送する通信路（qubit として光子を用いる場合は、光ファイバーケーブル等）を盗聴者に干渉され難くする、などの処置を行う。） □

1.3.1 プロトコルの検証

Alice と Bob の間の公衆回線は常時盗聴されていても良いとしているので、盗聴者の盗聴行為が問題となるのは、Alice から Bob に 1 qubit が送られる際の、その経路上でである。1 qubit 配送中には、これが 01 系状態なのか $+-$ 系状態なのか、Alice はまだ誰にも開示していないので、盗聴者にも当然わからない。もしわかれば、例 1.2.2 で示されたように、01 系状態に対しては 01 系測定を行い、$+-$ 系状態に対しては $+-$ 系測定を行うことにより、Alice が送信した状態が何であったのかを確実に決定でき、かつその状態に何の変化も与えることはない。従って、盗聴行為が Alice と Bob に知られることも無く盗聴は成功する。しかし、開示は 1 qubit が Bob の下に届いた以降に行われるので、このように都合の良い測定を選んで、測定を行うことは出来ない。**盗聴者が出来るのは、例えば、配送中の 1 qubit に対し、適当な確率に従って 01 系測定か $+-$ 系測定かを選択し、その測定を行うことである。ここではそのような盗聴行為を想定する。**

盗聴が無かった場合

プロトコルの (i) の (a), (b), (c) が成功裏に終わると（即ち、記録を破棄なしに無事終了すると）、Alice は 01 系状態を送信し Bob は 01 系測定をした場合と、Alice は $+-$ 系状態を送信し Bob は $+-$ 系測定をした場合のどちらかが起こったことになる。例 1.2.2 で調べた事実により、どちらの場合にしても、Alice と Bob は、0 と 1 の 2 つのうち同じビットを記録することになる。例えば、Alice が $+-$ 系状態の $|-\rangle$ を送信した場合、Bob は $+-$ 系測定である正規直交基底 $\{|+\rangle, |-\rangle\}$ についての測定を行うので、Bob は測定結果 $-$ を得る。従って、Alice、Bob 共にビット 1 を記録することになる。ゆえに、プロトコルの (i) が終了した段階では、Alice と Bob は全く同じ $n+m$ ビット列を保持することになる。従って、それに続くプロトコルの (ii) も成功裏に終わり、Alice と Bob は同一の n ビット列を共有することになる。この n ビット列がランダムな n ビット列であることは、プロトコルの (i) の (a), (b) と (ii) とで、選択はランダムに行われたことにより保証される。

盗聴があった場合

盗聴があったにもかかわらず、盗聴は無かったとしてプロトコルが無事終了してしまう確率を計算する。まず、例 1.2.2 で明らかにされた次の事実に注意する：01 系状態に対し $+-$ 系測定を行うと、確率 1/2 で +

か $-$ が得られ、と同時に、その測定結果に依存し $+-$ 系状態のどちらかが生じる。逆に、$+-$ 系状態に対し 01 系測定を行うと、確率 1/2 で 0 か 1 が得られ、と同時に、その測定結果に依存し 01 系状態のどちらかが生じる。

盗聴者が配送中の 1 qubit に対し測定を行う際に、01 系測定を選択する確率を p、$+-$ 系測定を選択する確率を $1-p$ とする。さて、**このような盗聴が常時行われていると仮定し**、プロトコルの (i) の一連の (a), (b), (c) が成功裏に終わったという条件の下で、Alice と Bob が記録したビットが同一となる条件付確率を、まず始めに求めよう。プロトコルの (i) の一連の (a), (b), (c) が成功裏に終わったという条件の下では、次の [1], [2], [3], [4] の 4 つの場合が生じ得る。このとき、その条件の下でこれら 4 つの場合のそれぞれが生じる条件付確率は、等しく 1/4 となることに注意しよう。

[1] Alice は状態 $|0\rangle$ を送信し Bob は 01 系測定をした場合 この場合に、Alice と Bob が記録したビットが同一となるのは、盗聴者が 01 系測定を選択した場合（この場合、qubit の状態に変化は起きない）か、盗聴者は $+-$ 系測定を選択し、その結果生じた $+-$ 系状態に対し Bob は 01 系測定を行い、測定結果として 0 を得てしまった場合である。従って、Alice は状態 $|0\rangle$ を送信し Bob は 01 系測定をしたという条件の下で、Alice と Bob が記録したビットが同一となる条件付確率は、

$$p + (1-p)\left(\frac{1}{2}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{2}\right) = \frac{1}{2} + \frac{1}{2}p \tag{1.22}$$

となる。ここで、左辺第 2 項の 2 番目の括弧の中にある 2 つの $1/2 \cdot 1/2$ は、それぞれ、盗聴者の測定結果が $+$ であった場合と $-$ であった場合に対応する（図 1.1 参照）。

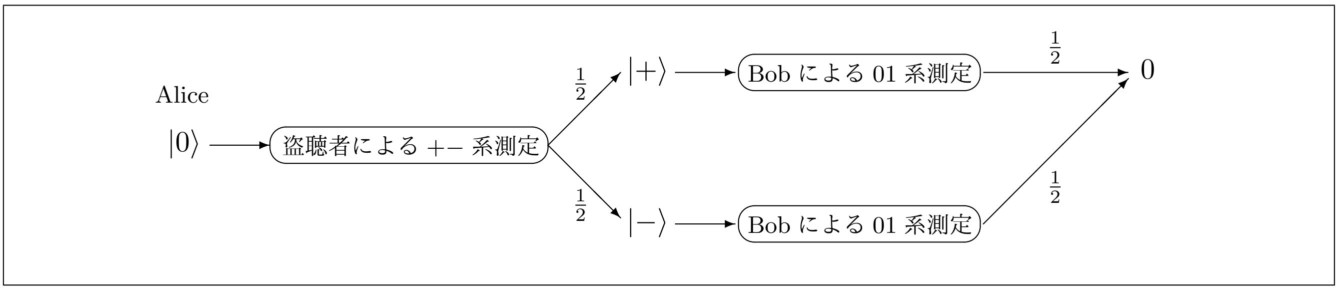

図 1.1: 状態 $|0\rangle$ に対する盗聴者による $+-$ 系測定と、その後の Bob による 01 系測定（$\frac{1}{2}$ は確率を表す）

[2] Alice は状態 $|1\rangle$ を送信し Bob は 01 系測定をした場合 この場合に、Alice と Bob が記録したビットが同一となるのは、盗聴者が 01 系測定を選択した場合（この場合、qubit の状態に変化は起きない）か、盗聴者は $+-$ 系測定を選択し、その結果生じた $+-$ 系状態に対し Bob は 01 系測定を行い、測定結果として 1 を得てしまった場合である。従って、Alice は状態 $|1\rangle$ を送信し Bob は 01 系測定をしたという条件の下で、Alice と Bob が記録したビットが同一となる条件付確率は、

$$p + (1-p)\left(\frac{1}{2}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{2}\right) = \frac{1}{2} + \frac{1}{2}p \tag{1.23}$$

となる。ここで、左辺第 2 項の 2 番目の括弧の中にある 2 つの $1/2 \cdot 1/2$ は、それぞれ、盗聴者の測定結果が $+$ であった場合と $-$ であった場合に対応する（図 1.2 参照）。

[3] Alice は状態 $|+\rangle$ を送信し Bob は $+-$ 系測定をした場合 この場合に、Alice と Bob が記録したビットが同一となるのは、盗聴者が $+-$ 系測定を選択した場合（この場合、qubit の状態に変化は起きない）か、盗聴者は 01 系測定を選択し、その結果生じた 01 系状態に対し Bob は $+-$ 系測定を行い、測定結果として $+$ を得てしまった場合である。従って、Alice は状態 $|+\rangle$ を送信し Bob は $+-$ 系測定をしたという条件の下で、Alice と Bob が記録したビットが同一となる条件付確率は、

$$(1-p) + p\left(\frac{1}{2}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{2}\right) = 1 - \frac{1}{2}p \tag{1.24}$$

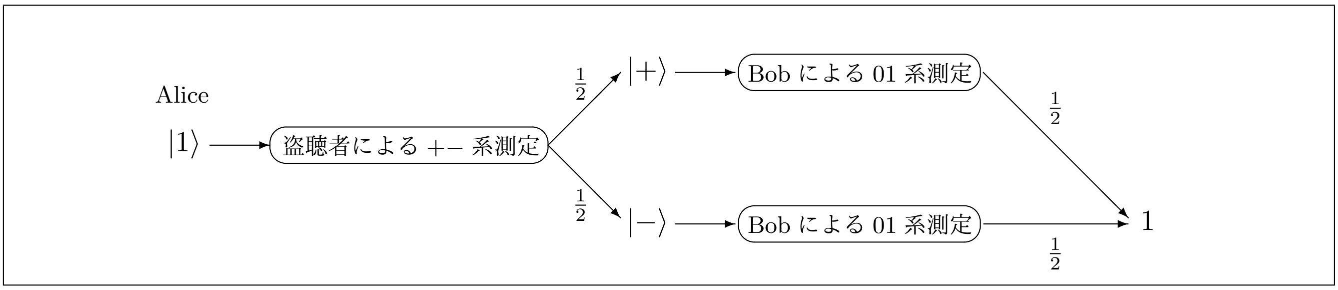

図 1.2: 状態 $|1\rangle$ に対する盗聴者による +− 系測定と、その後の Bob による 01 系測定

となる。ここで、左辺第 2 項の括弧の中にある 2 つの $1/2 \cdot 1/2$ は、それぞれ、盗聴者の測定結果が 0 であった場合と 1 であった場合に対応する（図 1.3 参照）。

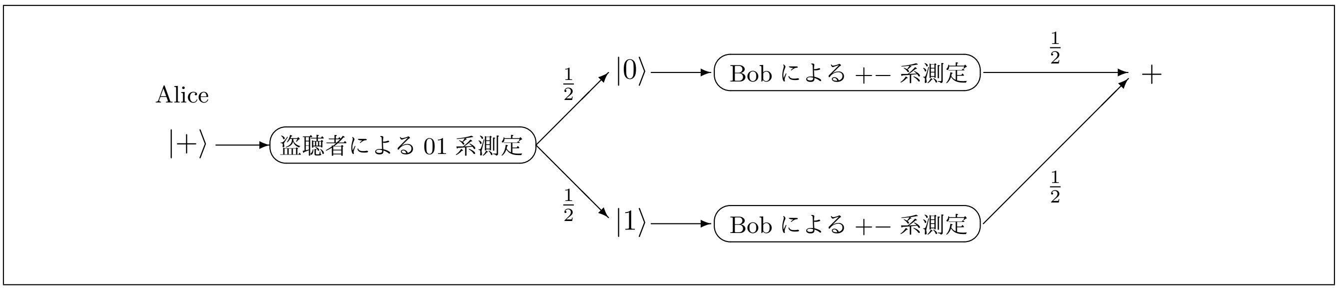

図 1.3: 状態 $|+\rangle$ に対する盗聴者による 01 系測定と、その後の Bob による +− 系測定

[4] Alice は状態 $|-\rangle$ を送信し Bob は +− 系測定をした場合 この場合に、Alice と Bob が記録したビットが同一となるのは、盗聴者が +− 系測定を選択した場合（この場合、qubit の状態に変化は起きない）か、盗聴者は 01 系測定を選択し、その結果生じた 01 系状態に対し Bob は +− 系測定を行い、測定結果として − を得てしまった場合である。従って、Alice は状態 $|-\rangle$ を送信し Bob は +− 系測定をしたという条件の下で、Alice と Bob が記録したビットが同一となる条件付確率は、

$$(1-p)+p\left(\frac{1}{2}\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2}\right)=1-\frac{1}{2}p \tag{1.25}$$

となる。ここで、左辺第 2 項の括弧の中にある 2 つの $1/2 \cdot 1/2$ は、それぞれ、盗聴者の測定結果が 0 であった場合と 1 であった場合に対応する（図 1.4 参照）。

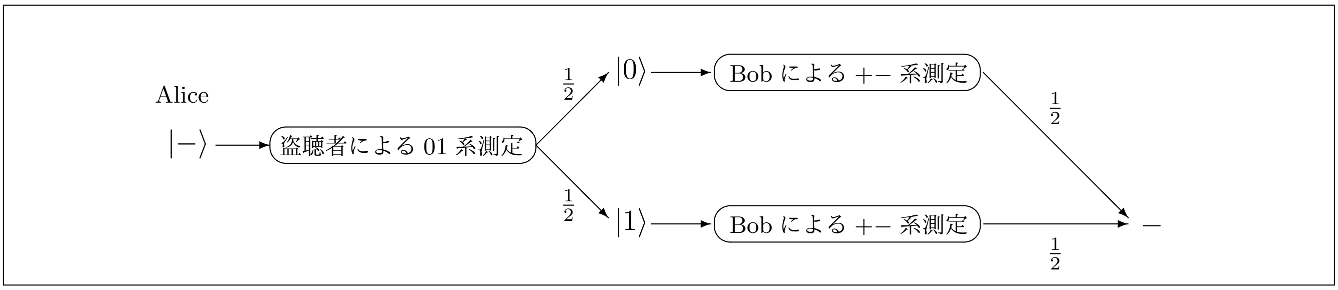

図 1.4: 状態 $|-\rangle$ に対する盗聴者による 01 系測定と、その後の Bob による +− 系測定

上述の通り、プロトコルの (i) の一連の (a), (b), (c) が成功裏に終わったという条件の下で、以上の 4 つの場合 [1], [2], [3], [4] のそれぞれが起こる条件付確率は、どれも 1/4 であるので、プロトコルの (i) の一連の (a), (b), (c) が成功裏に終わったという条件の下で、Alice と Bob が記録したビットが同一となる条件付

確率は、
$$\frac{1}{4}\left(\frac{1}{2}+\frac{1}{2}p\right)+\frac{1}{4}\left(\frac{1}{2}+\frac{1}{2}p\right)+\frac{1}{4}\left(1-\frac{1}{2}p\right)+\frac{1}{4}\left(1-\frac{1}{2}p\right)=\frac{3}{4} \tag{1.26}$$
となる（p に依らないことに注意）。

従って、盗聴があったにもかかわらず、盗聴は無かったとしてプロトコルが無事終了してしまう確率は、(ii) でランダムに選択した m 個のビットの全てが Alice と Bob とで同一となる確率なので、
$$\left(\frac{3}{4}\right)^m \tag{1.27}$$
となる。これは、盗聴があったにもかかわらず、それを検知できない確率である。例えば、$m=100$ とすれば $(3/4)^m \simeq 3.2\times 10^{-13}$ であり、殆ど起こりえないことになる。従って、m を十分に大きく取れば、盗聴があった時には、ほぼ確実にそれを検知できることになる。

1.4　量子測定: 部分系に対する測定

本節では、量子系の部分系に対して行う量子測定について考察する。

定理 1.4.1. テンソル積は次の性質を持つ。

(i) $(A\otimes B)^\dagger = A^\dagger \otimes B^\dagger$.

(ii) 行列 A_1, A_2, B_1, B_2 に対し、行列の積 A_1A_2, B_1B_2 が定義されるとき、次が成り立つ：
$$(A_1\otimes B_1)(A_2\otimes B_2)=(A_1A_2)\otimes(B_1B_2). \tag{1.28}$$
従って、上式は、テンソル積と行列の積との “交換の規則” を与える。 □

問 9. 定理 *1.4.1* を証明せよ。 □

定理 1.4.2. ベクトル $|r_1\rangle,\ldots,|r_{d_1}\rangle$ を複素ベクトル空間 $\mathbb{C}^{d_1}$ の任意の正規直交基底とし、ベクトル $|s_1\rangle,\ldots,|s_{d_2}\rangle$ を複素ベクトル空間 $\mathbb{C}^{d_2}$ の任意の正規直交基底とする。このとき、d_1d_2 個のベクトル $|r_j\rangle\otimes|s_k\rangle$ $(j=1,\ldots,d_1; k=1,\ldots,d_2)$ は複素ベクトル空間 $\mathbb{C}^{d_1d_2}$ の正規直交基底となる。 □

問 10. 定理 *1.4.2* を証明せよ。（ヒント：定理 *1.4.1* を用い、$(|r_{j_1}\rangle\otimes|s_{k_1}\rangle, |r_{j_2}\rangle\otimes|s_{k_2}\rangle)=\delta_{j_1j_2}\delta_{k_1k_2}$ を示す） □

量子力学の公理 4 (量子測定 II-1)**.** $\mathcal{Q}_1, \mathcal{Q}_2$ を、それぞれ状態空間が $\mathbb{C}^{d_1}, \mathbb{C}^{d_2}$ で与えられる任意の量子系とする。ここで、$\mathcal{Q}_1$ と $\mathcal{Q}_2$ は、全体として合成系 $\mathcal{Q}$ を構成しているものとする。このとき、$|r_1\rangle,\ldots,|r_{d_1}\rangle$ を $\mathcal{Q}_1$ の状態空間 $\mathbb{C}^{d_1}$ の任意の正規直交基底とすると、量子系 $\mathcal{Q}_1$ に対し、次の性質を持つ**量子測定**を行うことが出来る。

(i) 測定結果として、$r_1,\ldots,r_{d_1}$ のうち、どれか一つが得られる。

(ii) 測定の直前に、量子系 $\mathcal{Q}$ の状態は、規格化されたベクトル $|\psi\rangle(\in \mathbb{C}^{d_1 d_2})$ で表されていたものとする。更に、この $|\psi\rangle$ は次のように表現されていたものとする。

$$|\psi\rangle = \sum_{j=1}^{d_1}\sum_{k=1}^{d_2} \alpha_{r_j,s_k}|r_j\rangle \otimes |s_k\rangle. \tag{1.29}$$

ここで、$|s_1\rangle, \ldots, |s_{d_2}\rangle$ は $\mathcal{Q}_2$ の状態空間 $\mathbb{C}^{d_2}$ の任意の正規直交基底である。また、α_{r_j,s_k} $(j = 1, \ldots, d_1; k = 1, \ldots, d_2)$ は複素数である。このとき、各 $j = 1, \ldots, d_1$ に対し、確率

$$p_1(r_j) = \sum_{k=1}^{d_2} |\alpha_{r_j,s_k}|^2 \tag{1.30}$$

で測定結果 r_j が得られる。そして、測定結果として r_j が得られた場合、測定直後の量子系 $\mathcal{Q}$ の状態は次のベクトルで表される。

$$\frac{1}{\sqrt{p_1(r_j)}} \sum_{k=1}^{d_2} \alpha_{r_j,s_k}|r_j\rangle \otimes |s_k\rangle. \tag{1.31}$$

□

上記量子力学の公理 4 で、量子系 $\mathcal{Q}_1$ と量子系 $\mathcal{Q}_2$ の立場を入れ替えた、次の公理も成立する。

量子力学の公理 5 (量子測定 II-2)**.** $\mathcal{Q}_1, \mathcal{Q}_2$ を、ぞれぞれ状態空間が $\mathbb{C}^{d_1}, \mathbb{C}^{d_2}$ で与えられる任意の量子系とする。ここで、$\mathcal{Q}_1, \mathcal{Q}_2$ は、全体として合成系 $\mathcal{Q}$ を構成しているものとする。このとき、$|s_1\rangle, \ldots, |s_{d_2}\rangle$ を $\mathcal{Q}_2$ の状態空間 $\mathbb{C}^{d_2}$ の任意の正規直交基底とすると、量子系 $\mathcal{Q}_2$ に対し、次の性質を持つ**量子測定**を行うことが出来る。

(i) 測定結果として、$s_1, \ldots, s_{d_2}$ のうち、どれか一つが得られる。

(ii) 測定の直前に、量子系 $\mathcal{Q}$ の状態は、規格化されたベクトル $|\psi\rangle(\in \mathbb{C}^{d_1 d_2})$ で表されていたものとする。更に、この $|\psi\rangle$ は次のように表現されていたものとする。

$$|\psi\rangle = \sum_{j=1}^{d_1}\sum_{k=1}^{d_2} \alpha_{r_j,s_k}|r_j\rangle \otimes |s_k\rangle. \tag{1.32}$$

ここで、$|r_1\rangle, \ldots, |r_{d_1}\rangle$ は $\mathcal{Q}_1$ の状態空間 $\mathbb{C}^{d_1}$ の任意の正規直交基底である。また、α_{r_j,s_k} $(j = 1, \ldots, d_1; k = 1, \ldots, d_2)$ は複素数である。このとき、各 $k = 1, \ldots, d_2$ に対し、確率

$$p_2(s_k) = \sum_{j=1}^{d_1} |\alpha_{r_j,s_k}|^2 \tag{1.33}$$

で測定結果 s_k が得られる。そして、測定結果として s_k が得られた場合、測定直後の量子系 $\mathcal{Q}$ の状態は次のベクトルでで表される。

$$\frac{1}{\sqrt{p_2(s_k)}} \sum_{j=1}^{d_1} \alpha_{r_j,s_k}|r_j\rangle \otimes |s_k\rangle. \tag{1.34}$$

□

問 11. ベクトル (1.31) の係数 $\frac{1}{\sqrt{p_1(r_j)}}$、及びベクトル (1.34) の係数 $\frac{1}{\sqrt{p_2(s_k)}}$ は、規格化のための係数である。ベクトル (1.31) と (1.34) が規格化されていることを確認せよ。 □

問 12. 量子力学の公理 *4* の *(ii)* の主張は、$\mathcal{Q}_2$ の状態空間 $\mathbb{C}^{d_2}$ の正規直交基底 $|s_1\rangle, \ldots, |s_{d_2}\rangle$ の取り方に依存しないことを証明せよ。同様に、量子力学の公理 *5* の *(ii)* の主張は、$\mathcal{Q}_1$ の状態空間 $\mathbb{C}^{d_1}$ の正規直交基底 $|r_1\rangle, \ldots, |r_{d_1}\rangle$ の取り方に依存しないことを証明せよ。 □

例 1.4.3 (2 qubit の量子系での各 1 qubit の測定)**.** ここでは、量子力学の公理 *4*、及び量子力学の公理 *5* の使い方に慣れるために、*2* つの 1 *qubit* の量子系 $\mathcal{Q}_1$ と $\mathcal{Q}_2$ から成る 2 *qubit* の量子系 $\mathcal{Q}$ を考え、量子系 $\mathcal{Q}_1$ と $\mathcal{Q}_2$ のそれぞれに対する量子測定について考察する。

量子系 $\mathcal{Q}$ の状態が、次のベクトル $|\psi\rangle (\in \mathbb{C}^4)$ で表されていたものとする。

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{1.35}$$

ここで、式 (1.8) より、$|00\rangle \equiv |0\rangle \otimes |0\rangle$、及び $|11\rangle \equiv |1\rangle \otimes |1\rangle$ と定義されていることに注意されたい。また、量子力学の公理 *2* より、一般に、ベクトル $|b_1 b_2\rangle$ $(b_1 = 0, 1; b_2 = 0, 1)$ は、量子系 $\mathcal{Q}_1$ の *qubit* は状態 $|b_1\rangle$ にあり、量子系 $\mathcal{Q}_2$ の *qubit* は状態 $|b_2\rangle$ にある、という量子系 $\mathcal{Q}$ の状態を表している。

さて、全系 $\mathcal{Q}$ がこの状態 $|\psi\rangle$ にあるとき、部分系 $\mathcal{Q}_1$ に対して、正規直交基底 $\{|0\rangle, |1\rangle\}$ に関して測定を行うことを考えよう。これは、部分系 $\mathcal{Q}_1$ に対する測定なので、量子力学の公理 *4* が適用される。すると、量子力学の公理 *4* の *(i)* より、この測定の測定結果は、0 と 1 のどちらかとなる。更に、量子力学の公理 *4* の *(ii)* を適用するために、$|\psi\rangle$ を次のように変形する。

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + 0|0\rangle \otimes |1\rangle + 0|1\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle && (1.36) \\ &= \sum_{b_1=0,1} \sum_{b_2=0,1} \alpha_{b_1,b_2} |b_1\rangle \otimes |b_2\rangle. && (1.37) \end{aligned}$$

ここで、$\alpha_{0,0} = 1/\sqrt{2}, \alpha_{0,1} = 0, \alpha_{1,0} = 1, \alpha_{1,1} = 1/\sqrt{2}$ となる。なお、$|\psi\rangle$ は規格化されていることに注意。従って、量子力学の公理 *4* の *(ii)* より次が成り立つ。

測定結果 0 を得る確率と測定直後の状態： 測定結果 0 を得る確率は、$p_1(0) = |\alpha_{0,0}|^2 + |\alpha_{0,1}|^2 = 1/2 + 0 = 1/2$ となる。そして、測定直後の $\mathcal{Q}$ 状態は、

$$\begin{aligned} \frac{1}{\sqrt{p_1(0)}}(\alpha_{0,0}|0\rangle \otimes |0\rangle + \alpha_{0,1}|0\rangle \otimes |1\rangle) &= \frac{1}{\sqrt{1/2}}\left(\frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + 0|0\rangle \otimes |1\rangle\right) && (1.38) \\ &= |0\rangle \otimes |0\rangle = |00\rangle && (1.39) \end{aligned}$$

となる。

測定結果 1 を得る確率と測定直後の状態： 測定結果 1 を得る確率は、$p_1(1) = |\alpha_{1,0}|^2 + |\alpha_{1,1}|^2 = 0 + 1/2 = 1/2$ となる。そして、測定直後の $\mathcal{Q}$ 状態は、

$$\begin{aligned} \frac{1}{\sqrt{p_1(1)}}(\alpha_{1,0}|1\rangle \otimes |0\rangle + \alpha_{1,1}|1\rangle \otimes |1\rangle) &= \frac{1}{\sqrt{1/2}}\left(0|1\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle\right) && (1.40) \\ &= |1\rangle \otimes |1\rangle = |11\rangle && (1.41) \end{aligned}$$

となる。

さて、部分系 $\mathcal{Q}_1$ に対する、正規直交基底 $\{|0\rangle, |1\rangle\}$ に関する上述の測定が終わった直後に、更に、部分系 $\mathcal{Q}_2$ に対して、正規直交基底 $\{|0\rangle, |1\rangle\}$ に関して測定を行うことを考えよう。これは、部分系 $\mathcal{Q}_2$ に対する測定なので、量子力学の公理 *5* が適用される。

部分系 $\mathcal{Q}_1$ に対する測定で測定結果 0 が得られた場合： 部分系 $\mathcal{Q}_1$ に対する測定が行われた直後の全系 $\mathcal{Q}$ 状態は、$|00\rangle$ で表されている。量子力学の公理 *5* の *(ii)* を適用するために、$|00\rangle$ を次のように変形する。

$$\begin{aligned} |00\rangle &= 1|0\rangle\otimes|0\rangle + 0|0\rangle\otimes|1\rangle + 0|1\rangle\otimes|0\rangle + 0|1\rangle\otimes|1\rangle && (1.42) \\ &= \sum_{b_1=0,1}\sum_{b_2=0,1}\alpha_{b_1,b_2}|b_1\rangle\otimes|b_2\rangle. && (1.43) \end{aligned}$$

ここで、$\alpha_{0,0}=1, \alpha_{0,1}=\alpha_{1,0}=\alpha_{1,1}=0$ となる。なお、$|00\rangle$ は規格化されていることに注意。従って、量子力学の公理 *5* の *(ii)* より、部分系 $\mathcal{Q}_2$ に対して、正規直交基底 $\{|0\rangle, |1\rangle\}$ に関して測定を行った場合に測定結果 0 を得る確率は、$p_2(0)=|\alpha_{0,0}|^2+|\alpha_{1,0}|^2=1+0=1$ となり、確率 1 で測定結果 0 が得られる。そして、測定直後の $\mathcal{Q}$ 状態は、

$$\begin{aligned} \frac{1}{\sqrt{p_2(0)}}(\alpha_{0,0}|0\rangle\otimes|0\rangle + \alpha_{1,0}|1\rangle\otimes|0\rangle) &= \frac{1}{\sqrt{1}}(1|0\rangle\otimes|0\rangle + 0|1\rangle\otimes|0\rangle) && (1.44) \\ &= |0\rangle\otimes|0\rangle = |00\rangle && (1.45) \end{aligned}$$

となり、$\mathcal{Q}_2$ に対するこの測定が行われる直前と同じである。

部分系 $\mathcal{Q}_1$ に対する測定で測定結果 1 が得られた場合： 部分系 $\mathcal{Q}_1$ に対する測定が行われた直後の全系 $\mathcal{Q}$ 状態は、$|11\rangle$ で表されている。量子力学の公理 *5* の *(ii)* を適用するために、$|11\rangle$ を次のように変形する。

$$\begin{aligned} |11\rangle &= 0|0\rangle\otimes|0\rangle + 0|0\rangle\otimes|1\rangle + 0|1\rangle\otimes|0\rangle + 1|1\rangle\otimes|1\rangle && (1.46) \\ &= \sum_{b_1=0,1}\sum_{b_2=0,1}\alpha_{b_1,b_2}|b_1\rangle\otimes|b_2\rangle. && (1.47) \end{aligned}$$

ここで、$\alpha_{0,0}=\alpha_{0,1}=\alpha_{1,0}=0, \alpha_{1,1}=1$ となる。なお、$|11\rangle$ は規格化されていることに注意。従って、量子力学の公理 *5* の *(ii)* より、部分系 $\mathcal{Q}_2$ に対して、正規直交基底 $\{|0\rangle, |1\rangle\}$ に関して測定を行った場合に測定結果 1 を得る確率は、$p_2(1)=|\alpha_{0,1}|^2+|\alpha_{1,1}|^2=0+1=1$ となり、確率 1 で測定結果 1 が得られる。そして、測定直後の $\mathcal{Q}$ 状態は、

$$\begin{aligned} \frac{1}{\sqrt{p_2(1)}}(\alpha_{0,1}|0\rangle\otimes|1\rangle + \alpha_{1,1}|1\rangle\otimes|1\rangle) &= \frac{1}{\sqrt{1}}(0|0\rangle\otimes|1\rangle + 1|1\rangle\otimes|1\rangle) && (1.48) \\ &= |1\rangle\otimes|1\rangle = |11\rangle && (1.49) \end{aligned}$$

となり、$\mathcal{Q}_2$ に対するこの測定が行われる直前と同じである。

このようにして、全系 $\mathcal{Q}$ が $|\psi\rangle$ で表される状態にあるとき、部分系 $\mathcal{Q}_1$ に対して行われる正規直交基底 $\{|0\rangle, |1\rangle\}$ に関する測定の結果と、その直後に部分系 $\mathcal{Q}_2$ に対して行われる正規直交基底 $\{|0\rangle, |1\rangle\}$ に関する測定の結果は、常に同じになる。 □

問 13. 例 *1.4.3* に現れる $|\psi\rangle$ や $|00\rangle, |11\rangle$ が規格化されていることを確認せよ。 □

問 14. 量子力学の公理 *4* と *5* に基づいて、例 *1.4.3* の各結果をチェックせよ。 □

例 1.4.4 (EPR パラドックス)**.** 上記の例 *1.4.3* の物理的意味について考察しよう。

量子系 $\mathcal{Q}$ は *2* つの *qubit* の部分系 $\mathcal{Q}_1, \mathcal{Q}_2$ から成っているが、$\mathcal{Q}_1$ と $\mathcal{Q}_2$ を接近させて相互作用させることにより、$\mathcal{Q}$ の状態を

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1.50}$$

に置くことは可能である。さて、その後、*2* つの *qubit* を互いに空間的に離れた場所に移動させることを考えよう。部分系 $\mathcal{Q}_1$ の *qubit* は *Alice* に送られ、部分系 $\mathcal{Q}_2$ の *qubit* は、*Alice* とは空間的に離れた場所にいる *Bob* に送られるとする。

Alice が自分の持っている *qubit* $\mathcal{Q}_1$ に対して、正規直交基底 $\{|0\rangle, |1\rangle\}$ に関する測定を行うと、例 *1.4.3* の計算結果より、*Alice* は、確率 $1/2$ で全くランダムに測定結果 0 と 1 のどちらかを得る。そして、*Alice* が測定結果 0 を得た場合には、その直後の全系 $\mathcal{Q}$ の状態は $|00\rangle$ で表される。一方、*Alice* が測定結果 1 を得た場合には、その直後の全系 $\mathcal{Q}$ の状態は $|11\rangle$ で表される。*Alice* による測定の直後に、離れた場所にいる *Bob* が、自分の持っている *qubit* $\mathcal{Q}_2$ に対して、やはり正規直交基底 $\{|0\rangle, |1\rangle\}$ に関する測定を行うとする。すると、例 *1.4.3* の計算結果より、*Alice* が測定結果 0 を得た場合には、*Bob* は必ず測定結果 0 を得る。また、*Alice* が測定結果 1 を得た場合には、*Bob* は必ず測定結果 1 を得ることになる。このように、状態 $|\psi\rangle$ を利用すると、離れた場所にいる *Alice* と *Bob* が、瞬間的に 0 か 1 かの（古典的な）ビットを共有することが出来る。

2 つの *qubit* の間隔はどんなに大きくても良い、*Alice* と *Bob* は銀河系の端と端にいても構わないのである。*Alice* と *Bob* は同じビットを瞬間的に共有できる。これは一見、光より速い情報の伝播を禁止した相対性理論に矛盾するように見える。しかし、この共有するビットが 0 か 1 かは、*Alice* や *Bob* にはコントロールすることは出来ない。0 か 1 かは全くランダムに決まるものなので、*Alice* が *Bob* に、0 か 1 のうち、意図したビットを送ることは出来ない。従って、相対性理論とは矛盾しない。

特殊相対性理論では、ある観測者にとっては異なる時刻に離れた場所で起こることが、その観測者に対して十分に速い速度で移動する観測者にとっては同時刻に起こっている場合が生じ得る。従って、移動している観測者にとって離れた場所に瞬時に情報が送られるということは、静止している観測者から見ると、過去に情報を送られるということに成り得るのである。このことから、種々の矛盾が生じる。しかし、上述の *Alice* と *Bob* の間では、*Alice* から *Bob* に情報を送ることは出来ないので、矛盾は生じない。

いずれにしても、*Alice* と *Bob* とはランダムなビットを共有することは可能である。実際、この現象を利用した量子鍵共有プロトコルが提案されている。このプロトコルにも、盗聴検知機能が付いており、*BB84* と同様の原理に基づいて動作する。

なお、2 *qubit* の状態 $(|00\rangle + |11\rangle)/\sqrt{2}$ は、量子力学が正しいとすると、上述の測定値の相関が起こり得ることを予想した *Einstein, Podolsky, Rosen* の頭文字をとり、*EPR pair* と呼ばれる。 □

問 15. 例 *1.4.4* の状況で、即ち、全系 $\mathcal{Q}$ の状態が $(|00\rangle + |11\rangle)/\sqrt{2}$ で表されているときに、*Alice* が部分系 $\mathcal{Q}_1$ に対して、正規直交基底 $\{|+\rangle, |-\rangle\}$ に関する測定を行い、その直後に、*Bob* が部分系 $\mathcal{Q}_1$ に対して、正規直交基底 $\{|+\rangle, |-\rangle\}$ に関する測定を行った場合、何が起こるかを考察せよ。 □

ところで、量子力学の公理 3 を、量子力学の公理 4 や量子力学の公理 5 の形式に、近い形に書き換えることは可能である。次の量子力学の公理 6 は、量子力学の公理 3 のそのような書き換えであり、量子力学の公理 3 と等価である。

量子力学の公理 6 (量子測定 I'). $\mathcal{Q}$ を状態空間が $\mathbb{C}^d$ で与えられる任意の量子系とする。そして、$|r_1\rangle, \dots, |r_d\rangle$ を $\mathbb{C}^d$ の任意の正規直交基底とする。このとき、量子系 $\mathcal{Q}$ に対し、次の性質を持つ量子測定を行うことが出来る。

(i) 測定結果として、$r_1, \dots, r_d$ のうち、どれか一つが得られる。

(ii) 測定の直前に、量子系 $\mathcal{Q}$ の状態が、規格化されたベクトル $|\psi\rangle$ で表されていたものとする。更に、この $|\psi\rangle$ は次のように表現されていたものとする。

$$|\psi\rangle = \sum_{i=1}^{d} \alpha_{r_i} |r_i\rangle. \tag{1.51}$$

ここで、α_{r_i} $(i = 1, \dots, d)$ は複素数である。このとき、各 $i = 1, \dots, d$ に対し、確率 $|\alpha_{r_i}|^2$ で測定結果 r_i が得られ、その場合、測定直後の量子系 $\mathcal{Q}$ の状態は $|r_i\rangle$ で表される。 □

問 16. 量子力学の公理 *6* と量子力学の公理 *3* の同値性を証明せよ。 □

第2章　量子計算のための量子力学入門 2 — 時間発展と量子計算機の基本構成 —

2.1　量子系の時間発展

一般に、計算とは、時間の経過と共に進行する一連の過程である。例えば、C 言語プログラムの実行では、実行開始後、プログラムで参照している変数の値と、プログラム中の実行している文の位置が、1 ステップ毎に刻々と変化する。その際、変化の規則はプログラムによって与えられる。Turing machine の計算では、Turing machine の内部状態、テープヘッドの位置、そしてテープに書かれている記号が、1 ステップ毎に刻々と変化する。その際、変化の規則は遷移関数 (transition function) によって与えられる。量子計算においても、計算は、時間の経過と共に進行する過程である。計算が行われる際、量子計算機の内部は、1 ステップ毎に刻々と変化する。しかし、量子計算機は量子力学に基づいて動作するので、計算の過程で起こる変化は、量子力学に従うものでなければならない。

量子系で起こる変化には、性質の異なる 2 つのものがある。一つは、既に学んだとおり、量子測定の結果として生じる変化である。そして、もう一つは、**量子系の時間発展**と呼ばれるものである。量子系の時間発展の公理は次のように与えられる。**閉じた量子系**とは、外界の量子系と量子力学的な相互作用をしておらず、また問題としている期間に量子測定も行われない量子系のことである [1]。また、正方行列 U が**ユニタリー行列**であるとは、

$$U^\dagger U = UU^\dagger = I \tag{2.1}$$

を満たすことである。ここで I は恒等行列（単位行列）である。

量子力学の公理 7 (量子系の時間発展)**.** *$\mathcal{Q}$ を任意の閉じた量子系とする。そして、$\mathcal{Q}$ の状態空間は $\mathbb{C}^d$ であるとする。このとき、任意の 2 つの時刻 t_1, t_2 に対し、ある d 次ユニタリー行列 $U(t_2, t_1)$ が存在し次が成り立つ。時刻 t_1 において $\mathcal{Q}$ の状態が $|\psi_1\rangle (\in \mathbb{C}^d)$ で表され、時刻 t_2 において $\mathcal{Q}$ の状態が $|\psi_2\rangle (\in \mathbb{C}^d)$ で表されるならば、必ず*

$$|\psi_2\rangle = U(t_2, t_1)|\psi_1\rangle \tag{2.2}$$

を満たす。 □

このように、閉じた量子系の時間発展はユニタリー行列によって記述される。従って、量子計算機においても、それは量子力学に従って動作するものなので、量子測定が行われていないときには、計算機内部の量子状態（qubit 列の量子状態）の時間発展は、式 (2.2) のようにユニタリー行列で規定される。

例 2.1.1 (1 qubit の量子系の時間発展: 量子 NOT ゲート)**.** *1 qubit の量子系の時間発展の例として、量子 NOT ゲートについて考察しよう。*

古典的な通常の計算では、NOT 演算は 1 ビットに作用し次の変換を引き起こす。

$$0 \mapsto 1, \quad 1 \mapsto 0. \tag{2.3}$$

[1] 例えば、量子系の外界がその量子系に対し “古典的な器”（外場）として存在し、外界は量子系に作用を及ぼすが、量子系からの “反作用” はなく、量子系の量子状態の推移の如何によらず、外界は一定もしくは決まった変化を行うとき、この量子系は閉じた量子系である。NMR(核磁気共鳴) 装置内に置かれた溶液分子中の原子核スピンは、外場として、一定で一様な強磁場、並びに高周波磁場にさらされている。それが小さな分子の場合には、原子核スピンは、数秒〜数十秒間にわたり、閉じた量子系とみなすことができる。

この NOT 演算は、NOT ゲートによって実現される。一方、量子計算では、NOT 演算は、次のユニタリー行列 U_{NOT} を 1 $qubit$ の状態に施すによって、実現される。

$$U_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{2.4}$$

実際、

$$U_{NOT}|0\rangle = |1\rangle, \quad U_{NOT}|1\rangle = |0\rangle \tag{2.5}$$

が成り立っており、量子計算機上では、

$$|0\rangle \mapsto |1\rangle, \quad |1\rangle \mapsto |0\rangle \tag{2.6}$$

という 1 $qubit$ の状態の変化として、(2.3) の NOT 演算が実現される。この NOT 演算の時間発展 (2.6) を引き起こすユニタリー行列 U_{NOT} は、**量子 *NOT* ゲート**と呼ばれる。 □

問 17. 例 *2.1.1* で、量子 NOT ゲート U_{NOT} がユニタリー行列であることを確認せよ。また、式 (1.3) を利用し、式 (2.5) を確認せよ。 □

量子系の時間発展を考えるとき重要なのは、式 (2.2) を通じて、その時間発展を規定する行列 $U(t_2, t_1)$ は、ユニタリー行列であり、正則だということである。これは、ある時刻において量子系の量子状態を決めると、量子系が閉じている限り、それ以後とそれ以前の全ての時刻の量子状態が、ただ一通りに定まる、ということを意味する。例えば、式 (2.2) より、$|\psi_1\rangle$ から $|\psi_2\rangle$ は当然一意に決まるが、$|\psi_1\rangle = U(t_2, t_1)^{-1}|\psi_2\rangle$ より、$|\psi_2\rangle$ から $|\psi_1\rangle$ も一意に決まる。従って、任意の時刻 t_1 での量子系の量子状態 $|\psi_1\rangle$ を固定すると、別な任意の時刻 t_2 でのその量子系の量子状態 $|\psi_2\rangle$ はただ 1 つに定まる。このように、閉じた量子系の時間発展は**可逆**[2] である。

量子計算機は、量子力学に基いて動作するので、量子計算機が行う計算も可逆でなければならない。実際、NOT 演算は可逆、即ち、変換 (2.3) は全単射なので、量子計算機上でそれを実現する量子 NOT ゲートが存在できたのである。これに対し、例えば、1 ビットに対する次の演算は可逆ではない。

$$0 \mapsto 1, \quad 1 \mapsto 1. \tag{2.7}$$

従って、量子計算機上でこの演算は実現できない。これは即ち、$U|0\rangle = |1\rangle$ かつ $U|1\rangle = |1\rangle$ を満たすユニタリー行列 U は存在しないからである。

問 18. $U|0\rangle = |1\rangle$ かつ $U|1\rangle = |1\rangle$ を満たすユニタリー行列 U は存在しないことを証明せよ。 □

パソコンやワークステーションなど、古典的な通常の計算機上での計算過程は、計算機内部にある膨大な数のビットに対し、NOT ゲートや AND ゲートなどの基本論理ゲートを、膨大な回数、逐次的に適用することから成り立っている。そして、理論的には、計算時間というものは、そのような基本論理ゲートの適用の回数として計測される。

量子計算においても、計算過程の基本は、古典的な場合と同様である。ある種の基本ゲートが用意され、計算機内部に多数ある qubit に、それが逐次的に適用されることにより、計算が進められて行くのである。量子計算において、この基本ゲートの役割を担うのは、**基本量子ゲート**である。基本量子ゲートは、或るクラスのユニタリー行列である。上述の量子 NOT ゲートは、そのような基本量子ゲートの 1 つである。このように、量子計算機上での計算過程は、計算機内部にある多数の qubit への、基本量子ゲートの適用の過程

[2] ここで、“可逆” という言葉は、数学的に言うと写像が全単射である、という意味で使っている。

である。そして、古典的な場合と同様に、**量子計算における計算時間は、計算の過程で、計算機内部の量子状態に施した基本量子ゲートの数によって定義される**[3]。

次の例で与えられる量子 Controlled NOT ゲートも、基本量子ゲートの一つである。それは、2 qubit の量子系に作用し、量子系に時間発展をもたらす。

例 2.1.2 (2 qubit の量子系の時間発展: 量子 Controlled NOT ゲート)**.** 2 *qubit* の量子系の時間発展について考察しよう。古典的な通常の計算では、*Controlled NOT* 演算は 2 ビットに作用し次の変換を引き起こすものとして定義される。

$$00 \mapsto 00, \quad 01 \mapsto 01, \quad 10 \mapsto 11, \quad 11 \mapsto 10. \tag{2.8}$$

この演算では、左のビットが 1 のときは、右のビットに *NOT* 演算が施され、左のビットが 0 のときは、右のビットは変化しないので、この演算は、*Controlled NOT* と呼ばれる。この *Controlled NOT* 演算は、$\mapsto$ の左辺の 2 ビットと右辺の 2 ビットが一対一に対応しており、可逆な演算である。従って、量子計算機上でそれを実現することは可能である。即ち、量子計算では、*Controlled NOT* 演算は、次のユニタリー行列 U_{CNOT} を 2 *qubit* の量子系に作用させ、時間発展を引き起こすことにより、実現される。

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2.9}$$

実際、

$$U_{CNOT}|00\rangle = |00\rangle, \quad U_{CNOT}|01\rangle = |01\rangle, \quad U_{CNOT}|10\rangle = |11\rangle, \quad U_{CNOT}|11\rangle = |10\rangle \tag{2.10}$$

が成り立っており、量子計算機上では、

$$|00\rangle \mapsto |00\rangle, \quad |01\rangle \mapsto |01\rangle, \quad |10\rangle \mapsto |11\rangle, \quad |11\rangle \mapsto |10\rangle \tag{2.11}$$

という 2 *qubit* の状態の変化として、(2.8) の *controlled NOT* 演算が実現される。この *controlled NOT* 演算の時間発展 (2.11) を引き起こすユニタリー行列 U_{CNOT} は、**量子 *controlled NOT* ゲート**と呼ばれる。 □

問 19. 例 *2.1.2* で U_{CNOT} がユニタリー行列であることを確認せよ。また、式 (1.9) を利用し、式 (2.10) を確認せよ。 □

2.2 量子並列性: モジュラー冪の量子並列的な計算

例 1.1.2 で見たように、ベクトル $|b_{n-1}b_{n-2}\ldots b_1b_0\rangle$ $(b_0, b_1 \ldots, b_{n-1} = 0, 1)$ は、n qubit の量子系の状態を表している。特に、それは、n qubit の量子系を構成する n 個の 1 qubit の量子系の量子状態が、それぞれ状態ベクトル $|b_{n-1}\rangle, |b_{n-2}\rangle, \ldots, |b_1\rangle, |b_0\rangle$ で表されている、という n qubit の量子系の量子状態を表している。任意の n に対し、n qubit の量子系をしばしば**量子レジスタ**と呼ぶ。量子レジスタは、量子計算機の内部において、通常の計算機の CPU の内部にあるレジスタと同様の役割を果たす。即ち、n 桁の二進整数を保持するのである。以後、我々は、通常の計算機の理論で行うように、$b_{n-1}b_{n-2}\ldots b_1b_0$ を、n ビット列であると同時に、二進表示された n 桁の整数と解釈する。

$\{0,1\}^n$ を n ビット列全体からなる集合とする。また、2 つの n ビット列 z と w に対し、$z \oplus w$ を、z と w の対応するビットのそれぞれについて XOR 演算を行い、その結果得られた n ビット列とする。このとき、次の定理が成り立つ。

[3] より正確に言うと、universal set と呼ばれる、或る特殊なユニタリー行列からなる集合があり、その集合の元であるところの個々のユニタリー行列が、基本量子ゲートと呼ばれる。univesal set の選び方は一通りではない。従って、基本量子ゲートは相対的な概念である。例えば、量子計算の理論的な解析でよく用いられる univesal set は、例 2.1.2 で考察してる量子 Controlled NOT ゲートと、或る特殊な 2 次のユニタリー行列からなり、そこには、量子 NOT ゲートは含まれない。本稿では、universal set を広めにとり、量子 NOT ゲートや後述のアダマールゲートもそれに含めている。なお、一般に universal set は無限集合である。これは、ユニタリー行列の要素は複素数であり、行列の次数を固定しても、ユニタリー行列は無限に多く存在することに対応する。

定理 2.2.1. 任意の関数 $f\colon \{0,1\}^n \to \{0,1\}^m$ に対し、ある 2^{n+m} 次ユニタリー行列 U_f が存在し、任意の $x \in \{0,1\}^n$ と任意の $y \in \{0,1\}^m$ に対し、次が成り立つ。

$$U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle.$$

□

問 20. 定理 *2.2.1* を証明せよ。 □

定理 2.2.1 の U_f は、n qubit の量子系（左の量子レジスタ）と m qubit の量子系（右の量子レジスタ）からなる $n+m$ qubit の量子系に、時間発展をもたらすものである。特に、$y = 0^m (\in \{0,1\}^m)$ とおくと、次が成り立つ。

$$U_f(|x\rangle \otimes |0^m\rangle) = |x\rangle \otimes |f(x)\rangle. \tag{2.12}$$

この式の意味するところは次の通りである。左の量子レジスタが状態 $|x\rangle$ にあり、右の量子レジスタが状態 $|0^m\rangle$ にあるとき、U_f を 2 つの量子レジスタからなる全系に施すと、左の量子レジスタのビット列 x に対し、まず $f(x)$ の値が計算され、それが右の量子レジスタに格納される。即ち、これは、x から $f(x)$ を計算する時間発展である。

問 21. 行列のテンソル積は次の性質を持つことを証明せよ。

(i) $(\alpha A) \otimes B = A \otimes (\alpha B) = \alpha(A \otimes B)$ （ここで α は任意の複素数),

(ii) $A \otimes (B + C) = A \otimes B + A \otimes C, \quad (A + B) \otimes C = A \otimes C + B \otimes C.$ □

さて、n qubit の量子系（左の量子レジスタ）の状態が、次のように、あらゆる n ビット列の重ね合わせの状態になっていたものとする。

$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle. \tag{2.13}$$

ここで、$1/\sqrt{2^n}$ は $|\psi_0\rangle$ を規格化するための因子である。全系が状態 $|\psi_0\rangle \otimes |0^m\rangle$ にあるとき、U_f を施すと次のような時間発展となる。

$$\begin{aligned}
U_f(|\psi_0\rangle \otimes |0^m\rangle) &= U_f\left(\left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\right) \otimes |0^m\rangle\right) = \frac{1}{\sqrt{2^n}} U_f\left(\left(\sum_{x \in \{0,1\}^n} |x\rangle\right) \otimes |0^m\rangle\right) &(2.14)\\
&= \frac{1}{\sqrt{2^n}} U_f\left(\sum_{x \in \{0,1\}^n} (|x\rangle \otimes |0^m\rangle)\right) = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} U_f(|x\rangle \otimes |0^m\rangle) &(2.15)\\
&= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |f(x)\rangle. &(2.16)
\end{aligned}$$

ここで、問 21 の結果と式 (2.12) を使った。

上の計算では、U_f の適用は式 (2.12) と同じく 1 回きりなのに、式 (2.16) を見ると、あらゆる $x \in \{0,1\}^n$ に対して、$f(x)$ の値が計算されていることがわかる。n ビット列 x は 2^n 通りあるのに、そのそれぞれに対する $f(x)$ の値が、たった 1 回の U_f の適用で完了してしまったのである。これが**量子並列性**と呼ばれるもので、量子計算機のスピードの源である。しかしながら、量子力学の公理 3 より、U_f のこの適用の直後、状態 (2.16) にある全系を、正規直交規定 $\{|x\rangle \otimes |y\rangle\}$ $(x \in \{0,1\}^n, y \in \{0,1\}^m)$ に関して測定すると、測定結果として得られるのは、一対の $x, f(x)$ だけである。従って、量子並列性を有効に役立てるためには、別の工夫が必要である。そのような工夫が可能であり、量子並列的に計算された指数関数的に多くの計算結果を首尾よく取り出せる場合だけ、量子計算は、古典計算に対して高速なものとなる。それが起こりえる場合が、素因数分解であり、この事実は、1994 年に Peter W. Shor によって発見された。

問 **22.**

(i) ベクトル $|x\rangle$ $(x \in \{0,1\}^n)$ は、$\mathbb{C}^{2^n}$ の正規直交基底であることを証明せよ。（ヒント：定理 *1.4.2* を繰り返し使う）

(ii) *(i)* の結果を用い、$|\psi_0\rangle$ が規格化されていることを証明せよ。 □

Shor の量子素因数分解アルゴリズムでは、モジュラー冪（法冪）計算

$$a \mapsto y^a \bmod N \tag{2.17}$$

を量子計算機上で行う。ここで、a は非負整数、y は正整数、N は素因数分解しようとしている合成数 $N = pq$ であり（p と q は異なる素数）、$y < N$ と $a < 2N^2$ を満たしている。$y^a \bmod N$ は、y^a を N で割った余りである。

定理 2.2.1 の f として、$f(a) = y^a \bmod N$ を選ぶと、次が成り立つ（我々は、ビット列と非負整数を同一視していることに注意）。

$$U_{y,N}(|a\rangle \otimes |b\rangle) = |a\rangle \otimes |b \oplus (y^a \bmod N)\rangle. \tag{2.18}$$

ここで、$U_{y,N}$ は y と N によって定まるユニタリー行列である。

さて、通常の（古典的な）モジュラー冪計算 (2.17) は、$O((\log_2 N)^3)$ 個の基本論理ゲートからなる論理回路によって行うことができる。モジュラー冪計算を実現するそれらの基本論理ゲートを、ある系統的な方法に従い、基本量子ゲートで置き換えることが可能である。但し、その際、ゲートの数は定数倍だけ増える（また、計算に必要な qubit 数も定数倍だけ増える）。しかし、増加は定数倍なので、ユニタリー行列 $U_{y,N}$ は、$O((\log_2 N)^3)$ 回の基本量子ゲートの適用により実現可能なことが、このような措置を行った結果として、証明できる。

Shor の量子素因数分解アルゴリズムでは、モジュラー冪計算を量子並列的に行う。量子計算においては、計算時間は、qubit に施した基本量子ゲートの数で計るので、この量子並列的なモジュラー冪計算には、$O((\log_2 N)^3)$ ステップを要することになる。この計算が、Shor の量子素因数分解アルゴリズムにおいて、最も計算時間が掛かる部分である。

式 (2.18) より、モジュラー冪の量子並列的な計算は、次のように表現される。

$$U_{y,N}\left(\left(\frac{1}{\sqrt{2^n}}\sum_{a=0}^{2^n-1}|a\rangle\right)\otimes|0\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{a=0}^{2^n-1}|a\rangle \otimes |y^a \bmod N\rangle. \tag{2.19}$$

2.3 量子フーリエ変換

正整数 n に対し、2^n 次正方行列 QFT_n を次のように定義する。

$$\mathrm{QFT}_n = \frac{1}{\sqrt{q}}\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{(q-1)} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(q-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{(q-1)} & \omega^{(q-1)2} & \dots & \omega^{(q-1)^2} \end{pmatrix}. \tag{2.20}$$

ここで、$q = 2^n, \omega = e^{2\pi i/q}$ である。QFT_n は**量子フーリエ変換**と呼ばれ、Shor の量子素因数分解アルゴリズムの心臓部を形成する。

補題 2.3.1. a が整数で $|a| < q$ のとき、次が成り立つ。

$$\sum_{c=0}^{q-1} e^{2\pi iac/q} = \begin{cases} q & (a = 0 \text{ のとき}), \\ \\ 0 & (a \neq 0 \text{ のとき}). \end{cases} \tag{2.21}$$

証明. $a = 0$ のとき、$\sum_{c=0}^{q-1} e^{2\pi iac/q} = \sum_{c=0}^{q-1} 1 = q$. 一方、$a \neq 0$ のときには、$0 < |a/q| < 1$ であり、$e^{2\pi ia/q} \neq 1$ なので、等比数列の和の公式より、

$$\sum_{c=0}^{q-1} e^{2\pi iac/q} = \sum_{c=0}^{q-1} (e^{2\pi ia/q})^c = \frac{(e^{2\pi ia/q})^q - 1}{e^{2\pi ia/q} - 1} = \frac{e^{2\pi ia} - 1}{e^{2\pi ia/q} - 1} = \frac{1 - 1}{e^{2\pi ia/q} - 1} = \frac{0}{e^{2\pi ia/q} - 1} = 0. \tag{2.22}$$

□

定理 2.3.2. QFT_n はユニタリー行列である。

証明. $\mathrm{QFT}_n^\dagger \mathrm{QFT}_n = I$ を示せば十分である（それが言えれば、線型代数学より、自動的に $\mathrm{QFT}_n \mathrm{QFT}_n^\dagger = I$ が成り立つ）。行列 $\mathrm{QFT}_n^\dagger \mathrm{QFT}_n$ の第 (j, k)-要素 $(\mathrm{QFT}_n^\dagger \mathrm{QFT}_n)_{jk}$ を計算する。

$$(\mathrm{QFT}_n^\dagger \mathrm{QFT}_n)_{jk} = \sum_{l=1}^{q} (\mathrm{QFT}_n^\dagger)_{jl} (\mathrm{QFT}_n)_{lk} = \sum_{l=1}^{q} \overline{(\mathrm{QFT}_n)_{lj}} (\mathrm{QFT}_n)_{lk}. \tag{2.23}$$

QFT_n の第 (l, j)-要素 $(\mathrm{QFT}_n)_{lj}$ は $\frac{1}{\sqrt{q}}\omega^{(l-1)(j-1)}$ なので、

$$\begin{aligned} (\mathrm{QFT}_n^\dagger \mathrm{QFT}_n)_{jk} &= \sum_{l=0}^{q} \overline{\frac{1}{\sqrt{q}}\omega^{(l-1)(j-1)}} \frac{1}{\sqrt{q}}\omega^{(l-1)(k-1)} = \frac{1}{q}\sum_{c=0}^{q-1} \overline{\omega^{(j-1)c}} \omega^{(k-1)c} & (2.24) \\ &= \frac{1}{q}\sum_{c=0}^{q-1} e^{-2\pi i(j-1)c/q} e^{2\pi i(k-1)c/q} = \frac{1}{q}\sum_{c=0}^{q-1} e^{2\pi i(k-j)c/q} & (2.25) \end{aligned}$$

となる。従って、$|k - j| < q$ に注意し、補題 2.3.1 を用いると、

$$(\mathrm{QFT}_n^\dagger \mathrm{QFT}_n)_{jk} = \frac{1}{q}\sum_{c=0}^{q-1} e^{2\pi i(k-j)c/q} = \begin{cases} \frac{q}{q} = 1 & (j = k \text{ のとき}), \\ \\ \frac{0}{q} = 0 & (j \neq k \text{ のとき}) \end{cases} \tag{2.26}$$

となり、$\mathrm{QFT}_n^\dagger \mathrm{QFT}_n = I$ が成り立つ。 □

さて、$0 \leq a < 2^n$ なる整数 a に対し、次が成り立つ。

$$|a\rangle = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{2.27}$$

ここで、$|a\rangle \in \mathbb{C}^{2^n}$ であり、1 が現れているのは $|a\rangle$ の第 $a + 1$ 成分であり、その他の成分は全て 0 になっている。また、我々の約束により、整数 a は、n ビット列とも解釈されている。例えば、$n = 2$ の場合、式 (1.9)

は次のように書き直すことができる。従って、この場合、確かに式 (2.27) が成り立っている。

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |3\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{2.28}$$

問 23. 一般の n に対し、式 (2.27) を証明せよ。 □

定理 2.3.3. 量子フーリエ変換 QFT_n に対し、次が成り立つ。

$$\mathrm{QFT}_n\,|a\rangle = \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i ac/q} |c\rangle. \tag{2.29}$$

証明. 式 (2.27) より、$\mathrm{QFT}_n\,|a\rangle$ は次のように計算される。

$$\begin{aligned}
\mathrm{QFT}_n\,|a\rangle &= \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{(q-1)} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(q-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{(q-1)} & \omega^{(q-1)2} & \dots & \omega^{(q-1)^2} \end{pmatrix} |a\rangle = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 \\ \omega^a \\ \omega^{2a} \\ \vdots \\ \omega^{(q-1)a} \end{pmatrix} & (2.30) \\
&= \frac{1}{\sqrt{q}} \left[\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \omega^a \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \omega^{2a} \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \omega^{(q-1)a} \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right] & (2.31) \\
&= \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} \omega^{ca} |c\rangle = \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i ac/q} |c\rangle. & (2.32)
\end{aligned}$$

□

QFT_n は、n qubit の量子系に作用し、時間発展を引き起こすユニタリー行列であるが、ここで非常に重要なことは、QFT_n は $O(n^2)$ 回の基本量子ゲートの適用により実現できる、ということである。その基本ゲートとは、1 qubit に作用するアダマールゲート H、及び 2 qubit に作用するユニタリー行列 B_{jk} $(0 \le j < k < n)$ である。

1 qubit の量子系に作用する次のユニタリー行列 H は、アダマール (Hadamard) ゲートと呼ばれ、基本量子ゲートの一つである。

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.33}$$

アダマールゲート H が状態 $|0\rangle, |1\rangle$ に作用すると、その直後の状態は次のように与えられる。

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle, \qquad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle. \tag{2.34}$$

このように、アダマールゲートは、$|0\rangle$ と $|1\rangle$ の重ね合わせ状態を作るなどの目的にも利用できる。なお、$H^{-1} = H^\dagger = H$ に注意。

問 24. アダマールゲート H がユニタリー行列であることを確認せよ。また、式 (2.34) を確認せよ。 □

2 qubit の量子系に作用するユニタリー行列 B_{jk} $(0 \leq j < k < n)$ は、次のように定義される。

$$B_{jk} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta_{jk}} \end{pmatrix}. \tag{2.35}$$

但し、$\theta_{jk} = \pi/2^{k-j}$ である。B_{jk} $(0 \leq j < k < n)$ も、基本量子ゲートの一つである。B_{jk} が状態 $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ に作用すると、その直後の状態は次のように与えられる。

$$B_{jk}|00\rangle = |00\rangle, \quad B_{jk}|01\rangle = |01\rangle, \quad B_{jk}|10\rangle = |10\rangle, \quad B_{jk}|11\rangle = e^{i\theta_{jk}}|11\rangle. \tag{2.36}$$

即ち、B_{jk} は、これら 4 つのベクトルのうち、ベクトル $|11\rangle$ に作用するときのみ、係数 $e^{i\theta_{jk}}$ を生じさせる。しかし、他のベクトルに対しては、変化を与えない。

問 25. B_{jk} がユニタリー行列であることを確認せよ。また、式 (2.36) を確認せよ。 □

やや象徴的な書き方をすると、n qubit の任意の状態 $|\psi\rangle$ に対して量子フーリエ変換 QFT_n を施した結果、生じる状態 $\mathrm{QFT}_n\,|\psi\rangle$ は、次のように、基本量子ゲート H、及び B_{jk} を $|\psi\rangle$ に順々に施すことより実現できる（施す順序は左から右である）。

$$H_n; B_{n-1,n}, H_{n-1}; B_{n-2,n}, B_{n-2,n-1}, H_{n-2}; \ldots ; B_{1,n}, B_{1,n-1}, B_{1,n-2}, \ldots, B_{1,3}, B_{1,2}, H_1 \tag{2.37}$$

H_j は、n qubit のうち、第 j 番目の 1 qubit に作用する H であり、B_{jk} は、n qubit のうち、第 j 番目と第 k 番目の 2 qubit に作用する（ここで、第 1 番目の 1 qubit が二進表示の LSB、即ち 1 の位に対応するとしている）。従って、量子フーリエ変換 QFT_n の実現のために必要な基本量子ゲートの数は $O(n^2)$ である。故に、QFT_n という時間発展を生じさせるのに掛かる計算ステップは、n について 2 次の多項式である。

問 26. (2.37) は、いくつの基本量子ゲートからなっているか、数えよ。そして、その数は $O(n^2)$ であることを確認せよ。 □

第3章　Shorの素因数分解量子アルゴリズム

3.1　準備

以下で、N は異なる2つの奇素数 p, q の積とする。即ち、$N = pq$ かつ p, q は3以上で $p \neq q$ なる2つの素数とする。N が与えられたとき、その素因数である p と q を見出すことが、素因数分解の問題である。もし多項式時間で N の素因数分解を行うことが出来れば、RSA暗号も多項式時間で破られてしまう。なお、現在用いられている1024ビットのRSA暗号では、$N \sim 2^{1024}$ であり、$p \sim q$ となるように p, q は選ばれるので、$p, q \sim 2^{512}$ である。

整数 a, b に対して、$\gcd(a, b)$ とは、a と b の最大公約数のことである。

定義 3.1.1. $\gcd(y, N) = 1$ のとき、即ち、整数 y と N が互いに素のとき、$y^r \equiv 1 \bmod N$ を満たす最小の正整数 r $(r \geq 1)$ を、$y \bmod N$ の位数 *(order)* と呼ぶ。 □

$\gcd(y, N) = 1$ のとき、オイラーの定理により $y^{\varphi(N)} \equiv 1 \bmod N$ であり、また、オイラーの関数 $\varphi(N)$ の定義から $\varphi(N) < N$ である。従って、$\gcd(y, N) = 1$ のとき、$y \bmod N$ の位数は必ず存在し、それは N より小さい。

例 3.1.2 (位数)**.** $N = 15, y = 7$ の場合に、$y \bmod N$ の位数について考えよう。$\gcd(7, 15) = 1$ なので、$7 \bmod 15$ の位数は定義される。それでは、$7 \bmod 15$ の位数を求めてみよう。a の値を1から15まで変化させて、$7^a \bmod 15$ の値をそれぞれ順番に計算してみると、下の表 *3.1* のようになる。ここで、$7^a \bmod 15$ とは、7^a を15で割った余りである。

表 3.1: a の値を1から15まで変化させたときの $7^a \bmod 15$ の値の変化

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$7^a \bmod 15$	7	4	13	1	7	4	13	1	7	4	13	1	7	4	13

従って、表 *3.1* より、$7^a \bmod 15 = 1$（即ち、$7^a \equiv 1 \bmod 15$）となるのは、$a = 4, 8, 12$ の場合である。この中で最小のものは4なので、$7 \bmod 15$ の位数は4である。

なお、オイラーの定理から、$7^{\varphi(15)} \equiv 1 \bmod 15$ が成り立つが、$\varphi(15) = \varphi(3 \cdot 5) = (3-1)(5-1) = 2 \cdot 4 = 8$ であり、上の表で $a = 8$ のときと一致する。位数4は15よりも小さく、更に $\varphi(15)$ よりも小さいことに注意。 □

$\gcd(y, N) = 1$ のとき、r を $y \bmod N$ の位数とすると、定義によって $y^r \equiv 1 \bmod N$ を満たす。従って、任意の整数 a に対し、$y^{a+r} = y^a y^r \equiv y^a 1 = y^a \bmod N$ となる。ゆえに、$y^{a+r} \equiv y^a \bmod N$ となり、関数 $a \mapsto y^a \bmod N$ は周期 r の関数である。また、位数の定義から、この関数は、r より短い周期を持たない。例えば、例 3.1.2 で調べた $N = 15, y = 7$ の場合では、位数 r は4であったが、表 3.1 を見ると、確かに、$y^a \bmod N$ は周期4で変化していることがわかる。

Shorの素因数分解量子アルゴリズムでは、素因数分解を、$\gcd(y, N) = 1$ となる整数 y をランダムに生成した上で、$y \bmod N$ の位数を求める問題に還元する。そして、位数を求める計算を量子計算機の上で行う。

3.2 Shor のアルゴリズムのメインルーティン

Shor の素因数分解量子アルゴリズムは確率アルゴリズムである。そのメインルーティンは、古典的な通常の計算機上で実行されるものであり、次のように記述される。

Shor の素因数分解量子アルゴリズム

Input: N. （ここで N は、2 つの異なる奇素数 p と q の積）
Output: p, q.

[1] 整数 y $(2 \leq y \leq N-1)$ をランダムに生成する.

[2] $1 < \gcd(y, N)$ ならば, $\gcd(y, N)$ と $N/\gcd(y, N)$ を、p, q として出力して計算終わり.
そうでない場合はステップ [3] へ.

[3] N と y を引数とする量子サブルーティンを量子計算機上で実行し、$y \bmod N$ の位数 r を求める. （但し、正しい位数 r が求まる確率は $1/(C \log_2 \log_2 N)$ 以上である）

[4] もし r が偶数なら, $\gcd(y^{r/2}-1, N)$ と $\gcd(y^{r/2}+1, N)$ を計算し, 共に 1 でも N でもなければ, これらを p, q として出力する.

このメインルーティンは、4 つのステップ [1], [2], [3], [4] からなる。このうち 3 番目のステップ [3] で呼び出される量子サブルーティンが、量子計算機で実行される量子アルゴリズムである。なお、C は、N と y に依らない或る正の実数である。

このアルゴリズムは、確率アルゴリズムであり、計算が終了しても、出力がない場合がある。その場合は、N の素因数 p, q は求まらなかったということである。しかし、出力があった場合には、その出力は、正しい素因数 p, q となっている。

それでは、出力が得られる確率（回答率）の下界を求めよう。そのためには、ステップ [2] で $\gcd(y, N) = 1$ と判定され、ステップ [3] 以下が実行される場合の回答率を求めれば十分である [1]。次節で示されるように、ステップ [3] の量子サブルーティンの実行後に、正しい位数 r が得られる確率は、$1/(C \log_2 \log_2 N)$ 以上である。一方、ステップ [3] で正しい位数 r が得られた場合に、[4] で素因数 p, q が得られる確率を求めるには、次の定理が必要である。

定理 3.2.1. N は異なる *2* つの奇素数 p, q の積とする。整数 y が $2 \leq y \leq N-1$ の範囲で $g(y, N) = 1$ を満たしながらランダムに選ばれる場合、r が偶数であり、かつ、$y^{r/2}-1$ は N で割り切れず、$y^{r/2}+1$ も N で割り切れない確率は $1/2$ 以上である。ここで、r は $y \bmod N$ の位数である。

証明. 参考文献・推奨文献の [10],[2] 参照。[2] の APPENDIX B にある証明がわかりやすい。 □

まず次の点に注意する。r が偶数なら、位数の定義から、$(y^{r/2}-1)(y^{r/2}+1) = y^r - 1 \equiv 0 \bmod N$ となり、$(y^{r/2}-1)(y^{r/2}+1)$ は N で割り切れる。また、$N = pq$ であり、p, q は素数である。従って、次の 4 つのうちのいづれかが成り立つ。

(i) $y^{r/2}-1$ は N で割れ切れる。

(ii) $y^{r/2}-1$ は p で割り切れ、$y^{r/2}+1$ は q で割り切れる。

[1] $\varphi(N) = (p-1)(q-1)$ となるので、ステップ [2] で $1 < \gcd(y, N)$ と判定される確率は $2/\sqrt{N}$ 程度である。従って、現在用いられている RSA 暗号の場合のように $N \sim 2^{1024}$ のときには、この確率は 2^{-511} 程度であり、極めて小さく、ステップ [2] で素因数分解が求まり、計算が終了することは、ほとんど起こり得ない。

(iii) $y^{r/2}-1$ は q で割り切れ、$y^{r/2}+1$ は p で割り切れる。

(iv) $y^{r/2}+1$ は N で割り切れる。

ステップ [3] で正しい位数 r が得られた場合には、定理 3.2.1 より、1/2 以上の確率で、r は偶数であり、かつ、$y^{r/2}-1$ は N で割り切れず、$y^{r/2}+1$ も N で割り切れない、ということになる。従って、このとき、上の (i), (iv) の場合は起こりえず、(ii) か (iii) の場合のみが起こる。よって、ステップ [3] で正しい位数 r が得られた場合には、ステップ [4] で、$\gcd(a^{r/2}-1, N)$ と $\gcd(a^{r/2}+1, N)$ を計算することにより、1/2 以上の確率で、正しい素因数 p と q が得られ、この p, q が出力される。従って、Shor の素因数分解量子アルゴリズムの回答率は、$1/(C\log_2\log_2 N)\times 1/2 = 1/(2C\log_2\log_2 N)$ 以上となる。

一方、Shor の素因数分解量子アルゴリズムの計算時間はどうなるかというと、次の通りに評価される。ステップ [2], [4] の gcd の計算はユークリッドのアルゴリズムを用いることにより、それぞれ $O((\log_2 N)^2)$ 時間で完了する。問題となるのは、量子計算機上で実行されるステップ [3] の計算だが、次節で示されるように、これには、$O((\log_2 N)^3)$ 時間がかかる。メインルーティンの中では、この計算時間が一番大きいので、Shor のアルゴリズムの計算時間は $O((\log_2 N)^3)$ となる。

ここで、多項式時間アルゴリズムの定義を思い出しておこう。一般に、正整数 N を入力とするアルゴリズムが多項式時間アルゴリズムであるとは、ある多項式 $p(x)$ が存在し、任意の正整数 N に対し、N を入力としたときの計算時間が $p(\log_2 N)$ 以下となることである。

上述の通り、Shor のアルゴリズムは、$O((\log_2 N)^3)$ の計算時間をかけ、回答率 $1/(2C\log_2\log_2 N)$ で正しい素因数 p と q を計算する。これは、多項式時間アルゴリズムとして十分である。それは次の理由による。この Shor のアルゴリズムを、十分に大きな正整数 D に対し、$\lceil D\log_2\log_2 N\rceil$ 回繰り返し実行すれば、1 に任意に近い確率で、正しい素因数 p と q が得られる。この反復の結果として得られる新しいアルゴリズムの計算時間は、$O((\log_2 N)^3\log_2\log_2 N)$ であり、これは多項式時間のアルゴリズムである。故に、この新しいアルゴリズムは、1 に任意に近い確率で、正しい素因数 p と q を出力する多項式時間アルゴリズムであり、これで、多項式時間の素因数分解アルゴリズムが得られた。

次節では、ステップ [3] で呼び出される量子サブルーティンを記述し、その解析を行う。この量子サブルーティンは、量子計算機上で実行されるものであり、N と y が（引数として）与えられたときに、$y \bmod N$ の位数 r を計算しようとするものである。そして、特に、上記の Shor の素因数分解量子アルゴリズムの解析で保留としていた次の事実を証明する。

> この量子サブルーティンの計算時間は $O((\log_2 N)^3)$ であり、正しい位数 r を計算する確率は $1/(C\log_2\log_2 N)$ 以上である。

このように、この量子サブルーティンは効率的よく位数計算を行うが、現在のところ、古典的な計算機の上で動くアルゴリズムで、このように効率的な位数計算を行うものは知られていない。（従って、現在のところ、RSA 暗号は安全である。）

3.3 Shor のアルゴリズムの量子サブルーティン

量子サブルーティンは、次の 5 つのステップ [Q1]〜[Q5] で実行される。メインルーティンから、$\gcd(y, N)=1$ となる N と y が渡されたとする。

[Q1] 初期化. $N^2 \le 2^n < 2N^2$ となる正整数 n を選ぶ（以下では、2^n を q とおく）。そして、n qubit の量子系からなる量子レジスタ QR1 を用意し、その量子状態を $|0\rangle$ に設定する。この状態に量子フーリエ変換 QFT_n を適用する。すると次の状態 $|\psi_1\rangle$ が得られる。

$$|\psi_1\rangle = \mathrm{QFT}_n\,|0\rangle = \frac{1}{\sqrt{q}}\sum_{c=0}^{q-1} e^{2\pi i0c/q}|c\rangle = \frac{1}{\sqrt{q}}\sum_{c=0}^{q-1}|c\rangle = \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle. \tag{3.1}$$

ここで、定理 2.3.3 を用いた。従って、$|\psi_1\rangle$ は、2^n 個の状態ベクトル $|b_1 b_2 \dots b_n\rangle$ $(b_1, b_2 \dots, b_n = 0, 1)$ の重ね合わせの状態になっている。$2^n < 2N^2$ より、$n = O(\log_2 N)$ なので、この計算にかかった時間は $O(n^2) = O((\log_2 N)^2)$ である。

[Q2] 量子並列的なモジュラー冪の計算. m qubit の量子系からなる量子レジスタ QR2 を新たに用意し、その量子状態を $|0\rangle$ に設定する。ここで、$m = \lceil \log_2 N \rceil$ である。すると、2 つの量子レジスタ QR1 と QR2 をあわせた全系の量子状態は、ベクトル

$$|\psi_1\rangle \otimes |0\rangle = \left(\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \right) \otimes |0\rangle \tag{3.2}$$

で表される。この全系に式 (2.18) を満たす $U_{y,N}$ を適用すると、式 (2.19) より、次の状態 $|\psi_2\rangle$ が得られる。

$$|\psi_2\rangle = U_{y,N}(|\psi_1\rangle \otimes |0\rangle) = U_{y,N} \left(\left(\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \right) \otimes |0\rangle \right) = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \otimes |y^a \bmod N\rangle. \tag{3.3}$$

この計算では、量子並列的にモジュラー冪計算を行った。この計算にかかった時間は $O((\log_2 N)^3)$ である。

[Q3] 量子レジスタ QR2 の測定. このステップでは、部分系である量子レジスタ QR2 を、正規直交基底 $\{|z\rangle\}$ $(0 \le z \le 2^m - 1)$ に関して測定する。

量子力学の公理 5 を適用し、測定後の状態を求めよう。

まずはじめに、関数 $a \mapsto y^a \bmod N$ は周期 r を持つことに注意すると、任意に l $(0 \le l \le r-1)$ に対し、関数値 $y^a \bmod N$ は、全ての $a = l, l+r, l+2r, \dots, l+A_l r$ に対して同じ値を持つことがわかる。ここで、A_l は、$l + A_l r \le q-1$ となる最大の整数 A_l、即ち、$A_l = \lfloor (q-1-l)/r \rfloor$ である。従って、任意の j $(0 \le j \le A_l)$ に対し、$y^{l+jr} \equiv y^l \bmod N$ となる。よって、状態 $|\psi_2\rangle$ は、次のように書き直すことができる。

$$\begin{aligned}
|\psi_2\rangle &= \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \otimes |y^a \bmod N\rangle && (3.4)\\
&= \frac{1}{\sqrt{q}} \sum_{l=0}^{r-1} \sum_{j=0}^{A_l} |l+jr\rangle \otimes |y^{l+jr} \bmod N\rangle && (3.5)\\
&= \frac{1}{\sqrt{q}} \sum_{l=0}^{r-1} \sum_{j=0}^{A_l} |l+jr\rangle \otimes |y^l \bmod N\rangle. && (3.6)
\end{aligned}$$

この式変形では、はじめに、$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1}$ の中で足されるベクトルの順番を変え、量子レジスタ QR2 のケットベクトル $|y^a \bmod N\rangle$ が同じもの同士でまとめた。その上で、$y^{l+jr} \equiv y^l \bmod N$ を用いた。

従って、量子力学の公理 5 により、正規直交基底 $\{|z\rangle\}$ $(0 \le z \le 2^m - 1)$ に関して測定を行うと、得られる測定値は、$y^0 \bmod N, y^1 \bmod N, \dots, y^{r-1} \bmod N$ のうちのどれかであり、任意の l $(0 \le l \le r-1)$ に対して、測定値 $y^l \bmod N$ が得られた場合、測定直後の全系の状態は、次のベクトルで表されることになる。

$$\frac{1}{\sqrt{A_l+1}} \sum_{j=0}^{A_l} |l+jr\rangle \otimes |y^l \bmod N\rangle = \left(\frac{1}{\sqrt{A_l+1}} \sum_{j=0}^{A_l} |l+jr\rangle \right) \otimes |y^l \bmod N\rangle. \tag{3.7}$$

この測定により、どの測定値が得られようと、その後の計算は同様に進められるので、ここではある特定の測定結果 $y^l \bmod N$ が得られたとする。このとき、量子力学の公理 2 より、量子レジスタ QR1 の状態は、次のベクトル $|\psi_3^l\rangle$ で表される。

$$|\phi_3^l\rangle = \frac{1}{\sqrt{A_l+1}} \sum_{j=0}^{A_l} |l+jr\rangle. \tag{3.8}$$

また、量子レジスタ QR2 の状態は、次のベクトル

$$|y^l \bmod N\rangle \tag{3.9}$$

で表される。なお、以下の計算では、もはや量子レジスタ QR2 は使用しない。今後の計算では、現在 $|\phi_3^l\rangle$ で表される状態にある量子レジスタ QR1 のみを用いる。

[Q4] 量子フーリエ変換の適用. このステップでは、状態 $|\phi_3^l\rangle$ から位数 r を抽出するため、状態 $|\phi_3^l\rangle$ に量子フーリエ変換 QFT_n を適用する。但し、解析を簡単にし、量子フーリエ変換の効果を見やすくするために、以下では次の仮定をおく。

仮定: q/r は整数である。

一般の場合の取扱いは、参考文献・推奨文献の [10],[2] を参照されたい。この仮定の下では、$A_l = q/r - 1$ となり、ベクトル $|\psi_3^l\rangle$ は次のようになる。

$$|\phi_3^l\rangle = \sqrt{\frac{r}{q}} \sum_{j=0}^{M-1} |l + jr\rangle. \tag{3.10}$$

但し、$M = q/r$ とした。

さて、状態 $|\phi_3^l\rangle$ に量子フーリエ変換 QFT_n を適用すると、次の状態 $|\phi_4^l\rangle$ が得られる。

$$\begin{aligned}
|\phi_4^l\rangle = \mathrm{QFT}_n\,|\phi_3^l\rangle &= \sqrt{\frac{r}{q}} \sum_{j=0}^{M-1} \mathrm{QFT}_n\,|l + jr\rangle && (3.11)\\
&= \sqrt{\frac{r}{q}} \sum_{j=0}^{M-1} \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i(l+jr)c/q} |c\rangle && (3.12)\\
&= \frac{\sqrt{r}}{q} \sum_{c=0}^{q-1} \left(\sum_{j=0}^{M-1} e^{2\pi icj/M} \right) e^{2\pi ilc/q} |c\rangle. && (3.13)
\end{aligned}$$

ここで、定理 2.3.3 を用いた。補題 2.3.1 より、次が成り立つことに注意する。

$$\sum_{j=0}^{M-1} e^{2\pi icj/M} = \begin{cases} M & (c \text{ が } M \text{ の倍数のとき}), \\ \\ 0 & (c \text{ が } M \text{ の倍数でないとき}). \end{cases} \tag{3.14}$$

従って、状態 $|\phi_4^l\rangle$ は次のように書き直すことが出来る。

$$\begin{aligned}
|\phi_4^l\rangle &= \frac{\sqrt{r}}{q} \sum_{0 \le k \le (q-1)/M} M e^{2\pi il(kM)/q} |kM\rangle && (3.15)\\
&= \frac{\sqrt{r}}{q} \sum_{k=0}^{r-1} M e^{2\pi il(kM)/q} |kM\rangle && (3.16)\\
&= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{2\pi ilk/r} |kq/r\rangle. && (3.17)
\end{aligned}$$

ここで、$\lfloor (q-1)/M \rfloor = r - 1$ を用いた。

ステップ [Q1] と同様に、この計算にかかった時間は $O(n^2) = O((\log_2 N)^2)$ である。

[Q5] 量子レジスタ QR1 の測定. このステップでは、状態 $|\phi_4^l\rangle$ にある量子レジスタ QR1 を、正規直交基底 $\{|w\rangle\}$ $(0 \le w \le 2^n - 1)$ に関して測定する。まず、自明な等式

$$\left| \frac{1}{\sqrt{r}} e^{2\pi i l k/r} \right|^2 = \frac{1}{r} \tag{3.18}$$

に注意すると、$|\phi_4^l\rangle$ は確かに規格化されていることがわかる。従って、量子力学の公理 3 により、この測定の測定結果は、$0, q/r, 2q/r, \ldots, (r-1)q/r$ のうちのどれかであり、それぞれは同じ確率 $1/r$ で得られることがわかる。

従って、この測定で得られる測定値 c は、ある $k = 0, \ldots, r-1$ に対して $c = kq/r$ と表されるが、仮にこの k に対して $\gcd(k, r) = 1$ が成立したとしよう。q は 2^n のことであり既知なので、測定値 c から有理数 c/q の値が計算できる。このとき、$c/q = k/r$ であり $\gcd(k, r) = 1$ なので、この有理数 c/q を約分すれば、その分母が r である。このようにして、$\gcd(k, r) = 1$ である場合には、測定値 c から $y \bmod N$ の位数 r が求まる。この約分の計算は、ユークリッドのアルゴリズムを用い、（量子計算機ではなく）通常の計算機上で行なわれる。その計算時間は $O((\log_2 q)(\log_2 c)) = O((\log_2 q)^2) = O(n^2) = O((\log_2 N)^2)$ である。

それでは、この測定で $\gcd(k, r) = 1$ となる確率を求めよう。オイラーの関数 $\varphi(r)$ の定義から、この確率は $\varphi(r)/r$ である。$\varphi(r)$ については、不等式

$$\varphi(r) \ge \frac{r}{6 \ln \ln r} \qquad (r \ge 5) \tag{3.19}$$

が成り立つが、これを用いると、

$$\varphi(r)/r \ge \frac{1}{6 \ln \ln r} > \frac{1}{6 \ln \ln N} \tag{3.20}$$

となる。ここで $r \le \varphi(N) < N$ を使った。また、ln は自然対数である。上式で自然対数を、底を 2 とする対数に変換すると次が成り立つ。

$$\frac{1}{6 \ln \ln N} \ge \frac{1}{C \log_2 \log_2 N}. \tag{3.21}$$

ここで、C は N に依らない或る正の実数である。

従って、この測定を行って得られた測定値 c から、正しい位数 r が求められる確率は、$1/(C \log_2 \log_2 N)$ 以上である。

以上の量子サブルーティンでは、ステップ [Q2] のモジュラー冪の計算時間が一番長く、$O((\log_2 N)^3)$ なので、量子サブルーティンの全体としての計算時間は $O((\log_2 N)^3)$ となる。また、今見たように、正しい位数 r を計算する確率は $1/(C \log_2 \log_2 N)$ 以上である。これで、Shor の素因数分解量子アルゴリズムは、多項式時間の量子アルゴリズムであることがわかった。

参考文献・推奨文献

[1] P. A. M. Dirac. *The Principles of Quantum Mechanics*, 4th Edition. Oxford University Press, London, 1958. ISBN: 978-4-622-02512-2

[2] Artur Ekert and Richard Jozsa. Qunatum computation and Shor's factoring algorithm. *Reviews of Modern Physics*, Vol.68, No.3 (1996), pp.733–753. Available at URL: `http://dx.doi.org/10.1103/RevModPhys.68.733`

[3] Jozef Gruska. *Quantum Computing*. McGraw-Hill, London, 1999. ISBN: 0-07-709503-0

[4] 石坂智, 小川朋宏, 河内亮周, 木村元, 林正人. 「量子情報科学入門」. 共立出版, 2012. ISBN: 978-4-320-12299-4

[5] 宮野健次郎, 古澤明. 「量子コンピュータ入門」, 第 2 版. 日本評論社, 2016. ISBN: 978-4-535-78805-3

[6] 中原幹夫. 「量子物理学のための線形代数 — ベクトルから量子情報へ」. 培風館, 2016. ISBN: 4-563-02516-X

[7] Michael A. Nielsen and Issac L. Chuang. *Quantum Computation and Quantum Information*, 10th Aniversary Edition. Cambridge University Press, Cambridge, 2010. ISBN: 978-1-107-00217-3 Hardback

[8] 岡本龍明, 山本博資. シリーズ／情報科学の数学「現代暗号」. 産業図書, 1997. ISBN: 4-7828-5353-X

[9] John Preskill. *Quantum Computation*. Course notes available at URL: `http://www.theory.caltech.edu/people/preskill/ph219/`

[10] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, Vol.26, No.5 (1997), pp.1484–1509. Available at URL: `http://dx.doi.org/10.1137/S0097539795293172`

[11] 上坂吉則. 「量子コンピュータの基礎数理」. コロナ社, 2000. ISBN: 978-4-339-02376-3

[12] Umesh Vazirani. *Quantum Computation*, Spring 2007. Course notes available at URL: `http://www.cs.berkeley.edu/~vazirani/quantum.html`

文献 [10] は Shor の量子素因数分解アルゴリズムの原論文である。文献 [2] はその概説で取り付きやすい。文献 [10, 2] は、中部大学春日井キャンパス内なら、次の「中部大学付属三浦記念図書館 電子ジャーナルポータル」

`http://qd9sh5ye9c.search.serialssolutions.com/`

から、その電子版を入手できる。なお、[2] については（中部大学春日井キャンパス内なら）`http://dx.doi.org/10.1103/RevModPhys.68.733` から直接入手可能である。