

## 第 1 章

# 概論

演習 1.1 Deutsh-Jozsa の問題を誤り確率  $\epsilon < 1/2$  で解くには,  $O(3)$  の時間計算量が必要.

演習 1.2

## 第 2 章

# 量子力学入門

演習 2.1

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \end{pmatrix} - \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 0$$

演習 2.2 入出力基底が共に,

$$|0\rangle, |1\rangle$$

のとき,

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

上記の入出力基底を, 規定の変換行列  $U$

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

を用いて,

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

に取り替えると, 表現行列は,

$$U^{-1}AU = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

演習 2.3 問題文の  $A, B$  というオペレーターを  $T_A, T_B$  と書き, 問題文で与えられた基底に対するその表現行列をそれぞれ  $A, B$  と書くとする,

$$T_B T_A |v_i\rangle = T_B A_{ji} |w_j\rangle = A_{ji} B_{kj} |x_k\rangle = B_{kj} A_{ji} |x_k\rangle$$

なので,  $T_B T_A$  の基底  $\{|v_i\rangle\}$  から  $\{|x_i\rangle\}$  への表現行列は  $BA$ .

演習 2.4 任意の状態  $|\psi\rangle$  は,  $V$  の基底  $\{|v_i\rangle\}$  を用いて,

$$|\psi\rangle = \sum_i c_i |v_i\rangle$$

とかけ,  $V \rightarrow V$  の単位オペレーター  $I$  は,  $|\psi\rangle$  に対して,

$$I|\psi\rangle = |\psi\rangle$$

つまり

$$\sum_{i,j} c_i I_{ji} |v_j\rangle = \sum_j c_j |v_j\rangle$$

のように作用するので,

$$0 = \sum_{i,j} \left( c_i I_{ji} - \frac{c_j}{\dim V} \right) |v_j\rangle$$

が成立. よって, 基底の1次独立性から全ての  $j$  に対して,

$$c_j = \sum_i c_i I_{ji}$$

つまり

$$I_{ij} = \delta_{ij}.$$

ゆえに,  $I$  の表現行列は単位行列.

演習 2.5 式 (2.13) の内積の定義を満たすか確かめれば良い.

演習 2.6

$$(\lambda_i |w_i\rangle, |v\rangle) = (|v\rangle, \lambda_i |w_i\rangle)^* = \lambda_i^* (|v\rangle, |w_i\rangle)^* = \lambda_i^* (|w_i\rangle, |v\rangle)$$

演習 2.7 式 (2.14) で定義された  $C^2$  の標準内積を用いることにすると,

$$\langle w|v\rangle = 0.$$

$|w\rangle, |v\rangle$  を規格化すると, それぞれ

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

演習 2.8  $d$  次元の計量線型空間  $V$  の基底  $\{|w_k\rangle\}_{k=1}^d$  に対して,

$$|v_k\rangle = \begin{cases} \frac{w_k}{\|w_k\|} & (k=1) \\ \frac{|w_k\rangle - \sum_{i=1}^{k-1} \langle v_i|w_k\rangle |v_i\rangle}{\| |w_k\rangle - \sum_{i=1}^{k-1} \langle v_i|w_k\rangle |v_i\rangle \|} & (\text{otherwise}) \end{cases}$$

で定義された  $\{|v_k\rangle\}_{k=1}^d$  が  $V$  の正規直交基底になっていること示す.

正規性は, 明らかである.

直交性について, 帰納法で示す.  $k=1$  のとき,

$$\langle v_1|v_2\rangle \propto \langle v_1|w_2\rangle - \langle v_1|w_2\rangle \langle v_1|v_1\rangle = 0.$$

また,  $i \neq j$  ( $i, j = 1, 2, \dots, k$ ) なる任意の  $i, j$  で,

$$\langle v_j|v_i\rangle = 0$$

だと仮定すると,

$$\langle v_j|v_{k+1}\rangle \propto \langle v_j|w_{k+1}\rangle - \sum_{i=1}^k \langle v_i|w_{k+1}\rangle \langle v_j|v_i\rangle = \langle v_j|w_{k+1}\rangle - \langle v_j|w_{k+1}\rangle \langle v_j|v_j\rangle = 0.$$

以上より,  $i, j = 1, 2, \dots, d$  に対して,

$$\langle v_i | v_j \rangle = \delta_{ij}$$

が言えた. したがって,  $\{|v_k\rangle\}_{k=1}^d$  は線形独立で,  $V$  を張る. つまり,  $\{|v_k\rangle\}_{k=1}^d$  は  $V$  の正規直交基底.

### 演習 2.9

$$\begin{aligned}\sigma_0 &= |0\rangle\langle 0| + |1\rangle\langle 1| \\ \sigma_1 &= |0\rangle\langle 1| + |1\rangle\langle 0| \\ \sigma_2 &= -i|0\rangle\langle 1| + i|1\rangle\langle 0| \\ \sigma_3 &= |0\rangle\langle 0| - |1\rangle\langle 1|\end{aligned}$$

演習 2.10 式 (2.25) より,

$$|v_j\rangle\langle v_k| = \sum_{i,l} |v_i\rangle\langle v_i|v_j\rangle\langle v_k|v_l\rangle\langle v_l| = \sum_{i,l} |v_i\rangle\delta_{ij}\delta_{kl}\langle v_l|$$

なので, 正規直交基底の下での  $|v_j\rangle\langle v_k|$  表現行列  $A$  の成分  $A_{il}$  は,

$$A_{il} = \delta_{ij}\delta_{kl}.$$

演習 2.11  $X$  の固有値は  $1, -1$  で, 対応する規格化された固有ベクトルはそれぞれ,

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

$Y$  の固有値は  $1, -1$  で, 対応する規格化された固有ベクトルはそれぞれ,

$$\frac{1}{\sqrt{2}} \begin{pmatrix} i \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ -1 \end{pmatrix}.$$

$Z$  の固有値は  $1, -1$  で, 対応する規格化された固有ベクトルはそれぞれ,

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

### 演習 2.12

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

の固有方程式は,

$$(\lambda - 1)^2 = 0$$

となり,  $A$  の固有空間の直和  $W$  として,

$$W = \left\{ t \begin{pmatrix} 0 \\ 1 \end{pmatrix} \middle| t \in \mathbb{C} \right\} \neq \mathbb{C}^2$$

より,  $A$  は対角化不可能.

### 演習 2.13

$$(|w\rangle\langle v|)^\dagger = \langle v|^\dagger |w\rangle^\dagger = |v\rangle\langle w|$$

演習 2.14 任意の  $|v\rangle, |w\rangle \in V$  に対して,

$$\left( \left( \sum_i a_i A_i \right)^\dagger |v\rangle, |w\rangle \right) = \left( |v\rangle, \sum_i a_i A_i |w\rangle \right) = \sum_i a_i (|v\rangle, A_i |w\rangle) = \sum_i (a_i^* |v\rangle, A_i |w\rangle) = \left( \sum_i a_i^* A_i^\dagger |v\rangle, |w\rangle \right)$$

であり,  $|w\rangle$  は任意なので,

$$\left( \sum_i a_i A_i \right)^\dagger = \sum_i a_i^* A_i^\dagger$$

演習 2.15 任意の  $|v\rangle, |w\rangle \in V$  に対して,

$$(|v\rangle, A |w\rangle) = (A^\dagger |v\rangle, |w\rangle) = (|v\rangle, (A^\dagger)^\dagger |w\rangle)$$

演習 2.16

$$P^2 = \sum_i \sum_j |i\rangle \langle i| |j\rangle \langle j| = \sum_i \sum_j |i\rangle \delta_{ij} \langle j| = \sum_i |i\rangle \langle i| = P$$

演習 2.17 「正規行列  $A$  の固有値が実数  $\iff$  正規行列  $A$  は Hermite」を示す.

$\implies$  スペクトル分解をすると,  $a \in \mathbb{R}$  として,

$$A = \sum_a a |a\rangle \langle a|$$

とかけるので,

$$A^\dagger = \sum_a a^* |a\rangle \langle a| = \sum_a a |a\rangle \langle a| = A.$$

$\impliedby$   $A$  が Hermite とする.  $A$  の固有値  $\lambda$  と対応する固有ベクトル  $|v\rangle$  として,

$$\lambda = (|v\rangle, A |v\rangle) = (A |v\rangle, |v\rangle) = \lambda^*$$

より,  $\lambda$  は実数であることが言えた.

演習 2.18 ユニタリ行列  $U$  の固有値  $\lambda$  と対応する固有ベクトル  $|v\rangle$  として,

$$\langle v|v\rangle = (U |v\rangle, U |v\rangle) = |\lambda|^2 \langle v|v\rangle$$

で,  $\langle v|v\rangle \neq 1$  なので,

$$|\lambda| = 1.$$

演習 2.19 Pauli 行列の定義より明らか.

演習 2.20 完全性条件を挟んで,

$$A''_{ij} = \langle w_i | A | w_j \rangle = \sum_k \sum_l \langle w_i | v_k \rangle \langle v_k | A | v_l \rangle \langle v_l | w_j \rangle = \sum_k \sum_l \langle w_i | v_k \rangle A'_{kl} \langle v_l | w_j \rangle$$

演習 2.21  $M$  が Hermite ならば, 式 (2.37) = 式 (2.41) が明らか.

演習 2.22 Hermite オペレータ  $A$  の異なる固有値  $\lambda_i, \lambda_j$  ( $\lambda_i \neq \lambda_j$ ) と対応する固有ベクトル  $|i\rangle, |j\rangle$  とすると,

$$0 = (|i\rangle, A |j\rangle) - (A |i\rangle, |j\rangle) = (\lambda_j - \lambda_i^*) \langle i|j\rangle \rightarrow \langle i|j\rangle = 0$$

演習 2.23 射影オペレータ  $P$  の固有値  $\lambda$  と対応する固有ベクトル  $|v\rangle$  とすると,  $P^2 = P$  より,

$$0 = (P^2 - P)|v\rangle = \lambda(\lambda - 1)|v\rangle.$$

左から  $\langle v|$  をかけて,

$$0 = \lambda(\lambda - 1) \rightarrow \lambda = 0, 1.$$

演習 2.24 任意のオペレータ  $A$  は,

$$A = \frac{A + A^\dagger}{2} + i\frac{A - A^\dagger}{2i}$$

の形でかける. また, 任意の  $|v\rangle$  に対して, Hermite オペレータ  $H$  の期待値は,

$$(|v\rangle, H|v\rangle) = (H^\dagger|v\rangle, |v\rangle) = (H|v\rangle, |v\rangle) = (|v\rangle, H|v\rangle)^*$$

と実となるので,

$$\langle v|\frac{A + A^\dagger}{2}|v\rangle, \langle v|\frac{A - A^\dagger}{2i}|v\rangle \in \mathbb{R}.$$

よって,  $A$  を正のオペレーターとすると, 任意の  $|v\rangle$  に対して,

$$0 \leq \langle v|A|v\rangle = \langle v|\frac{A + A^\dagger}{2}|v\rangle + i\langle v|\frac{A - A^\dagger}{2i}|v\rangle \rightarrow \langle v|\frac{A - A^\dagger}{2i}|v\rangle = 0.$$

$|v\rangle$  は, 任意なので,  $A = A^\dagger$  が成り立つ.

演習 2.25

$$\langle v|A^\dagger A|v\rangle = (|v\rangle, A^\dagger A|v\rangle) = (A|v\rangle, A|v\rangle) = \|A|v\rangle\|^2 \geq 0.$$

演習 2.26

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

とする. テンソル積の形で書くと,

$$\begin{aligned} |\psi\rangle^{\otimes 2} &= \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2} \\ |\psi\rangle^{\otimes 3} &= \frac{|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle}{2\sqrt{2}}. \end{aligned}$$

Kronecker 積の形で書くと,

$$\begin{aligned} |\psi\rangle^{\otimes 2} &= \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \\ |\psi\rangle^{\otimes 3} &= \frac{1}{2\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}. \end{aligned}$$

演習 2.27

$$X \otimes Z = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad I \otimes X = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad X \otimes I = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

$I \otimes X \neq X \otimes I$  にあるようにテンソル積は非可換.

演習 2.28 テンソル積の転置共役  $(A \otimes B)^\dagger$  を,

$$\left( (A \otimes B)^\dagger (|v_1\rangle \otimes |w_1\rangle), |v_2\rangle \otimes |w_2\rangle \right) = (|v_1\rangle \otimes |w_1\rangle, (A \otimes B) (|v_2\rangle \otimes |w_2\rangle))$$

で定義すると,

$$\begin{aligned} \left( (A \otimes B)^\dagger (|v_1\rangle \otimes |w_1\rangle), |v_2\rangle \otimes |w_2\rangle \right) &= (|v_1\rangle \otimes |w_1\rangle, A |v_2\rangle \otimes B |w_2\rangle) \\ &= (|v_1\rangle, A |v_2\rangle) (|w_1\rangle, B |w_2\rangle) \\ &= (A^\dagger |v_1\rangle, |v_2\rangle) (B^\dagger |w_1\rangle, |w_2\rangle) \\ &= ((A^\dagger \otimes B^\dagger) (|v_1\rangle \otimes |w_1\rangle), |v_2\rangle \otimes |w_2\rangle). \end{aligned}$$

$|v_1\rangle \otimes |w_1\rangle, |v_2\rangle \otimes |w_2\rangle$  は任意なので,  $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$  を得る.

テンソル積の複素共役  $(A \otimes B)^*$  を, オペレータ形式でどう定義すればわからないので, Kronecker 積の形で考える.

$$(A \otimes B)^* = \begin{pmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{pmatrix}^* = \begin{pmatrix} A_{11}^*B^* & A_{12}^*B^* & \dots & A_{1n}^*B^* \\ A_{21}^*B^* & A_{22}^*B^* & \dots & A_{2n}^*B^* \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}^*B^* & A_{m2}^*B^* & \dots & A_{mn}^*B^* \end{pmatrix} = A^* \otimes B^*$$

テンソル積の転置  $(A \otimes B)^T$  を,

$$(A \otimes B)^T = (A \otimes B)^{*\dagger}$$

で定義すると, 上で示したテンソル積の転置共役, 複素共役に対する分配性から,

$$(A \otimes B)^T = (A \otimes B)^{*\dagger} = (A^* \otimes B^*)^\dagger = A^{*\dagger} \otimes B^{*\dagger} = A^T \otimes B^T.$$

演習 2.29  $U_1, U_2$  がユニタリするとき,

$$(U_1 \otimes U_2)(U_1 \otimes U_2)^\dagger = (U_1 \otimes U_2)(U_1^\dagger \otimes U_2^\dagger) = (U_1 U_1^\dagger) \otimes (U_2 U_2^\dagger) = I_1 \otimes I_2$$

演習 2.30  $A_1, A_2$  が Hermitian のとき,

$$(A_1 \otimes A_2)^\dagger = A_1^\dagger \otimes A_2^\dagger = A_1 \otimes A_2$$

演習 2.31  $A, B$  が正のオペレータのとき, 任意のベクトル  $|v\rangle \otimes |w\rangle$  に対して,

$$(\langle v| \otimes \langle w|) (A \otimes B) (|v\rangle \otimes |w\rangle) = \langle v|A|v\rangle \langle w|B|w\rangle \geq 0$$

より,  $A \otimes B$  も正のオペレータ.

演習 2.32 ここでは, 射影オペレータ  $P$  を,

$$P^\dagger = P, P^2 = P$$

を満たすオペレータと定義する。この定義は、式 (2.35) と矛盾しない。

$P_1, P_2$  が射影オペレータのとき、

$$\begin{aligned}(P_1 \otimes P_2)^\dagger &= P_1 \otimes P_2 \\ (P_1 \otimes P_2)(P_1 \otimes P_2) &= I_1 \otimes I_2\end{aligned}$$

より、 $P_1 \otimes P_2$  は射影オペレータ。

演習 2.33 Hadamard 変換  $H$  は、

$$H = \frac{1}{\sqrt{2}} (|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|).$$

上式の最後の項の  $-$  符号に注意する。

例えば、 $n = 2$  のとき、

$$\begin{aligned}H^{\otimes 2} &= \frac{1}{2} (|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|) \otimes (|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|) \\ &= \frac{1}{2} (|00\rangle\langle 00| + |01\rangle\langle 00| + |00\rangle\langle 01| - |01\rangle\langle 01| + |10\rangle\langle 00| + |11\rangle\langle 00| + |10\rangle\langle 01| - |11\rangle\langle 01| \\ &\quad + |00\rangle\langle 10| + |01\rangle\langle 10| + |00\rangle\langle 11| - |01\rangle\langle 11| - |10\rangle\langle 10| - |11\rangle\langle 10| - |10\rangle\langle 11| + |11\rangle\langle 11|) \\ &= \frac{1}{2} \sum_{x,y} (-1)^{x \cdot y} |x\rangle\langle y|.\end{aligned}$$

ここで、 $x, y$  は各成分が 0 または 1 の 2 次元のベクトルで、 $x \cdot y$  は標準内積。

一般の  $n$  に対しても、 $x, y$  を各成分が 0 または 1 の  $n$  次元のベクトル、 $x \cdot y$  を標準内積として、

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{x \cdot y} |x\rangle\langle y|$$

を得ることは少し考えればわかる。

特に、Kronecker 積の形で書くと、

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H^{\otimes 2} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

演習 2.34 基底

$$|0\rangle, |1\rangle$$

の下での表現行列が、

$$\begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix}$$

なるオペレータ  $A$  を考える。固有値問題を解くと、基底を

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

取り替えることで、表現行列  $A$  が

$$\begin{pmatrix} 7 & 0 \\ 0 & 1 \end{pmatrix}$$



と対角化できることがわかる。つまり,

$$A = 7|+\rangle\langle+| + 1|-\rangle\langle-|.$$

ゆえに, オペレータ  $A$  の平方根  $f(A)$  を

$$\sqrt{A} = \sqrt{7}|+\rangle\langle+| + |- \rangle\langle-|$$

で定義できる. 同様に, オペレータ  $A$  の対数  $\log A$  を

$$\sqrt{A} = \log 7|+\rangle\langle+|$$

で定義できる.

演習 2.35

$$\mathbf{v} \cdot \boldsymbol{\sigma} = \begin{pmatrix} v_3 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 \end{pmatrix}$$

の固有値  $\lambda = \pm 1$  の対応する固有ベクトルをそれぞれ  $|-1\rangle, |1\rangle$  とかくと,

$$\mathbf{v} \cdot \boldsymbol{\sigma} = |1\rangle\langle 1| - |-1\rangle\langle -1|.$$

よって,

$$\begin{aligned} \exp(i\theta \mathbf{v} \cdot \boldsymbol{\sigma}) &= e^{i\theta} |1\rangle\langle 1| - e^{-i\theta} |-1\rangle\langle -1| \\ &= \cos \theta (|1\rangle\langle 1| + |-1\rangle\langle -1|) + i \sin \theta (|1\rangle\langle 1| - |-1\rangle\langle -1|) \\ &= (\cos \theta) I + i(\sin \theta) \mathbf{v} \cdot \boldsymbol{\sigma} \end{aligned}$$

演習 2.36 Pauli 行列の定義より明らか.

演習 2.37

$$\text{tr} AB = A_{ij} B_{ji} = A_{ij} B_{ji} = \text{tr} BA$$

演習 2.38 トレースの定義と  $\sum$  の線型性より明らか.

演習 2.39 (1)  $L_V \times L_V$  上で定義された内積

$$(A, B) = \text{tr}(A^\dagger B)$$

が, 式 (2.13) を満たすか調べれば良い;

$$\begin{aligned} \left( A, \sum_i \lambda_i B_i \right) &= \text{tr} \left( \sum_i \lambda_i A^\dagger B_i \right) = \sum_i \lambda_i \text{tr} (A^\dagger B_i) = \sum_i \lambda_i (A, B_i) \\ (A, B) &= \text{tr}(A^\dagger B) = \text{tr}(B^T A^*) = \text{tr}(B^\dagger A)^* = (B, A)^* \\ (A, A) &= \text{tr}(A^\dagger A) = \sum_{i,j} A_{ij}^\dagger A_{ji} = \sum_{i,j} A_{ji}^* A_{ji} = \sum_{i,j} |A_{ji}|^2 \geq 0 \\ 0 &= (A, A) \Leftrightarrow A = O. \end{aligned}$$

(2)  $V$  が  $d$  次元のとき,  $A: V \rightarrow V$  なるオペレータ  $A$  は  $d^2$  の自由度を持つので,  $L_V$  は  $d^2$  次元.

(3)  $L_V$  の正規直交基底  $\{A_i\}_{i=1}^{d^2}$  のうち, 全ての  $i$  に対して  $A_i$  が Hermite となる正規直交基底  $\{A_i\}_{i=1}^{d^2}$  を求める.  $V$  の正規直交基底を  $\{|i\rangle\}_{i=1}^d$  とすると,  $L_V$  の正規直交基底は  $\{e_{ij} = |i\rangle\langle j|\}_{i,j=1}^d$  となる;

$$(e_{ij}, e_{kl}) = \text{tr}(|j\rangle\langle i|k\rangle\langle l|) = \delta_{ij}\delta_{kl}.$$

$\{e_{ij}\}_{i,j=1}^d$  は,  $i = j$  のとき Hermite だが,  $i \neq j$  のときは Hermite ではない. そこで,  $\{e_{ii}\}_{i=1}^d$  で張られる  $L_V$  の部分空間  $L_P$  とその正規直交補空間  $L_Q$  を考える.  $L_P$  の Hermite な正規直交基底は,  $\{e_{ii}\}_{i=1}^d$  である. 一方,  $L_Q$  の Hermite な正規直交基底は,

$$e'_{ij} = \frac{e_{ij} + e_{ji}}{\sqrt{2}}, e''_{ij} = \frac{e_{ij} - e_{ji}}{\sqrt{2}i} \quad (i < j)$$

である. 以上より,  $L_V = L_P \oplus L_Q$  の Hermite な正規直交基底は,

$$\left\{ |i\rangle\langle i|, \frac{|i\rangle\langle j| + |j\rangle\langle i|}{\sqrt{2}}, \frac{|i\rangle\langle j| - |j\rangle\langle i|}{\sqrt{2}i} \right\}_{i,j=1,2,\dots,d, i < j}$$

演習 2.40 Pauli 行列の定義より明らかに,

$$[\sigma_j, \sigma_k] = 2i\epsilon_{jkl}\sigma_l.$$

演習 2.41 Pauli 行列の定義より明らかに,

$$\{\sigma_i, \sigma_j\} = 2\delta_{ij}I.$$

演習 2.42

$$[A, B] + \{A, B\} = AB - BA + AB + BA = 2AB.$$

演習 2.43

$$\sigma_j\sigma_k = \frac{[\sigma_j, \sigma_k] + \{\sigma_j, \sigma_k\}}{2} = \delta_{jk}I + i\epsilon_{jkl}\sigma_l.$$

演習 2.44

$$B = A^{-1}AB = A^{-1}\frac{[A, B] + \{A, B\}}{2} = 0.$$

演習 2.45

$$[A, B]^\dagger = (AB - BA)^\dagger = B^\dagger A^\dagger - A^\dagger B^\dagger = [B^\dagger, A^\dagger].$$

演習 2.46

$$[A, B] = -(BA - AB) = -[B, A].$$

演習 2.47

$$(i[A, B])^\dagger = -i[B^\dagger, A^\dagger] = -i[B, A] = i[A, B].$$

演習 2.48 ベクトル空間  $V$  上で定義された Hermite の行列  $H$  のスペクトル分解は,  $H$  の固有値  $\lambda \in \mathbb{R}$  として,

$$H = \sum_{\lambda} \lambda |\lambda\rangle\langle\lambda|$$

なので,

$$\begin{aligned} J &= \sqrt{H^\dagger H} = \sqrt{HH} = \sqrt{\sum_{\lambda} \sum_{\lambda'} \lambda' \lambda |\lambda\rangle\langle\lambda| \langle\lambda|\lambda'\rangle \langle\lambda'|} = \sqrt{\sum_{\lambda} \lambda^2 |\lambda\rangle\langle\lambda|} = \sum_{\lambda} |\lambda| |\lambda\rangle\langle\lambda| \\ K &= \sqrt{HH^\dagger} = \sqrt{HH} = J \end{aligned}$$

ここで,  $\{|\lambda\rangle\}$  は  $V$  の正規直交基底になっている. したがって, Hermite 行列  $H$  の極分解は,

$$H = U\sqrt{H^2} = \sqrt{H^2}U.$$

特に,  $\lambda \geq 0$  なら  $H$  は正の行列  $P$  となり,

$$J = K = P$$

が成立するので,  $P$  の極分解は,

$$P = IP = PI.$$

ユニタリ行列  $U$  の極分解は,

$$U = IU = UI.$$

**演習 2.49** ベクトル空間  $V$  上で定義された正規行列  $A$  のスペクトル分解は,  $A$  の固有値  $a$ , 対応する固有ベクトル  $|a\rangle$  として,

$$A = \sum_a a |a\rangle \langle a|.$$

ここで,  $\{|a\rangle\}$  は  $V$  の正規直交基底になっている. すると,

$$J = \sqrt{A^\dagger A} = \sqrt{\sum_a \sum_{a'} a' a^* |a\rangle \langle a| a' \langle a'|} = \sqrt{\sum_a |a|^2 |a\rangle \langle a|} = \sum_a \sqrt{|a|} |a\rangle \langle a|.$$

定理 2.3 の証明より,

$$U = \sum_a |e_a\rangle \langle a|$$

とすれば,  $A$  の左極分解は,

$$A = UJ.$$

右極分解についても同様.

**演習 2.50**

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

として,  $A^\dagger A$

$$A^\dagger A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

の固有値は

$$\lambda_{\pm} = \frac{3 \pm \sqrt{5}}{2}$$

で, 対応する固有ベクトル  $|\lambda_{\pm}\rangle$  は,

$$|\lambda_{\pm}\rangle = \frac{1}{10 \pm 2\sqrt{5}} \begin{pmatrix} 1 \pm \sqrt{5} \\ 2 \end{pmatrix}.$$

よって,  $J = \sqrt{A^\dagger A}$  は,

$$J = A^\dagger A = \sqrt{\lambda_+} |\lambda_+\rangle \langle \lambda_+| + \sqrt{\lambda_-} |\lambda_-\rangle \langle \lambda_-|$$

あとで計算する

演習 2.51

$$HH^\dagger = I.$$

演習 2.52

$$HH = I.$$

演習 2.53

$$|\lambda = \pm 1\rangle = \left( \pm\sqrt{2} - 1 \right)$$

演習 2.54  $A, B$  は可換な Hermite なので, 同じ正規直交基底  $\{|i\rangle\}$  で同時対角化可能で,

$$A = \sum_i a_i |i\rangle \langle i|, B = \sum_i b_i |i\rangle \langle i|$$

とかけるので,

$$\exp(A) \exp(B) = \sum_i \sum_j e^{a_i} |i\rangle \langle i| e^{b_j} |j\rangle \langle j| = \sum_i e^{a_i + b_i} |i\rangle \langle i| = \exp(A + B).$$

演習 2.55  $H$  は Hermite なので,  $H, H^\dagger$  が可換だから, 演習 2.54 より,

$$U(t_1, t_2)U^\dagger(t_1, t_2) = \exp[-iH(t_1 - t_2)] \exp[iH^\dagger(t_1 - t_2)] = \exp[i(H^\dagger - H)(t_1 - t_2)] = I.$$

演習 2.56 ユニタリオペレータ  $U$  は正規なので,  $\lambda_i = e^{i\theta_i}$  ( $\theta_i \in R$ ) として,

$$U = \sum_i \lambda_i |\lambda_i\rangle \langle \lambda_i|$$

とスペクトル分解できる. よって,

$$K = -i \log U = \sum_i \theta_i |i\rangle \langle i|$$

となり, これは明らかに Hermite. したがって,

$$\exp(iK) = \sum_i e^{i\theta_i} |i\rangle \langle i| = U.$$

演習 2.57 状態  $|\psi\rangle$  に対して,  $L_l$  を測定した後の状態  $|\phi\rangle$  は,

$$|\phi\rangle = \frac{L_l |\psi\rangle}{\langle \psi | L_l^\dagger L_l | \psi \rangle}.$$

さらに, この状態に対して,  $M_m$  を測定した後の状態は,

$$\frac{M_m |\phi\rangle}{\langle \phi | M_m^\dagger M_m | \phi \rangle} = \frac{M_m L_l |\psi\rangle}{\langle \psi | L_l^\dagger M_m^\dagger M_m L_l | \psi \rangle} = \frac{N_{lm} |\psi\rangle}{\langle \psi | L_l^\dagger M_m^\dagger N_{lm} | \psi \rangle}.$$

演習 2.58 平均測定値  $E(M)$  は,

$$E(M) = \langle \psi | M | \psi \rangle = m \langle \psi | \psi \rangle = m.$$

標準偏差  $\Delta(M)$  は,

$$\Delta(M) = \sqrt{\langle \psi | M^2 | \psi \rangle - \langle \psi | M | \psi \rangle^2} = \sqrt{m^2 - m^2} = 0.$$

## 演習 2.59

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|$$

なので, 平均値は,

$$\langle 0|X|0\rangle = 0.$$

標準偏差  $\Delta(X)$  は,

$$\Delta(X) = \sqrt{\langle 0|X^2|0\rangle - \langle 0|X|0\rangle^2} = \sqrt{1 - 0} = 1.$$

演習 2.60 まず,  $v_3 \neq 1$  のときを考える.

$$\mathbf{v} \cdot \boldsymbol{\sigma} = \begin{pmatrix} v_3 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 \end{pmatrix}$$

より, 固有値は,  $\mathbf{v}$  が単位ベクトルなことに注意して,

$$0 = \lambda^2 - |\mathbf{v}|^2 = \lambda^2 - 1 \rightarrow \lambda = \pm 1.$$

対応する固有ベクトルは,

$$|\lambda = \pm 1\rangle = \frac{1}{\sqrt{2(1 \mp v_3)}} \begin{pmatrix} -v_1 + iv_2 \\ v_3 \mp 1 \end{pmatrix}$$

よって, 射影オペレータは,

$$\begin{aligned} P_{\pm} &= |\lambda = \pm 1\rangle\langle \lambda = \pm 1| \\ &= \frac{1}{2(1 \mp v_3)} \begin{pmatrix} -v_1 + iv_2 \\ v_3 \mp 1 \end{pmatrix} \begin{pmatrix} v_1 - iv_2 & v_3 \mp 1 \end{pmatrix} \\ &= \frac{1}{2(1 \mp v_3)} \begin{pmatrix} v_1^2 + v_2^2 & (-v_1 + iv_2)(v_3 \mp 1) \\ (-v_1 + iv_2)(v_3 \mp 1) & (v_3 \mp 1)^2 \end{pmatrix} \\ &= \frac{1}{2(1 \mp v_3)} \begin{pmatrix} 1 - v_3^2 & (-v_1 + iv_2)(v_3 \mp 1) \\ (-v_1 + iv_2)(v_3 \mp 1) & (v_3 \mp 1)^2 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 1 \pm v_3 & \pm(v_1 - iv_2) \\ \pm(v_1 - iv_2) & 1 \mp v_3 \end{pmatrix} \\ &= \frac{I \pm \mathbf{v} \cdot \boldsymbol{\sigma}}{2}. \end{aligned}$$

一方,  $v_3 = 1$  のとき,  $v_1 = v_2 = 0$  となり,

$$\mathbf{v} \cdot \boldsymbol{\sigma} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z.$$

固有ベクトルは,

$$|\lambda = 1\rangle = |0\rangle, |\lambda = -1\rangle = |1\rangle.$$

よって, 射影オペレータは,

$$P_+ = |0\rangle\langle 0|, P_- = |1\rangle\langle 1| \rightarrow P_{\pm} = \frac{I \pm \mathbf{v} \cdot \boldsymbol{\sigma}}{2}.$$

演習 2.61  $v_3 \neq 1$  のとき,  $|0\rangle$  の状態を測定して  $+1$  を得る確率は,

$$|\langle \lambda = +1 | \mathbf{v} \cdot \boldsymbol{\sigma} | 0 \rangle|^2 = |\langle \lambda = +1 | 0 \rangle|^2 = \left| \frac{-v_1 + iv_2}{\sqrt{2(1-v_3)}} \right|^2 = \frac{1+v_3}{2}.$$

これは,  $v_3 = 1$  でも成立する.  $+1$  を測定した直後の状態は,

$$\frac{P_+ |0\rangle}{\sqrt{\langle 0 | P_+^\dagger P_+ | 0 \rangle}} = \frac{|\lambda = +1\rangle \langle \lambda = +1 | 0 \rangle}{\sqrt{\langle \lambda = +1 | 0 \rangle \langle 0 | \lambda = +1 \rangle}} = e^{i\theta} |\lambda = +1\rangle.$$

ここで,  $\theta$  は  $\langle \lambda = +1 | 0 \rangle$  の偏角.

演習 2.62 測定オペレータが POVM と一致するとすると,

$$M_m = M_m^\dagger M_m.$$

$M_m^\dagger M_m$  は正のオペレータなので,  $M_m$  も正のオペレータ. よって, 演習 2.24 より  $M_m$  も Hermite. したがって,

$$M_m = M_m^\dagger M_m = M_m^2$$

となり,  $M_m$  は射影オペレータ.

また, 完全性条件

$$\sum_m M_m^\dagger M_m = \sum_m M_m = I$$

から,

$$\begin{aligned} M_m &= \sum_{m'} M_{m'} M_m = M_m^2 + \sum_{m' \neq m} M_{m'} M_m = M_m + \sum_{m' \neq m} M_{m'} M_m \\ &\rightarrow \sum_{m' \neq m} M_{m'} M_m = O \end{aligned}$$

となり,  $M_{m'} M_m (m' \neq m)$  は正のオペレータゆえ,

$$M_{m'} M_m = O \quad (m' \neq m).$$

先に示した  $M_m^2 = M_m$  と合わせて,

$$M_{m'} M_m = \delta_{mm'} M_m.$$

こうして, 測定オペレータが POVM と一致するとすると,  $M_m$  が直交射影オペレータになることが言えた.

演習 2.63 定理 2.3 より, 明らか.

演習 2.64

$$\langle \psi_i | \phi_j \rangle \propto \delta_{ij}$$

を満たすような  $|\psi_i\rangle (\forall i \neq j)$  と直交する  $|\phi_j\rangle (\neq 0)$  を作りたい.  $\{|\psi_i\rangle\}$  で張られる  $m$  次元ベクトル空間  $V$  の部分空間  $W_j$  は  $\{|\psi_i\rangle\}_{i \neq j}$  で張られるとして, その直交補空間  $W_j^\perp$  とする.  $W_j^\perp$  への射影オペレータ  $P_j^\perp$  としてやれば, 作りたかった  $|\phi_j\rangle$  を

$$|\phi_j\rangle = P_j^\perp |\psi_j\rangle$$

で作れる.  $\{|\psi_i\rangle\}$  の線型独立性から,  $|\phi_j\rangle \neq 0$  が保証される.

こうして作った  $\{|\phi_j\rangle\}$  を使って,

$$E_j = \begin{cases} c |\phi_i\rangle \langle \phi_i| & (j = 1, 2, \dots, m) \\ I - \sum_{k=1}^{k=m} E_k & (j = m+1) \end{cases}$$

なる  $\{E_i\}$  を作る. ここで,  $c$  は任意の状態  $|\psi\rangle$  に対して,

$$c < \frac{1}{\sum_{k=1}^{k=m} \langle \psi | E_k | \psi \rangle}$$

を満たす定数. このように定義された  $\{E_i\}$  が求めたかった POVM (正かつ  $\sum_{k=1}^{m+1} E_k = I$  を満たす) である.

演習 2.65 基底を

$$\left\{ \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\}$$

ととれば良い.

演習 2.66

$$\frac{\langle 0| \otimes \langle 0| + \langle 1| \otimes \langle 1|}{\sqrt{2}} X_1 \otimes Z_2 \frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle}{\sqrt{2}} = \frac{\langle 0| \otimes \langle 0| + \langle 1| \otimes \langle 1|}{\sqrt{2}} \frac{|1\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle}{\sqrt{2}} = 0.$$

演習 2.67  $W$  の直交補空間  $W^\perp$  とかき, それぞれの正規直交基底を  $\{|w_i\rangle\}, \{|w_j^\perp\rangle\}$  とし,

$$U' = \sum_i U |w_i\rangle \langle w_i| + \sum_j |w_j^\perp\rangle \langle w_j^\perp|$$

とすればよい.

演習 2.68 あらゆる単一 q ビット  $|a\rangle, |b\rangle$  は,

$$\begin{aligned} |a\rangle &= a_0 |0\rangle + a_1 |1\rangle \\ |b\rangle &= b_0 |0\rangle + b_1 |1\rangle \end{aligned}$$

でかける.

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

に対して,

$$|\psi\rangle = |a\rangle |b\rangle$$

とかけると仮定すると,

$$a_0 b_1 = a_1 b_0 = 0, a_0 b_0 \neq 0, a_1 b_1 \neq 0$$

となるが, これを満たす  $a_0, a_1, b_0, b_1$  は存在せず矛盾.

演習 2.69 Bell 基底は,

$$|\beta_{xy}\rangle = \frac{|0, y\rangle + (-1)^x |1, \bar{y}\rangle}{\sqrt{2}}$$

でかけ,

$$\langle \beta_{x'y'} | \beta_{xy} \rangle = \frac{\delta_{yy'} + (-1)^{x+x'} \delta_{\bar{y}\bar{y}'}}{2} = \delta_{xx'} \delta_{yy'}.$$

となるので, 正規直交基底.

## 演習 2.70 Bell 状態

$$|\beta_{xy}\rangle = \frac{|0, y\rangle + (-1)^x |1, \bar{y}\rangle}{\sqrt{2}}$$

に対して,  $\langle\beta_{xy}|E \otimes I|\beta_{xy}\rangle$  は,

$$\langle\beta_{xy}|E \otimes I|\beta_{xy}\rangle = \frac{\langle 0|E|0\rangle + \langle 1|E|1\rangle}{2}$$

と  $x, y$  に依らない. 上に示したことから, Alice が Bob に送った  $q$  ビットを, Eve が観測しても得られる状態の期待値は Bell 状態に依らないので, Eve は Alice の送りたい情報を推論できない.

演習 2.71 密度オペレータ  $\rho$  は, 正のオペレータなので, スペクトル定理から,  $\rho$  の固有空間の正規直交基底  $\{|\psi_i\rangle\}$  を用いて,

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|.$$

とかけるので,

$$\begin{aligned} \text{tr}(\rho^2) &= \text{tr} \left( \sum_{i,j} p_i p_j |\psi_i\rangle \langle\psi_i| \psi_j\rangle \langle\psi_j| \right) \\ &= \sum_{i,j} p_i p_j \text{tr}(|\psi_i\rangle \langle\psi_i| \psi_j\rangle \langle\psi_j|) \\ &= \sum_{i,j} p_i p_j \delta_{ij} \text{tr}(|\psi_i\rangle \langle\psi_j|) \\ &= \sum_i p_i^2 \text{tr}(|\psi_i\rangle \langle\psi_i|) \\ &= \sum_i p_i^2 \leq \left( \sum_i p_i \right)^2 = 1. \end{aligned}$$

等号は,

$$p_i = \begin{cases} 1 & (i = i_0) \\ 0 & (\text{otherwise}) \end{cases}$$

つまり,  $\rho$  が純粋状態の時にのみ成り立つ.

## 演習 2.72 (1)

$$\begin{aligned} \rho^2 &= \frac{I + \mathbf{r} \cdot \boldsymbol{\sigma}}{2} \frac{I + \mathbf{r} \cdot \boldsymbol{\sigma}}{2} \\ &= \frac{1}{4} (I + 2r_i \sigma_i + r_i r_j \sigma^i \sigma^j) \\ &= \frac{1}{4} \left( I + 2r_i \sigma_i + r_i r_j \frac{\{\sigma^i, \sigma^j\}}{2} \right) \\ &= \frac{1}{4} ((1 + \mathbf{r}^2)I + 2\mathbf{r} \cdot \boldsymbol{\sigma}) \\ &= \frac{\mathbf{r}^2 - 1}{4} I + \rho \end{aligned}$$

で  $\rho$  は,

$$\rho = \rho^\dagger$$



を満たすので, 任意の状態  $|\psi\rangle$  に対して,  $\mathbf{r}^2 \leq 1$  なら,

$$\langle\psi|\rho|\psi\rangle = \langle\psi|\rho^2 + \frac{1-\mathbf{r}^2}{4}|\psi\rangle = \langle\psi|\rho^\dagger\rho|\psi\rangle + \langle\psi|\frac{1-\mathbf{r}^2}{4}|\psi\rangle \geq 0.$$

また,  $\text{tr}(\sigma_i) = 0$  なので,

$$\text{tr}(\rho) = 1.$$

以上より,  $\rho$  は, 正かつトレースが1なので, 定理 2.5 より  $\rho$  は密度オペレータ.

(2)  $\mathbf{r} = \mathbf{0}$ .

(3)

$$\rho \text{ が純粋状態} \Leftrightarrow \text{tr}(\rho^2) = 1 \Leftrightarrow \text{tr}\left(\frac{1-\mathbf{r}^2}{4} + \rho\right) \Leftrightarrow |\mathbf{r}| = 1.$$

(4)  $\mathbf{r} = (\sin\theta \cos\phi, \sin\theta \sin\phi, \cos\theta)$  として,

$$\rho = \frac{I + \mathbf{r} \cdot \boldsymbol{\sigma}}{2} = \frac{1}{2} \begin{pmatrix} 1 + \cos\theta & \sin\theta e^{-i\phi} \\ \sin\theta e^{i\phi} & 1 - \cos\theta \end{pmatrix} = |\psi\rangle \langle\psi|.$$

ただし, ここで

$$|\psi\rangle = \cos\frac{\theta}{2} |0\rangle + e^{i\phi} \sin\frac{\theta}{2} |1\rangle.$$

演習 2.73

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|$$

の左から  $\rho^{-1}$  をかけて,

$$1 = \sum_i p_i \rho^{-1} |\psi_i\rangle \langle\psi_i|.$$

左から  $\langle\psi_j|$ , 右から  $|\psi_j\rangle$  をかけて,

$$1 = p_j \langle\psi_j|\rho^{-1}|\psi_j\rangle \rightarrow p_j = \frac{1}{\langle\psi_j|\rho^{-1}|\psi_j\rangle}.$$

演習 2.74 複合システムの密度オペレータ  $\rho_{AB}$  は,

$$\rho_{AB} = |a\rangle \langle a| + |b\rangle \langle b|.$$

よって, システム  $A$  で縮約した密度オペレータは,

$$\rho^A = |a\rangle \langle a| \text{tr}(|b\rangle \langle b|) = |a\rangle \langle a|$$

なので,

$$\text{tr}(\rho^{A^2}) = 1$$

と  $\rho^A$  が純粋状態であることがわかる.

## 演習 2.75 各 Bell 状態

$$|\beta_{xy}\rangle = \frac{|0, y\rangle + (-1)^x |1, \bar{y}\rangle}{\sqrt{2}}$$

に対して, 密度オペレータは,

$$\begin{aligned} \rho &= \frac{|0, y\rangle + (-1)^x |1, \bar{y}\rangle}{\sqrt{2}} \frac{\langle 0, y| + (-1)^x \langle 1, \bar{y}|}{\sqrt{2}} \\ &= \frac{|0, y\rangle \langle 0, y| + (-1)^x |1, \bar{y}\rangle \langle 0, y| + (-1)^x |0, y\rangle \langle 1, \bar{y}| + |1, \bar{y}\rangle \langle 1, \bar{y}|}{2}. \end{aligned}$$

よって, 各 q ビットを縮約した密度オペレータは,

$$\begin{aligned} \rho^1 &= \frac{|y\rangle \langle y| + |\bar{y}\rangle \langle \bar{y}|}{2} = \frac{I}{2} \\ \rho^2 &= \frac{|0\rangle \langle 0| + |1\rangle \langle 1|}{2} = \frac{I}{2}. \end{aligned}$$

演習 2.76  $m \times n$  の行列  $C$  に対して,  $m \times m$  のユニタリ行列  $U$ ,  $n \times n$  のユニタリ行列  $V$ ,  $m \times n$  の行列  $D$ ;  $D =$

$$\begin{pmatrix} \lambda_1 & & & & \\ & \lambda_2 & & & \\ & & \ddots & & \\ & & & \lambda_{\text{rank } A} & \\ & & & & O_{m-\text{rank } A, n-\text{rank } A} \end{pmatrix}$$

を用いて,

$$C = UDV$$

とかける (特異値分解). ここで,  $\lambda_i$  は  $C$  の特異値で非負である.

$A \otimes B$  の任意の純粋状態  $|\psi\rangle$  に対して,  $A, B$  の正規直交基底  $|j\rangle, |k\rangle$  を用いて,

$$|\psi\rangle = \sum_{jk} C_{jk} |j\rangle |k\rangle.$$

$C$  の特異値分解を考えると, ユニタリ行列  $U, V$  が存在し,

$$|\psi\rangle = \sum_{ijk} U_{ji} D_{ii} V_{ik} |j\rangle |k\rangle.$$

ここで,

$$|i_A\rangle = \sum_j U_{ji} |j\rangle, |i_B\rangle = \sum_k V_{ik} |k\rangle$$

とすれば,  $|i_A\rangle, |i_B\rangle$  は  $A, B$  の正規直交基底なので,  $|i_A\rangle |i_B\rangle$  は  $A \otimes B$  の正規直交基底で,

$$|\psi\rangle = \sum_i D_{ii} |i_A\rangle |i_B\rangle.$$

ただし,  $\text{tr}(|\psi\rangle \langle \psi|) = 1$  より,

$$\sum_i D_i^2 = 1$$

を満たす.

演習 2.77 例えば,  $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$  の状態  $|\psi\rangle$ ;

$$|\psi\rangle = |0\rangle(|00\rangle + |11\rangle)$$

は,

$$\begin{aligned} |\psi\rangle &= \lambda_0 |0_A 0_B 0_C\rangle + \lambda_1 |1_A 1_B 1_C\rangle \\ \langle i_A | j_A \rangle &= \langle i_B | j_B \rangle = \langle i_C | j_C \rangle = \delta_{ij} \end{aligned}$$

の形でかけない. なぜなら,  $|\psi\rangle$  でかっこでくり出された  $|0\rangle$  のせいである.

演習 2.78  $|\psi\rangle$  の Schmidt 数が 1 なら,  $A, B$  の正規直交基底  $|i_A\rangle, |i_B\rangle$  として,  $|\psi\rangle$  は  $|\psi\rangle \propto |i_A\rangle |i_B\rangle$  と積状態. 逆に,  $|\psi\rangle = |a\rangle |b\rangle$  なら,  $|a\rangle, |b\rangle$  のそれぞれが  $A, B$  の正規直交基底になるような基底の変換  $U_A, U_B$  が存在する (Schmidt の直交化法).

$\rho^A, \rho^B$  が純粋状態とすると,  $\rho^{AB} = |a\rangle |b\rangle \langle a| \langle b|$ . これは,  $|\psi\rangle = |a\rangle |b\rangle$  が積状態であることを意味している. 逆に,  $|\psi\rangle$  が積状態であるとする,  $|\psi\rangle$  とかけ,  $\rho^A = |a\rangle \langle a|, \rho^B = |b\rangle \langle b|$  と  $\rho^A, \rho^B$  が純粋状態であることを意味している.

演習 2.79 (1)

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

はそれ自身で Schmidt 分解.

(2)

$$\frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle + |1\rangle}{\sqrt{2}} + 0 \frac{|0\rangle - |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

(3)

$$\frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

の特異値分解を演習 2.50 を参考にしてやって, 定理 2.7 の証明に従って頑張る.

演習 2.80

$$\begin{aligned} |\psi\rangle &= \sum_i \lambda_i |i_A\rangle |i_B\rangle \\ |\phi\rangle &= \sum_i \lambda_i |\tilde{i}_A\rangle |\tilde{i}_B\rangle \end{aligned}$$

に対して,

$$\begin{aligned} U &= \sum_j |j_A\rangle \langle \tilde{j}_A| \\ V &= \sum_j |j_B\rangle \langle \tilde{j}_B| \end{aligned}$$

とすれば,  $U, V$  はユニタリで,

$$|\psi\rangle = (U \otimes V) |\phi\rangle$$

を満たす.

## 演習 2.81

$$\rho^A = \sum_i p_i |i^A\rangle \langle i^A|$$

の純粋化

$$\begin{aligned} |AR_1\rangle &= \sum_i \sqrt{p_i} |i^A\rangle |i^{R1}\rangle \\ |AR_2\rangle &= \sum_i \sqrt{p_i} |i^A\rangle |i^{R2}\rangle \end{aligned}$$

に対して,

$$U_R = \sum_i |i^{R1}\rangle \langle i^{R2}|$$

とすれば,  $U_R$  はユニタリで,

$$|AR_1\rangle = (I_A \otimes U_R) |AR_2\rangle$$

を満たす.

## 演習 2.82

$$\rho^A = \sum_i p_i |\psi_i\rangle \langle \psi_i|$$

とする.

(1) (2.211) 式と同様.

(2)  $R$  を測定して, 結果  $i$  を得る確率は,

$$R_i = I \otimes |i\rangle \langle i|$$

として,

$$\text{tr}(R_i^\dagger R_i \rho^{AR}) = \text{tr}(R_i \rho^{AR}).$$

結果  $i$  を得た後の状態は,

$$\frac{R_i \rho^{AR} R_i}{\text{tr}(R_i \rho^{AR})}.$$

(3) システム  $AR$  に対する  $\rho^A$  の任意の純粋化  $|AR\rangle$  とは, システム  $R$  上の正規直交基底を任意にとって行った純粋化の意味. システム  $A$  の正規直交基底は, システム  $AR$  に対する  $\rho^A$  の任意の純粋化  $|AR\rangle$  は,  $R$  上のユニタリオペレータ  $U_R$  として,

$$|AR\rangle = \sum_i \sqrt{p_i} |\psi_i\rangle \otimes U_R |i\rangle.$$

純粋状態  $|AR\rangle \langle AR|$  に対して,  $R$  を測定して  $i$  を得る確率は,

$$R_i = I \otimes U_R |i\rangle \langle i| U_R^\dagger$$

として,

$$\text{tr} \left[ R_i^\dagger R_i (|AR\rangle \langle AR|) \right] = \sum_{j,k} \sqrt{p_j} \sqrt{p_k} \text{tr} \left[ (I \otimes U_R |i\rangle \langle i| U_R^\dagger) (|\psi_j\rangle \otimes U_R |j\rangle) (\langle \psi_k| \otimes \langle k| U_R^\dagger) \right]$$

$$\begin{aligned}
&= \sum_k \sqrt{p_i} \sqrt{p_k} \operatorname{tr} \left[ (|\psi_i\rangle \otimes U_R |i\rangle) (\langle\psi_k| \otimes \langle k| U_R^\dagger) \right] \\
&= \sum_k \sqrt{p_i} \sqrt{p_k} \langle\psi_k|\psi_i\rangle \langle i|k\rangle \\
&= p_i.
\end{aligned}$$

$i$  を得た後の状態は,

$$\frac{R_i \rho^{AR} R_i}{p_i} = (|\psi_i\rangle \otimes |i\rangle) (\langle\psi_i| \otimes \langle i|).$$

以上より, 任意の  $\rho^A$  の任意の純粋化に対して,  $R$  を測定すると確率  $p_i$  で, システム  $A$  の測定後の状態が  $|\psi_i\rangle$  となる  $R$  の正規直交基底  $\{U_R |i\rangle\}$  が存在することが言えた.

問題 2.1 演習 2.35 で見たように, 単位ベクトル  $\mathbf{n}$  に対して,

$$(\mathbf{n} \cdot \boldsymbol{\sigma})^n = \begin{cases} \mathbf{n} \cdot \boldsymbol{\sigma} & (n : \text{even}) \\ I & (n : \text{odd}) \end{cases}.$$

よって, Taylor の定理より,

$$\begin{aligned}
f(\theta \mathbf{n} \cdot \boldsymbol{\sigma}) &= I \sum_{n:\text{even}} \frac{f^{(n)}(0)}{n!} \theta^n + \mathbf{n} \cdot \boldsymbol{\sigma} \sum_{n:\text{odd}} \frac{f^{(n)}(0)}{n!} \theta^n \\
&= I \sum_{n:\text{even}} \frac{f^{(n)}(0)}{n!} \frac{\theta^n + (-\theta)^n}{2} + \mathbf{n} \cdot \boldsymbol{\sigma} \sum_{n:\text{odd}} \frac{f^{(n)}(0)}{n!} \frac{\theta^n - (-\theta)^n}{2} \\
&= I \sum_n \frac{f^{(n)}(0)}{n!} \frac{\theta^n + (-\theta)^n}{2} + \mathbf{n} \cdot \boldsymbol{\sigma} \sum_n \frac{f^{(n)}(0)}{n!} \frac{\theta^n - (-\theta)^n}{2} \\
&= \frac{f(\theta) + f(-\theta)}{2} I + \frac{f(\theta) - f(-\theta)}{2} \mathbf{n} \cdot \boldsymbol{\sigma}.
\end{aligned}$$

問題 2.2 (1)  $A, B$  のある正規直交基底  $\{|i^A\rangle\}, \{|i^B\rangle\}$  を用いて,  $A \otimes B$  の純粋状態  $|\psi\rangle$  は,  $\lambda_i > 0$  として,

$$|\psi\rangle = \sum_{i=1}^{\operatorname{Sch}(\psi)} \lambda_i |i^A\rangle |i^B\rangle$$

と Schmidt 分解可能. すると,

$$\rho^A = \operatorname{tr}_B(|\psi\rangle \langle\psi|) = \sum_{i=1}^{\operatorname{Sch}(\psi)} \lambda_i^2 |i^A\rangle \langle i^A|$$

となり, これは  $\rho^A$  のスペクトル分解にもなっていて,  $\rho^A$  の台の次元の数 ( $\operatorname{rank} \rho^A$ ) が  $\operatorname{Sch}(\psi)$  に等しいことを意味している.

(2)

$$|\psi\rangle = \sum_{i=1}^n |\alpha_i\rangle |\beta_i\rangle$$

とかけているとき  $\{|\alpha_i\rangle\}$  は互いに一次独立になっているとする. すると,  $\{|\alpha_i\rangle\}$  で張られる次元  $n$  のベクトル空間  $V$  が定義できる. ここで, (1) の結果を用いると,

$$\operatorname{Sch}(\psi) = \operatorname{rank}(\operatorname{tr}_B(|\psi\rangle \langle\psi|)) = \operatorname{rank} \left( \sum_{j,k=1}^n |\alpha_j\rangle \langle\beta_k| \beta_j\rangle \langle\alpha_k| \right) \leq n.$$

最後の不等式では,  $\left(\sum_{j,k=1}^n |\alpha_j\rangle \langle \beta_k| \beta_j\rangle \langle \alpha_k|\right)$  が,  $V$  上で定義されたある線形オペレータの行列表示 (サイズは  $n \times n$ ) になっていることを用いた.

(3)

$$\text{Sch}(\phi) \geq \text{Sch}(\gamma)$$

としても一般性を失わない.  $|\phi\rangle, |\gamma\rangle$  の Schmidt 分解は,

$$\begin{aligned} |\phi\rangle &= \sum_{i=1}^{\text{Sch}(\phi)} \lambda_i |i^A\rangle |i^B\rangle \\ |\gamma\rangle &= \sum_{i=1}^{\text{Sch}(\gamma)} \xi_i |\tilde{i}^A\rangle |\tilde{i}^B\rangle. \end{aligned}$$

$\alpha, \beta$  の一方が 0 の時は, 明らかに示すべき式が成立するので,  $\alpha \neq 0, \beta \neq 0$  として,

$$|\psi\rangle = \alpha |\phi\rangle + \beta |\gamma\rangle$$

のとき, (1) より,

$$\begin{aligned} \text{Sch}(\psi) &= \text{rank}(\text{tr}_B(|\psi\rangle \langle \psi|)) \\ &= \text{rank} \left( \alpha \sum_{i=1}^{\text{Sch}(\phi)} \lambda_i^2 |i^A\rangle \langle i^A| + \beta \sum_{i=1}^{\text{Sch}(\gamma)} \xi_i^2 |\tilde{i}^A\rangle \langle \tilde{i}^A| \right) \end{aligned}$$

この右辺の最小値は,

$$\alpha \sum_{i=1}^{\text{Sch}(\phi)} \lambda_i^2 |i^A\rangle \langle i^A| + \beta \sum_{i=1}^{\text{Sch}(\gamma)} \xi_i^2 |\tilde{i}^A\rangle \langle \tilde{i}^A| = \sum_{i=1}^{\text{Sch}(\phi)-\text{Sch}(\gamma)} \alpha \lambda_i^2 |i^A\rangle \langle i^A| + \sum_{i=1}^{\text{Sch}(\gamma)} (\alpha \lambda_i^2 + \beta \xi_i^2) |\tilde{i}^A\rangle \langle \tilde{i}^A|$$

で,

$$\alpha \lambda_i^2 + \beta \xi_i^2 = 0 \quad (i = 1, 2, \dots, \text{Sch}(\gamma))$$

のときに実現される. つまり,

$$\min \text{rank} \left( \alpha \sum_{i=1}^{\text{Sch}(\phi)} \lambda_i^2 |i^A\rangle \langle i^A| + \beta \sum_{i=1}^{\text{Sch}(\gamma)} \xi_i^2 |\tilde{i}^A\rangle \langle \tilde{i}^A| \right) = \sum_{i=1}^{\text{Sch}(\phi)-\text{Sch}(\gamma)} \alpha \lambda_i^2 |i^A\rangle \langle i^A| = \text{Sch}(\phi) - \text{Sch}(\gamma).$$

よって,

$$\text{Sch}(\psi) = \text{rank} \left( \alpha \sum_{i=1}^{\text{Sch}(\phi)} \lambda_i^2 |i^A\rangle \langle i^A| + \beta \sum_{i=1}^{\text{Sch}(\gamma)} \xi_i^2 |\tilde{i}^A\rangle \langle \tilde{i}^A| \right) \geq \text{Sch}(\phi) - \text{Sch}(\gamma).$$

問題 2.3 演習 2.35 で見たように,

$$Q^2 = R^2 = S^2 = T^2 = I.$$

このことと,  $Q, R, S, T$  が互いに非可換なことに注意して,

$$(Q \otimes S + R \otimes S + R \otimes T - Q \otimes T)^2 = 4I + [Q, R] \otimes [S, T].$$

$Q, R, S, T$  が Hermite なので, 式 (2,107) より,

$$|\langle [Q, R] \rangle| \leq 2 |\langle Q^2 \rangle| |\langle R^2 \rangle| = 2$$

$$|\langle [S, T] \rangle| \leq 2 |\langle S^2 \rangle| |\langle T^2 \rangle| = 2$$

が成り立つことと, 先に示した等式を合わせて,

$$\begin{aligned} \langle Q \otimes S + R \otimes S + R \otimes T - Q \otimes T \rangle^2 &\leq \left\langle (Q \otimes S + R \otimes S + R \otimes T - Q \otimes T)^2 \right\rangle \\ &= \langle 4I + [Q, R] \otimes [S, T] \rangle \leq 8. \end{aligned}$$

よって,

$$\langle Q \otimes S + R \otimes S + R \otimes T - Q \otimes T \rangle \leq 2\sqrt{2}.$$

## 第 3 章

# コンピュータ科学入門

演習 3.1 人間が新たな物理法則を見出すことで.

演習 3.2

演習 3.3  $\langle q_i, x_1, y_1, q_j, x_2, y_2, s_x, s_y \rangle$  というプログラムは, 内部状態  $q_i$  にある TM が読み出しテープの  $x_1$ , 書き込みテープの  $y_1$  を読み出したとき, 内部状態を  $q_j$  にして, 読み出しテープを  $x_2$ , 書き込みテープを  $y_2$  に書き換え, 読み出しテープのヘッドを  $s_1$ , 書き込みテープのヘッドを  $s_2$  だけ進めることを意味する. 入力ビット  $x$  の読み出し用テープと  $x$  を逆順にしたビット列  $y$  の出力用テープを考える. 考え方は, 以下の通り.

1. 入力テープの右端に行くまで, 入力ヘッドを右に移動させる.
2. 入力テープの値を, 出力テープに書き出す. その後, 入力テープは左に, 出力テープは右に動かしていく.
3. 入力ヘッドが左端に着いたら終了.

その実装は, 以下のようになる.

$$\begin{aligned} &\langle q_s, \triangleright, \triangleright, q_1, \triangleright, \triangleright, +1, 0 \rangle \\ &\langle q_1, 0, b, q_1, 0, b, +1, 0 \rangle \\ &\langle q_1, 1, b, q_1, 1, b, +1, 0 \rangle \\ &\langle q_1, b, b, q_2, b, b, -1, 0 \rangle \\ &\langle q_2, 0, b, q_2, b, 0, -1, +1 \rangle \\ &\langle q_2, 1, b, q_2, b, 1, -1, +1 \rangle \\ &\langle q_2, \triangleright, b, q_h, \triangleright, b, 0, 0 \rangle \end{aligned}$$

演習 3.4  $\langle q_i, x_1, y_1, q_j, x_2, y_2, s_x, s_y \rangle$  というプログラムは, 内部状態  $q_i$  にある TM が読み出しテープの  $x_1$ , 書き込みテープの  $y_1$  を読み出したとき, 内部状態を  $q_j$  にして, 読み出しテープを  $x_2$ , 書き込みテープを  $y_2$  に書き換え, 読み出しテープのヘッドを  $s_1$ , 書き込みテープのヘッドを  $s_2$  だけ進めることを意味する. 入力ビット  $x$  と  $y$  の読み出し用テープと  $x + y$  の計算結果の出力用テープを考える. このとき,  $x, y$  の桁数が同じになるように 0 が補われているとする. 考え方は以下の通り.

1. 入力テープの空白にたどり着くまで, 入力ヘッドを右に移動させる. そのとき, 入力テープと同じ値を出力テープに書き出しておく. すると, 出力テープに  $x$  がコピーされているはずである.
2. 出力テープの左端にたどり着くまで, 入力ヘッドを左に移動させる. このとき, 入力ヘッドは動かさない. すると, 入力ヘッドの右の区画に  $y$  の最下位ビット, 出力ヘッドの右の区画に  $x$  の最下位ビットがあるはずである.
3. 繰り上がりのなし/あるを状態  $q_3/q_4$  で区別しながら,  $x, y$  の各桁の足し算をしていく.
4. 全ての桁を足し終えたとき, 状態が  $q_3$  なら特に何もせず,  $q_4$  なら出力テープの最上位ビットに 1 を出力して



終了.

その実装は, 以下のようになる.

$\langle q_s, \triangleright, \triangleright, q_1, \triangleright, \triangleright, +1, 0 \rangle$   
 $\langle q_1, 0, b, q_1, b, 0, +1, +1 \rangle$   
 $\langle q_1, 1, b, q_1, b, 1, +1, +1 \rangle$   
 $\langle q_1, b, b, q_2, b, b, 0, -1 \rangle$   
 $\langle q_2, b, 0, q_2, b, 0, 0, -1 \rangle$   
 $\langle q_2, b, 1, q_2, b, 0, 1, -1 \rangle$   
 $\langle q_2, b, \triangleright, q_3, b, \triangleright, +1, +1 \rangle$   
 $\langle q_3, 0, 0, q_3, b, 0, +1, +1 \rangle$   
 $\langle q_3, 0, 1, q_3, b, 1, +1, +1 \rangle$   
 $\langle q_3, 1, 0, q_3, b, 1, +1, +1 \rangle$   
 $\langle q_3, 1, 1, q_4, b, 0, +1, +1 \rangle$   
 $\langle q_4, 0, 0, q_3, b, 1, +1, +1 \rangle$   
 $\langle q_4, 0, 1, q_4, b, 0, +1, +1 \rangle$   
 $\langle q_3, 1, 0, q_4, b, 0, +1, +1 \rangle$   
 $\langle q_3, 1, 1, q_4, b, 1, +1, +1 \rangle$   
 $\langle q_3, b, b, q_h, b, b, 0, 0 \rangle$   
 $\langle q_4, b, b, q_h, b, 1, 0, 0 \rangle$

演習 3.5

演習 3.6

演習 3.7

演習 3.8 NOT について;

$$\text{NOT } x = x \text{ NAND } x$$

AND について;

$$x \text{ AND } y = \text{NOT } (x \text{ NAND } y)$$

OR について;

$$x \text{ OR } y = (\text{NOT } x) \text{ NAND } (\text{NOT } y)$$

XOR について;

$$x \text{ XOR } y = (x \text{ OR } y) \text{ AND } (x \text{ NAND } y)$$

演習 3.9

$$\begin{aligned}
 g(n) = \Omega(f(n)) \text{ as } n \rightarrow \infty &\Leftrightarrow \exists n_0, \exists c > 0 \text{ s.t. } n \geq n_0 \Rightarrow g(n) \geq cf(n) \\
 &\Leftrightarrow \exists n_0, \exists c > 0 \text{ s.t. } n \geq n_0 \Rightarrow f(n) \leq \frac{1}{c}g(n) \\
 &\Leftrightarrow f(n) = O(g(n)) \text{ as } n \rightarrow \infty.
 \end{aligned}$$

演習 3.10  $g(n)$  が  $k$  次の多項式で,  $k \geq l$  なる正の定数  $l$  に対して,

$$\lim_{n \rightarrow \infty} \left| \frac{g(n)}{n^l} \right| = c$$

なる 0 以上の有界な定数  $c$  が存在する. つまり,

$$g(n) = O(n^l) \text{ as } n \rightarrow \infty.$$

演習 3.11 ロピタルの定理より,  $k > 0$  なる  $k$  に対して,

$$\lim_{n \rightarrow \infty} \left| \frac{\log n}{n^k} \right| = \lim_{n \rightarrow \infty} \frac{1}{kn^k} = 0$$

であるから,

$$\log n = O(n^k) \text{ as } n \rightarrow \infty.$$

演習 3.12 任意の  $k$  に対して,

$$\lim_{n \rightarrow \infty} \log \frac{n^k}{n^{\log n}} = \lim_{n \rightarrow \infty} (k - \log n) \log n = -\infty$$

なので,  $\log$  の連続性から,

$$\lim_{n \rightarrow \infty} \left| \frac{n^k}{n^{\log n}} \right| = 0.$$

つまり,

$$n^k = O(n^{\log n}) \text{ as } n \rightarrow \infty.$$

一方, 任意の  $k$  に対して,

$$\lim_{n \rightarrow \infty} \log \frac{n^{\log n}}{n^k} = \lim_{n \rightarrow \infty} (\log n - k) \log n = \infty$$

なので,  $\log$  の連続性から,

$$\lim_{n \rightarrow \infty} \left| \frac{n^{\log n}}{n^k} \right| = \infty.$$

つまり,

$$n^{\log n} \neq O(n^k) \text{ as } n \rightarrow \infty.$$

演習 3.13 任意の  $c \geq 1$  に対して,

$$\lim_{n \rightarrow \infty} \log \frac{c^n}{n^{\log n}} = \lim_{n \rightarrow \infty} n \log c - (\log n)^2 = \infty$$

なので,  $\log$  の連続性から,

$$\lim_{n \rightarrow \infty} \left| \frac{c^n}{n^{\log n}} \right| = \infty.$$

つまり,

$$c^n = \Omega(n^{\log n}) \text{ as } n \rightarrow \infty.$$

一方, 任意の  $c \geq 1$  に対して,

$$\lim_{n \rightarrow \infty} \log \frac{n^{\log n}}{c^n} = \lim_{n \rightarrow \infty} (\log n)^2 - n \log c = -\infty$$

なので,  $\log$  の連続性から,

$$\lim_{n \rightarrow \infty} \left| \frac{n^{\log n}}{c^n} \right| = -\infty.$$

つまり,

$$c^n \neq \Omega(n^{\log n}) \text{ as } n \rightarrow \infty.$$

#### 演習 3.14

$$\begin{aligned} \exists n_1, \exists c_1 > 0 \text{ s.t. } n \geq n_1 &\Rightarrow |e(n)| \leq c_1 |f(n)| \\ \exists n_2, \exists c_2 > 0 \text{ s.t. } n \geq n_2 &\Rightarrow |g(n)| \leq c_2 |h(n)| \end{aligned}$$

であるので,

$$n_0 = \max(n_1, n_2), \quad c = c_1 c_2$$

として,

$$\exists n_0, \exists c > 0 \text{ s.t. } n \geq n_0 \Rightarrow |e(n)g(n)| \leq c |f(n)h(n)|$$

が成り立つので,

$$e(n)g(n) = O(f(n)h(n)).$$

**演習 3.15** 「比較と交換」の演算を  $k$  回適用すると, 高々  $2^k$  個の要素が正しい順序に配列される. したがって,  $n!$  個の可能な配列のどの配列に対しても, 正しくソートするには, 少なくとも  $\log_2 n!$  回「比較と交換」適用する必要がある. 以下では, 正しくソートするのに必要な「比較と交換」の演算の回数  $N$  とする. ここで,  $n \geq e^2$  で,

$$N \geq \log_2 n! > \log n! \geq \int_0^1 \log x \, dx = n \log n - n \geq \frac{1}{2} n \log n$$

が成り立つので,

$$\lim_{n \rightarrow \infty} \frac{N}{n \log n} > \frac{1}{2}.$$

よって, ソーティングに必要な「比較と交換」の演算の回数は  $\Omega(n \log n)$ .

#### 演習 3.16

**演習 3.17** 素因数分解の決定問題 **P** に属するとすると, 素因数分解の決定問題は,  $n$  を素因数分解したい数の桁数,  $f(n)$  を多項式として, **TIMEO** ( $f(n)$ ). また, 数  $m$  の素因数を見つけるには, 2 から  $\sqrt{m}$  の数について, 素因数分解の決定問題のアルゴリズムを施せば良い. 以上より, 数  $m$  の素因数を見つけるのに必要な時間計算量は, **TIMEO** ( $\sqrt{m} f(\log m)$ ). これは,  $f(n)$  が多項式なので, 多項式時間である.

逆も同様に示せる.

演習 3.18 まず,  $\mathbf{P}=\mathbf{coP}$ であることを示す. 言語  $L$  を受理する Turing 機械  $M$  を考える. 言語  $L$  の補集合を  $\bar{L}$  とする. 言語  $\bar{L}$  を受理し, 言語  $L$  を拒絶する Turing 機械  $M'$  は, Turing 機械  $M$  で受理する入力を拒絶すれば良いだけなので,  $L$  と  $\bar{L}$  の属する計算量クラスは同じである. よって,  $\mathbf{P}=\mathbf{coP}$ .

$\mathbf{P}=\mathbf{NP}$  であるとする,  $\mathbf{coP}=\mathbf{coNP}$ . ここで, 上に示したことから,  $\mathbf{NP}=\mathbf{P}=\mathbf{coP}=\mathbf{coNP}$ . ゆえに, 示したい命題の対偶が示された.

演習 3.19 REACHABILITY 問題を解くにあたっては, グラフに多重辺がある場合, あらかじめ 1 本の辺に置き換えて良い. すると, 辺の数  $|E|$  は  $O(n^2)$  となる. そこで, 深さ優先探索や幅優先探索を行えば, REACHABILITY 問題を  $O(|E|) = O(n^2)$  で解ける.

演習 3.20 連結グラフ  $G$  に対して, 「 $G$  が Euler 閉路  $C$  をもつ」 $\iff$ 「 $G$  の各頂点の次数が偶数」を示す.

$\implies$ ) が Euler 閉路  $C$  上の頂点に注目すると, その頂点に入る辺に対応して必ずその頂点から出る辺が 1 対 1 で対応する. よって,  $G$  の各頂点の次数が偶数.

$\impliedby$ ) 連結グラフ  $G$  の各頂点の次数が偶数とすると, ある頂点  $v_0$  から出発点として,  $v_0$  に到達しない限り, 到達した点には奇数本のまだ通っていない辺が必ず存在するので, 進み続けることができる. こうして得られた閉路  $C$  とする. グラフ  $G$  は連結なので, まだ通っていない辺があれば, その辺に接続する頂点  $v_1$  が存在する. その  $v_1$  を出発点として,  $C$  同様閉路  $C_1$  を得る. こうして得られた  $C$  と  $C_1$  を合わせてできる新たな閉路を  $C$  と置き換える. この手順を, まだ通っていない辺がなくなるまで続けることで, Euler 閉路  $C$  を得られる.

演習 3.21  $L_1$  が  $L_2$  に,  $L_2$  が  $L_3$  に可約なので,

$$\begin{aligned} R(x) \in L_1 &\iff x \in L_2 \\ R'(y) \in L_2 &\iff y \in L_3 \end{aligned}$$

多項式時間の演算  $R, R'$  が存在する. よって,

$$(R \circ R')(y) \in L_1 \iff y \in L_3$$

なる多項式時間の演算  $R \circ R'$  が存在する. したがって,  $L_1$  は  $L_3$  に可約.

演習 3.22  $L$  が計算量クラス  $\mathbf{X}$  で完全だとすると,  $\mathbf{X}$  の任意の言語  $l$  に対して,

$$R_l(x) \in L \iff x \in l$$

なる多項式時間の演算  $R_l$  が存在する. 加えて,  $L$  が  $L'$  に可約なので,

$$R(y) \in L' \iff y \in L$$

なる多項式時間の演算  $R$  が存在する. 以上より,  $\mathbf{X}$  の任意の言語  $l$  に対して,

$$(R \circ R_l)(x) \in L_1 \iff x \in l$$

なる多項式時間の演算  $R \circ R_l$  が存在する. よって,  $L'$  も計算量クラス  $\mathbf{X}$  で完全.

演習 3.23

演習 3.24

演習 3.25

演習 3.26

## 演習 3.27

演習 3.28 **BPP** の元  $L_1$  に対して,  $x_1 \in L_1$  であるかを判定する確率的チューリング機械  $M_1$  は, その定義より多項式時間だけ計算したのち, 最大で  $1/4$  の確率で判定を誤る. 一方,  $0 \leq k < 1/2$  として, 言語  $L_2L$  に対して  $x_2$  が  $L_2$  に含まれるか否かの判定を, 多項式時間だけ計算したのち, 最大で  $1 - k$  の確率で誤る確率的チューリング機械  $M_2$  があるとする. このとき,  $x_2 \in L_2$  を入力として  $M_2$  を  $\lceil 2 \log 4 / (2k - 1)^2 \rceil$  回以上用いて得られた結果 (拒否 or 受容) のうち, より多く得られた結果を受容することで, 誤り確率を  $1/4$  未満に抑えることができる (定理 3.3 より).  $M_2$  を  $\lceil 2 \log 4 / (2k - 1)^2 \rceil$  以上用いても, 計算時間が多項式時間であることには変わらないので  $L_2 \in \mathbf{BPP}$ .

演習 3.29 Fredkin ゲートの真理値表より明らか.

演習 3.30 図 3.14 をよく見ればわかる.

演習 3.31

演習 3.32

## 第 4 章

# 量子回路

演習 4.1  $X$  の固有値, 固有ベクトルは,

$$\begin{aligned} |\lambda_X = +1\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \cos \frac{\pi}{4} |0\rangle + \sin \frac{\pi}{4} |1\rangle \\ |\lambda_X = -1\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \cos \frac{\pi}{4} |0\rangle + e^{i\pi} \sin \frac{\pi}{4} |1\rangle. \end{aligned}$$

$Y$  の固有値, 固有ベクトルは,

$$\begin{aligned} |\lambda_Y = +1\rangle &= \frac{|0\rangle - i|1\rangle}{\sqrt{2}} = \cos \frac{\pi}{4} |0\rangle + e^{i\frac{3\pi}{2}} \sin \frac{\pi}{4} |1\rangle \\ |\lambda_Y = -1\rangle &= \frac{|0\rangle + i|1\rangle}{\sqrt{2}} = \cos \frac{\pi}{4} |0\rangle + e^{i\frac{\pi}{2}} \sin \frac{\pi}{4} |1\rangle. \end{aligned}$$

$Z$  の固有値, 固有ベクトルは,

$$\begin{aligned} |\lambda_Z = +1\rangle &= |0\rangle = \cos 0 |0\rangle + \sin 0 |1\rangle \\ |\lambda_Z = -1\rangle &= |1\rangle = \cos \frac{\pi}{2} |0\rangle + \sin \frac{\pi}{2} |1\rangle. \end{aligned}$$

演習 4.2

$$\begin{aligned} \exp(iAx) &= \sum_k \frac{1}{k!} (iAx)^k \\ &= \sum_{k:\text{even}} \frac{1}{k!} (-1)^{\frac{k}{2}} (Ax)^k + i \sum_{k:\text{odd}} \frac{1}{k!} (-1)^{\frac{k-1}{2}} (Ax)^k \\ &= I \sum_{k:\text{even}} \frac{1}{k!} (-1)^{\frac{k}{2}} x^k + iA \sum_{k:\text{odd}} \frac{1}{k!} (-1)^{\frac{k-1}{2}} x^k \\ &= (\cos x)I + (i \sin x)A. \end{aligned}$$

演習 4.3

$$R_z\left(\frac{\pi}{4}\right) = e^{-i\frac{\pi}{8}} T.$$

演習 4.4

$$d$$

演習 4.5 Pauli 行列の反交換関係;

$$\{\sigma_i, \sigma_j\} = 2\delta_{ij}I$$

より,

$$(\mathbf{n} \cdot \boldsymbol{\sigma})^2 = \left( \sum_i n_i \sigma_i \right)^2 = \sum_{i,j} n_i n_j \sigma_i \sigma_j = \sum_i n_i^2 \sigma_i^2 + \sum_{i < j} n_i n_j \{\sigma_i, \sigma_j\} = I.$$

よって, 演習 4.2 より,

$$R_{\mathbf{n}}(\theta) = \exp\left(-i\theta \frac{\mathbf{n} \cdot \boldsymbol{\sigma}}{2}\right) = \left(\cos \frac{\theta}{2}\right) I - i \left(\sin \frac{\theta}{2}\right) \mathbf{n} \cdot \boldsymbol{\sigma}.$$

演習 4.6  $\mathbf{n}$  が  $z$  軸に平行になるような座標系が常にとれるので,  $\mathbf{n} = (0, 0, 1)$  のときだけ示せば十分である.

Bloch 球上の  $\lambda$  に対応する状態  $|\lambda\rangle$  を

$$|\lambda\rangle = \cos \frac{\theta_\lambda}{2} |0\rangle + e^{i\phi_\lambda} \sin \frac{\theta_\lambda}{2} |1\rangle$$

とすると,

$$\begin{aligned} R_z(\theta) |\lambda\rangle &= \left[ \left( \cos \frac{\theta}{2} \right) I - i \left( \sin \frac{\theta}{2} \right) Z \right] \left[ \cos \frac{\theta_\lambda}{2} |0\rangle + e^{i\phi_\lambda} \sin \frac{\theta_\lambda}{2} |1\rangle \right] \\ &= \cos \frac{\theta_\lambda}{2} \left[ \cos \frac{\theta}{2} - i \sin \frac{\theta}{2} \right] |0\rangle + e^{i\phi_\lambda} \sin \frac{\theta_\lambda}{2} \left[ \cos \frac{\theta}{2} + i \sin \frac{\theta}{2} \right] |1\rangle \\ &= e^{-i\frac{\theta}{2}} \cos \frac{\theta_\lambda}{2} |0\rangle + e^{i(\phi_\lambda + \frac{\theta}{2})} \sin \frac{\theta_\lambda}{2} |1\rangle \\ &= e^{-i\frac{\theta}{2}} \left[ \cos \frac{\theta_\lambda}{2} |0\rangle + e^{i(\phi_\lambda + \theta)} \sin \frac{\theta_\lambda}{2} |1\rangle \right] \end{aligned}$$

となり,  $|\lambda\rangle$  に  $R_z(\theta)$  を作用させることでえられる状態は, Bloch 球上で  $\lambda$  を  $z$  軸周りで  $\theta$  回転させたベクトルに対応していることが言えた.

演習 4.7

$$XY + YX = 0 \rightarrow XYX = -XXY = -Y$$

であること式 (4.7) を用いて,

$$XR_y(\theta)X = Xe^{-i\theta \frac{Y}{2}}X = X \left[ \left( \cos \frac{\theta}{2} \right) I + i \left( \sin \frac{\theta}{2} \right) Y \right] X = \left( \cos \frac{\theta}{2} \right) I - i \left( \sin \frac{\theta}{2} \right) Y = e^{i\theta \frac{Y}{2}} = R_y(-\theta).$$

演習 4.8 (1)  $\mu = 0, 1, 2, 3$ ,  $i = 1, 2, 3$  を走るとする. 任意の  $2 \times 2$  複素行列  $U$  は,  $I, X, Y, Z$  の線形結合でかける;

$$U = t_0 I + t_1 X + t_2 Y + t_3 Z.$$

$U$  がユニタリであるための必要十分条件は,  $t_\mu$  の偏角を  $\theta_\mu$  とすると,

$$\begin{aligned} UU^\dagger = 1 &\iff \sum_{\mu=0}^4 |t_\mu|^2 = 1, t_0 \bar{t}_i + \bar{t}_0 t_i = 0 \\ &\iff \sum_{\mu=0}^4 |t_\mu|^2 = 1, |t_0||t_i| \left( e^{i(\theta_0 - \theta_i)} + e^{-i(\theta_0 - \theta_i)} \right) = 0 \end{aligned}$$

まず,  $|t_\mu| \neq 0$  を考えると,  $U$  がユニタリであるための必要十分条件は,

$$\exists \theta \in \mathbb{R} \text{ s.t. } |t_0| = \cos \frac{\theta}{2}, \sum_{i=1}^3 |t_i|^2 = \sin^2 \frac{\theta}{2}, \exists n \in \mathbb{Z} \text{ s.t. } \theta_0 = \theta_i + \frac{2n+1}{2}\pi$$

と書き換えられる。ひとつめの条件は,  $\mathbf{n} = (n_1, n_2, n_3)$  を単位ベクトルとすれば,

$$|t_i| = n_i \sin \frac{\theta}{2}$$

と書けるとして良い。以上より,  $\forall_\mu |t_\mu| \neq 0$  のとき,

$$U = t_0 I + t_1 X + t_2 Y + t_3 Z$$

がユニタリであるための必要十分条件は,  $\theta \in \mathbb{R}$ ,  $n \in \mathbb{Z}$ ,  $\mathbf{n}$  を単位ベクトルとして,

$$t_0 = \cos \frac{\theta}{2} e^{i\theta_0}, t_i = n_i \sin \frac{\theta}{2} e^{i\theta_0 - \frac{2n+1}{2}\pi}$$

であることである。これは,  $\exists_\mu |t_\mu| = 0$  でも成立。よって, 任意の任意の  $2 \times 2$  のユニタリ行列  $U$  は,

$$U = e^{i\theta_0} \left[ \cos \frac{\theta}{2} \pm i \sin \frac{\theta}{2} (\mathbf{n} \cdot \boldsymbol{\sigma}) \right]$$

で表せる。 $\theta_0 = \alpha$  と書き換えて,  $\pm$  の符号は  $\mathbf{n}$  に入れてやれば,

$$U = e^{i\theta_0} \left[ \cos \frac{\theta}{2} - i \sin \frac{\theta}{2} (\mathbf{n} \cdot \boldsymbol{\sigma}) \right] = e^{i\alpha} R_{\mathbf{n}}(\theta).$$

(2)

$$H = \frac{X + Z}{\sqrt{2}}$$

なことを思い出せば,

$$\alpha = -\frac{\pi}{2}, \theta = \pi, \mathbf{n} = \left( \frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}} \right).$$

(3)

$$S = \frac{1+i}{2} I + \frac{1-i}{2} Z$$

なので,

$$\alpha = -\frac{\pi}{4}, \theta = \frac{\pi}{2}, \mathbf{n} = (0, 0, 1).$$

**演習 4.9**  $2 \times 2$  行列  $U = (\mathbf{u}_1, \mathbf{u}_2)$  がユニタリであるための必要十分条件は,  $U$  の各列に対する内積の条件が,

$$(\mathbf{u}_i, \mathbf{u}_j) = \delta_{ij}$$

を満たすことで, 式 (4.12) はこれを満たす。さらに,  $2 \times 2$  ユニタリ行列の独立な自由度は 4 で, 式 (4.12) はこのことも満たす。

**演習 4.10**

$$U = e^{i\alpha} R_x(\beta) R_y(\gamma) R_x(\delta).$$

**演習 4.11** 定理 4.1 では単一 q ビットに働く任意のオペレーター  $U$  が,

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

で表せることを示した。これは, 任意の Bloch 球面上での回転が, 適当な  $\beta, \gamma, \delta$  を選ぶことで,  $z$  軸周りに回転角  $\delta$  で回転し,  $y$  軸周りに回転角  $\gamma$  で回転し,  $z$  軸周りの回転角  $\beta$  することによって, 一意に特徴付けられることを示している。



回転は幾何学的な操作なので、回転軸を  $y, z$  に限らず、互いに直交する  $\mathbf{n}, \mathbf{m}$  としても、同様の主張が成立することがわかる。つまり、単一 q ビットに働く任意のオペレーター  $U_1$  が、

$$U_1 = e^{i\alpha_1} R_{\mathbf{n}}(\beta_1) R_{\mathbf{m}}(\gamma_1) R_{\mathbf{n}}(\beta_2)$$

で表せる。上式は、とある軸  $\mathbf{a}_1$  周りの  $\theta_1$  回転を表すオペレーターとも解釈できる。同様に、とある軸  $\mathbf{a}_2$  周りの  $\theta_2$  回転を表すオペレーター  $U_2$  は、

$$U_2 = e^{i\alpha_2} R_{\mathbf{m}}(\beta_2) R_{\mathbf{n}}(\gamma_3) R_{\mathbf{n}}(\beta_3)$$

と表せる。同様に  $U_3, U_4 \dots$  も作れる。とある軸  $\mathbf{a}$  周りに  $\theta$  回転させるという操作  $U$  は、軸  $\mathbf{a}_1$  周りの  $\theta_1$  回転  $\rightarrow$  軸  $\mathbf{a}_2$  周りの  $\theta_2$  回転  $\rightarrow$  軸  $\mathbf{a}_3$  周りの  $\theta_3$  回転  $\rightarrow \dots$  といういくつかの回転操作に分解できるので、

$$U = U_1 U_2 U_3 \dots = e^{i\alpha} R_{\mathbf{n}}(\beta_1) R_{\mathbf{m}}(\gamma_1) R_{\mathbf{n}}(\beta_2) R_{\mathbf{m}}(\gamma_2) R_{\mathbf{n}}(\gamma_3) R_{\mathbf{n}}(\gamma_4) \dots$$

の形で書けるはずである。

演習 4.12

演習 4.13

$$H = \frac{X + Z}{\sqrt{2}}$$

なので、 $X^2 = Z^2 = 1, \{X, Z\} = 0$  を用いて、

$$H X H = \frac{X X X + X X Z + Z X X + Z X Z}{2} = Z.$$

同様に、

$$\begin{aligned} H Y H &= \frac{X Y X + X Y Z + Z Y X + Z Y Z}{2} = -Y. \\ H Z H &= \frac{Z Z Z + Z Z X + X Z Z + X Z X}{2} = X. \end{aligned}$$

演習 4.14 演習 4.2, 4.3, 4.13 の結果を用いて、

$$\begin{aligned} H T H &= e^{i\frac{\pi}{8}} H R_z\left(\frac{\pi}{4}\right) H \\ &= e^{i\frac{\pi}{8}} H \left[ I \cos \frac{\pi}{4} + i Z \sin \frac{\pi}{4} \right] H \\ &= e^{i\frac{\pi}{8}} \left[ I \cos \frac{\pi}{4} + i X \sin \frac{\pi}{4} \right] \\ &= e^{i\frac{\pi}{8}} R_x\left(\frac{\pi}{4}\right). \end{aligned}$$

演習 4.15 (1) 演習 2.43 の結果を用いて、

$$(\mathbf{n}_2 \cdot \boldsymbol{\sigma})(\mathbf{n}_1 \cdot \boldsymbol{\sigma}) = \sum_{i,j} n_{1j} n_{2i} \sigma_i \sigma_j = \sum_{i,j} n_{1j} n_{2i} \left( \delta_{ij} I + i \sum_k \epsilon_{ijk} \sigma_k \right) = (\mathbf{n}_1 \cdot \mathbf{n}_2) I - i (\mathbf{n}_1 \times \mathbf{n}_2) \cdot \boldsymbol{\sigma}.$$

この関係式を用いると、

$$\begin{aligned} R_{\mathbf{n}_2}(\beta_2) R_{\mathbf{n}_1}(\beta_1) &= \left[ \left( \cos \frac{\beta_1}{2} \right) I - i \left( \sin \frac{\beta_1}{2} \right) \mathbf{n}_2 \cdot \boldsymbol{\sigma} \right] \left[ \left( \cos \frac{\beta_2}{2} \right) I - i \left( \sin \frac{\beta_2}{2} \right) \mathbf{n}_1 \cdot \boldsymbol{\sigma} \right] \\ &= \left( \cos \frac{\beta_1}{2} \cos \frac{\beta_2}{2} \right) I - i \left( \sin \frac{\beta_1}{2} \cos \frac{\beta_2}{2} \right) \mathbf{n}_2 \cdot \boldsymbol{\sigma} \end{aligned}$$

$$\begin{aligned}
& -i \left( \sin \frac{\beta_2}{2} \cos \frac{\beta_1}{2} \right) \mathbf{n}_1 \cdot \boldsymbol{\sigma} - \left( \sin \frac{\beta_1}{2} \sin \frac{\beta_2}{2} \right) (\mathbf{n}_1 \cdot \boldsymbol{\sigma}) (\mathbf{n}_2 \cdot \boldsymbol{\sigma}) \\
& = \left( \cos \frac{\beta_1}{2} \cos \frac{\beta_2}{2} - \sin \frac{\beta_1}{2} \sin \frac{\beta_2}{2} \mathbf{n}_1 \cdot \mathbf{n}_2 \right) I \\
& \quad - i \left( \sin \frac{\beta_1}{2} \cos \frac{\beta_2}{2} \mathbf{n}_1 + \sin \frac{\beta_2}{2} \cos \frac{\beta_1}{2} \mathbf{n}_2 - \sin \frac{\beta_1}{2} \sin \frac{\beta_2}{2} \mathbf{n}_1 \times \mathbf{n}_2 \right) \cdot \boldsymbol{\sigma}.
\end{aligned}$$

一方,

$$R_{\mathbf{n}_{12}}(\beta_{12}) = \left( \cos \frac{\beta_{12}}{2} \right) I - i \left( \sin \frac{\beta_{12}}{2} \right) \mathbf{n}_{12} \cdot \boldsymbol{\sigma}.$$

$R_{\mathbf{n}_{12}}(\beta_{12}) = R_{\mathbf{n}_2}(\beta_2)R_{\mathbf{n}_1}(\beta_1)$  であることと,  $I, X, Y, Z$  が互いに一次独立であることから,

$$\begin{aligned}
\cos \frac{\beta_{12}}{2} &= \cos \frac{\beta_1}{2} \cos \frac{\beta_2}{2} - \sin \frac{\beta_1}{2} \sin \frac{\beta_2}{2} \mathbf{n}_1 \cdot \mathbf{n}_2 \\
\sin \frac{\beta_{12}}{2} \mathbf{n}_{12} &= \sin \frac{\beta_1}{2} \cos \frac{\beta_2}{2} \mathbf{n}_1 + \sin \frac{\beta_2}{2} \cos \frac{\beta_1}{2} \mathbf{n}_2 - \sin \frac{\beta_1}{2} \sin \frac{\beta_2}{2} \mathbf{n}_1 \times \mathbf{n}_2.
\end{aligned}$$

(2) (1) より明らか.

演習 4.16

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{pmatrix} I & I \\ I & -I \end{pmatrix} \quad \text{と} \quad I \otimes H = \begin{pmatrix} H & H \\ H & H \end{pmatrix}$$

演習 4.17

$$\begin{pmatrix} I & O \\ O & H \end{pmatrix} \begin{pmatrix} I & O \\ O & Z \end{pmatrix} \begin{pmatrix} I & O \\ O & H \end{pmatrix} = \begin{pmatrix} I & O \\ O & HZH \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

つまり,

$$\begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \boxed{H} \text{---} \boxed{Z} \text{---} \boxed{H} \text{---} \end{array} = \begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \oplus \end{array}$$

演習 4.18 いずれのゲートも, 計算基底で,

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

演習 4.19 任意の密度行列  $\rho = (\rho_{ij})$  を

$$\rho = \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} \rho_{11} & \rho_{12} & \rho_{13} & \rho_{14} \\ \rho_{21} & \rho_{22} & \rho_{23} & \rho_{24} \\ \rho_{31} & \rho_{32} & \rho_{33} & \rho_{34} \\ \rho_{41} & \rho_{42} & \rho_{43} & \rho_{44} \end{pmatrix}$$

と書く.  $\rho$  に対応する混合状態に CNOT ゲート  $U$  を作用させると,

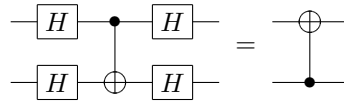
$$U\rho U^\dagger = \begin{pmatrix} I & O \\ O & X \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & O \\ O & X \end{pmatrix} = \begin{pmatrix} A & BX \\ XC & XDX \end{pmatrix} = \begin{pmatrix} \rho_{11} & \rho_{12} & \rho_{14} & \rho_{13} \\ \rho_{21} & \rho_{22} & \rho_{24} & \rho_{23} \\ \rho_{33} & \rho_{34} & \rho_{44} & \rho_{43} \\ \rho_{31} & \rho_{32} & \rho_{34} & \rho_{33} \end{pmatrix}$$

となり, 題意が示された.

演習 4.20 CNOT ゲート  $U$  として, 計算基底では,

$$\begin{aligned}
 (H \otimes H)U(H \otimes H) &= \frac{1}{2} \begin{pmatrix} H & H \\ H & -H \end{pmatrix} \begin{pmatrix} I & O \\ O & X \end{pmatrix} \begin{pmatrix} H & H \\ H & -H \end{pmatrix} \\
 &= \frac{1}{2} \begin{pmatrix} I + HXH & I - HXH \\ I - HXH & I + HXH \end{pmatrix} \\
 &= \frac{1}{2} \begin{pmatrix} I + Z & I - Z \\ I - Z & I + Z \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}
 \end{aligned}$$

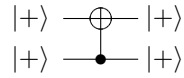
つまり,



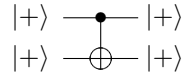
ここで,

$$(H \otimes H)U(H \otimes H)|+\rangle|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = |+\rangle|+\rangle$$

であることと, 先に示した回路の同等性を用いて,



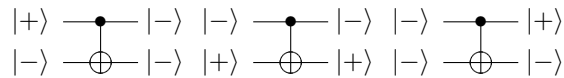
つまり,



を得る. 同様に,

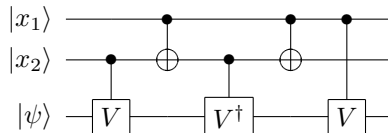
$$\begin{aligned}
 (H \otimes H)U(H \otimes H)|+\rangle|-\rangle &= |+\rangle|-\rangle \\
 (H \otimes H)U(H \otimes H)|-\rangle|+\rangle &= |-\rangle|-\rangle \\
 (H \otimes H)U(H \otimes H)|-\rangle|-\rangle &= |-\rangle|+\rangle
 \end{aligned}$$

であることと, 先に示した回路の同等性から,



を得る.

演習 4.21  $V$  が  $V^2 = U$  なるユニタリゲートとすると,

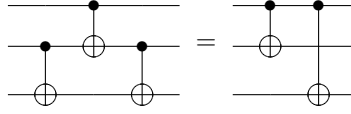


の標的ビットは,

$$\begin{cases} I & (x_1, x_2) = (0, 0) \\ VV^\dagger = I & (x_1, x_2) = (0, 1) \\ V^\dagger V = I & (x_1, x_2) = (1, 0) \\ VV = U & (x_1, x_2) = (1, 1) \end{cases}$$

となり, これは上記の回路が制御  $C^2(U)$  ゲートであることを示している.

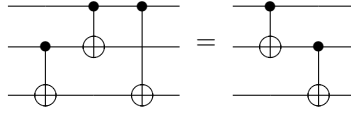
演習 4.22 まず,



である. なせなら, 左辺の回路の入力  $|a\rangle|b\rangle|c\rangle$  として,

$$|a\rangle|b\rangle|c\rangle \rightarrow |a\rangle|b\rangle|b \oplus c\rangle \rightarrow |a\rangle|a \oplus b\rangle|b \oplus c\rangle \rightarrow |a\rangle|a \oplus b\rangle|a \oplus b \oplus b \oplus c\rangle = |a\rangle|a \oplus b\rangle|a \oplus c\rangle$$

であるからである. さらに,

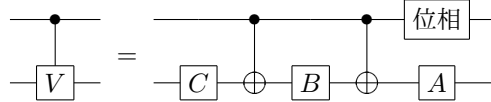


である. なせなら, 左辺の回路の入力  $|a\rangle|b\rangle|c\rangle$  として,

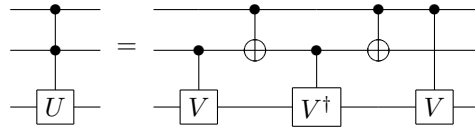
$$|a\rangle|b\rangle|c\rangle \rightarrow |a\rangle|b\rangle|b \oplus c\rangle \rightarrow |a\rangle|a \oplus b\rangle|b \oplus c\rangle \rightarrow |a\rangle|a \oplus b\rangle|a \oplus b \oplus c\rangle$$

であるからである.

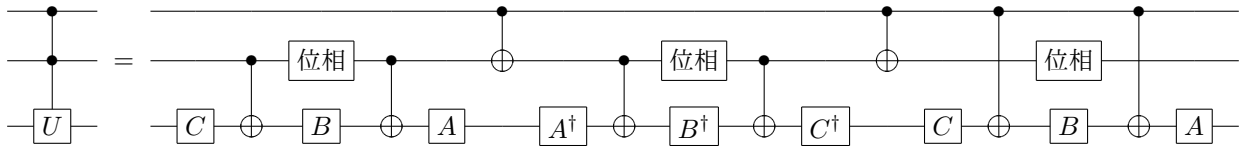
系 4.2 から, 任意の制御  $V$  が,  $ABC = I$  なるユニタリ  $A, B, C$  で,



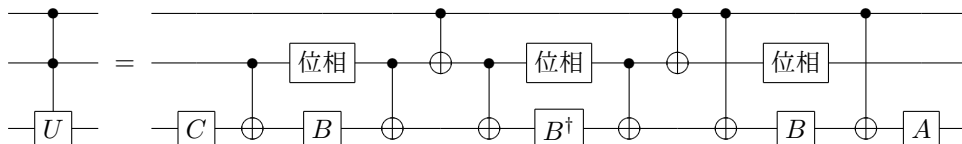
と書けることと, 演習 4.21 から 任意の  $C^2(U)$  は,  $V^2 = U$  なるユニタリ  $V$  を用いて,



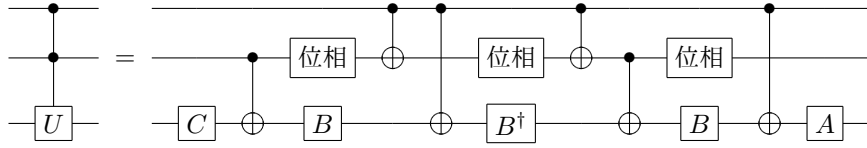
つまり,



と書ける.  $A, C$  のユニタリ性より,



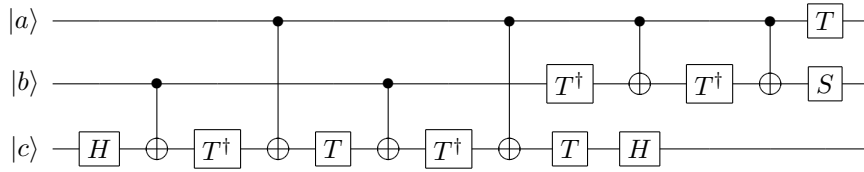
はじめに示した回路の等価性より,



以上より, 任意の  $C^2(U)$  は, 単一 q ビットゲート 8 個と CNOT ゲート 6 個で構築可能.

演習 4.23 問題の意味がわからない.

演習 4.24



という回路  $U$  は,

$$U |a\rangle \otimes |b\rangle \otimes |c\rangle = T |a\rangle \otimes T^\dagger X^a T^\dagger X^a S |b\rangle \otimes H (X^b T^\dagger X^a T)^2 H |c\rangle$$

で定義されている. ここで, 計算基底では,

$$T^\dagger X^a T^\dagger X^a S = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I & (a=0) \\ e^{-i\frac{\pi}{4}} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = e^{-i\frac{\pi}{4}} S & (a=1) \end{cases}$$

$$H (X^b T^\dagger X^a T)^2 H = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I & (ab=0) \\ -i \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -iX & (ab=1) \end{cases}$$

であることと,

$$T|0\rangle = |0\rangle, T|1\rangle = e^{i\frac{\pi}{4}}|1\rangle, S|0\rangle = |0\rangle, S|1\rangle = i|1\rangle$$

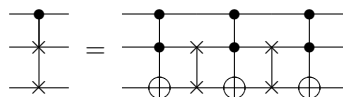
であることを用いて,

$$U |a\rangle \otimes |b\rangle \otimes |c\rangle = \begin{cases} T|0\rangle \otimes I|b\rangle \otimes I|c\rangle & (a=0) \\ T|1\rangle \otimes e^{-i\frac{\pi}{4}} S|0\rangle \otimes I|c\rangle & (a=1, b=0) \\ T|1\rangle \otimes e^{-i\frac{\pi}{4}} S|1\rangle \otimes -iX|c\rangle & (a=1, b=1) \end{cases}$$

$$= \begin{cases} |0\rangle \otimes |b\rangle \otimes |c\rangle & (a=0) \\ |1\rangle \otimes |0\rangle \otimes |c\rangle & (a=1, b=0) \\ |1\rangle \otimes |0\rangle \otimes X|c\rangle & (a=1, b=1) \end{cases}$$

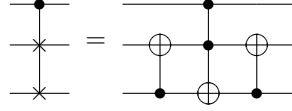
を得る. これは,  $U$  が Toffoli ゲートであることを示している.

演習 4.25 (1) Fredkin ゲートは, が Toffoli ゲート 3 つで,



と書ける.

(2) Fredkin ゲートは

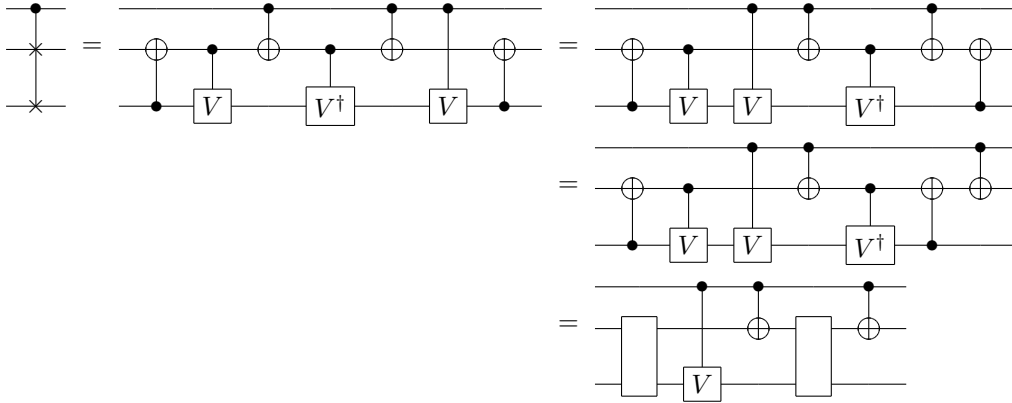


と書ける. なぜなら, 上の回路の入力  $|a\rangle|b\rangle|c\rangle$  として,

$$\begin{aligned} |a\rangle|b\rangle|c\rangle &\xrightarrow{\text{CNOT}} |a\rangle|b \oplus c\rangle|c\rangle \xrightarrow{\text{Toffoli}} |a\rangle|b \oplus c\rangle|ab \oplus ac \oplus c\rangle \\ &\xrightarrow{\text{CNOT}} |a\rangle|ab \oplus ac \oplus b\rangle|ab \oplus ac \oplus c\rangle = \begin{cases} |a\rangle|b\rangle|c\rangle & (a = 0) \\ |a\rangle|c\rangle|b\rangle & (a = 1) \end{cases} \end{aligned}$$

となるからである.

(3)(4)



演習 4.26 準備として,

$$R_y(\theta)X^cR_y(\phi) = \begin{cases} R_y(\theta + \phi) & (c = 0) \\ \begin{pmatrix} -\sin \frac{\theta-\phi}{2} & \cos \frac{\theta-\phi}{2} \\ \cos \frac{\theta-\phi}{2} & \sin \frac{\theta-\phi}{2} \end{pmatrix} & (c = 1) \end{cases}.$$

問題の回路  $U$  は, 以下で定義されている;

$$\begin{aligned} U|c_1\rangle \otimes |c_2\rangle \otimes |t\rangle &= |c_1\rangle \otimes |c_2\rangle \otimes R_y\left(\frac{\pi}{4}\right) X^{c_2} R_y\left(\frac{\pi}{4}\right) X^{c_1} R_y\left(-\frac{\pi}{4}\right) X^{c_2} R_y\left(-\frac{\pi}{4}\right) \\ &= \begin{cases} |c_1\rangle \otimes |c_2\rangle \otimes I|t\rangle = |c_1\rangle \otimes |c_2\rangle \otimes |t\rangle & (c_1 = 0, c_2 = 0) \\ |c_1\rangle \otimes |c_2\rangle \otimes I|t\rangle = |c_1\rangle \otimes |c_2\rangle \otimes |t\rangle & (c_1 = 0, c_2 = 1) \\ -|c_1\rangle \otimes |c_2\rangle \otimes Z|t\rangle & (c_1 = 1, c_2 = 0) \\ |c_1\rangle \otimes |c_2\rangle \otimes X|t\rangle & (c_1 = 1, c_2 = 1) \end{cases} \\ &= e^{i\theta(c_1, c_2, t)} |c_1\rangle |c_2\rangle |t \oplus c_1 \cdot c_2\rangle. \end{aligned}$$

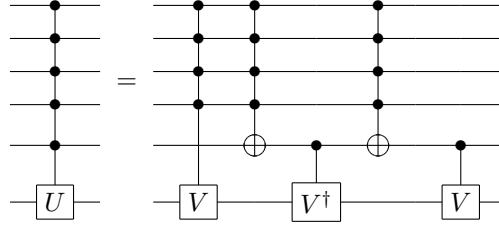
ここで,

$$\theta(c_1, c_2, t) = \begin{cases} \pi & (c_1 = 1, c_2 = 0, t = 0) \\ 0 & (\text{otherwise}) \end{cases}$$

とした.

演習 4.27

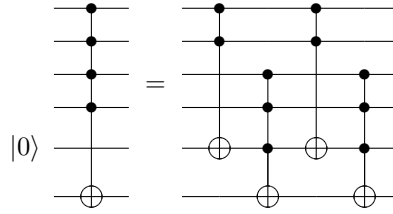
## 演習 4.28



演習 4.29 演習 4.30 詳しいことは, <https://arxiv.org/pdf/0708.3274.pdf>. ここでは, 概略を述べる.

まず,  $C^n(X)$  については下図のように,  $C^{\lfloor n/2 \rfloor}(X), C^{n-\lfloor n/2 \rfloor}(X)$  と作業ビット 1 つで作れる. そこで,  $C^n(X)$  を作るのに必要な Toffoli ゲート, CNOT ゲートの数の総和  $x_n$  として,

$$x_n = 2x_{\lfloor n/2 \rfloor} + 2x_{n-\lfloor n/2 \rfloor} \sim 4x_{n/2} \rightarrow x_n = O(4^{\log n}) = O(n).$$



このことと,  $C^n(U)$  は  $C^{n-1}(V), C^{n-1}(X), C^{n-1}(X), C^1(V), C^1(V^\dagger)$  で作れること (演習 4.28 と同様) から,  $C^n(U)$  を作るのに必要な Toffoli ゲート, CNOT ゲート, 単一 q ビットの数の総和  $y_n$  として,

$$y_n = y_{n-1} + O(n) \rightarrow y_n = O(n^2).$$

## 演習 4.31

$$\begin{aligned} CX_1C|a\rangle|b\rangle &= X_1|a\rangle X_2^a X_2^{\bar{a}}|b\rangle = X_1|a\rangle X_2^{a+\bar{a}}|b\rangle = X_1|a\rangle X_2|b\rangle \\ CY_1C|a\rangle|b\rangle &= Y_1|a\rangle X_2^a X_2^{\bar{a}}|b\rangle = Y_1|a\rangle X_2^{a+\bar{a}}|b\rangle = Y_1|a\rangle X_2|b\rangle \\ CZ_1C|a\rangle|b\rangle &= Z_1|a\rangle X_2^a X_2^{\bar{a}}|b\rangle = Z_1|a\rangle X_2^{a+\bar{a}}|b\rangle = Z_1|a\rangle I|b\rangle \\ CX_2C|a\rangle|b\rangle &= I|a\rangle X_2^a X_2 X_2^a|b\rangle = I|a\rangle X_2^{a+a+1}|b\rangle = I|a\rangle X_2|b\rangle \\ CY_2C|a\rangle|b\rangle &= I|a\rangle X_2^a Y_2 X_2^a|b\rangle = (-1)^a|a\rangle Y_2 X_2^a X_2^a|b\rangle = Z_1|a\rangle Y_2|b\rangle \\ CZ_2C|a\rangle|b\rangle &= I|a\rangle X_2^a Z_2 X_2^a|b\rangle = (-1)^a|a\rangle Z_2 X_2^a X_2^a|b\rangle = Z_1|a\rangle Z_2|b\rangle \\ R_{z,1}(\theta)C|a\rangle|b\rangle &= \left(\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z_1\right)|a\rangle X_2^a|b\rangle = X_2^a \left(\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z_1\right)|a\rangle|b\rangle = CR_{z,1}(\theta)|a\rangle|b\rangle \\ R_{x,1}(\theta)C|a\rangle|b\rangle &= \left(\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X_1\right)|a\rangle X_2^a|b\rangle = X_2^a \left(\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X_1\right)|a\rangle|b\rangle = CR_{x,1}(\theta)|a\rangle|b\rangle \end{aligned}$$

演習 4.32 (2.152) より,

$$\rho' = (I \otimes P_0)\rho(I \otimes P_0) + (I \otimes P_1)\rho(I \otimes P_1)$$

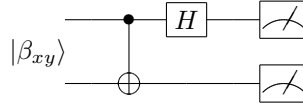
$$\rho = \rho_1 \otimes \rho_2$$

として,

$$\begin{aligned} \text{tr}_2(\rho') &= \text{tr}_2((I \otimes P_0)\rho(I \otimes P_0) + (I \otimes P_1)\rho(I \otimes P_1)) \\ &= \text{tr}_2(\rho_1 \otimes P_0 \rho_2 P_0 + \rho_1 \otimes P_1 \rho_2 P_1) \end{aligned}$$

$$\begin{aligned}
&= \rho_1 \text{tr}(P_0 \rho_2 P_0 + P_1 \rho_2 P_1) \\
&= \rho_1 \text{tr}(\rho_2 P_0 P_0 + \rho_2 P_1 P_1) \\
&= \rho_1 \text{tr}(\rho_2 P_0 + \rho_2 P_1) \\
&= \rho_1 \text{tr}(\rho_2) \\
&= \text{tr}_2(\rho)
\end{aligned}$$

## 演習 4.33

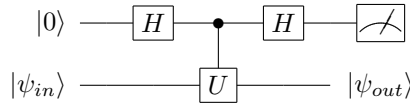


上の回路に対応すユニタリオペレータ  $U$  として,

$$\begin{aligned}
U |\beta_{xy}\rangle &= \frac{|0, y\rangle + |1, y\rangle + (-1)^x (|0, y\rangle - |1, y\rangle)}{2} \\
&= \frac{(1 + (-1)^x) |0, y\rangle + (1 - (-1)^x) |1, y\rangle}{2} \\
&= \begin{cases} |00\rangle & (x, y) = (0, 0) \\ |01\rangle & (x, y) = (0, 1) \\ |10\rangle & (x, y) = (1, 0) \\ |11\rangle & (x, y) = (1, 1) \end{cases}.
\end{aligned}$$

これは,  $U$  が Bell 基底  $|\beta_{xy}\rangle$  から計算基底へのユニタリ変換であることを示している.

## 演習 4.34



$U$  の固有値は  $\pm 1$  なので,

$$U = |+1\rangle \langle +1| - |-1\rangle \langle -1|$$

とかけ,  $U$  のユニタリ性より,

$$\langle +1| + 1\rangle = \langle -1| - 1\rangle = 1, \quad \langle +1| - 1\rangle = 0 \rightarrow | +1\rangle \langle +1| + | -1\rangle \langle -1| = I.$$

上の回路の演算は,

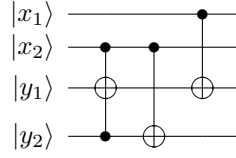
$$\begin{aligned}
|0\rangle |\psi_{in}\rangle &\rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |\psi_{in}\rangle \\
&\rightarrow \frac{|0\rangle \otimes |\psi_{in}\rangle}{2} + \frac{|1\rangle \otimes U |\psi_{in}\rangle}{2} \\
&\rightarrow \frac{(|0\rangle + |1\rangle) \otimes |\psi_{in}\rangle}{2} + \frac{(|0\rangle - |1\rangle) \otimes U |\psi_{in}\rangle}{2} \\
&= \frac{|0\rangle \otimes (1 + U) |\psi_{in}\rangle}{2} + \frac{|1\rangle \otimes (1 - U) |\psi_{in}\rangle}{2} \\
&= |0\rangle \otimes | +1\rangle \langle +1| \psi_{in}\rangle + |1\rangle \otimes | -1\rangle \langle -1| \psi_{in}\rangle
\end{aligned}$$

となるので,  $|\psi_{out}\rangle$  は, 第 1q ビットが  $|0\rangle$  のとき  $|+1\rangle$ , 第 1q ビットが  $|1\rangle$  のとき  $|-1\rangle$  を得る.



演習 4.35 制御ビットが  $\alpha|0\rangle + \beta|1\rangle$  でかけるとき, いずれの回路も確率  $|\alpha|^2, |\beta|^2$  で標的ビットを作用させる.

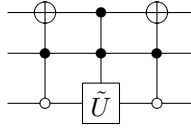
演習 4.36 Toffoli ゲートは 1 の位の桁上がりの役目を果たしており, 2 つの CNOT は各位の足し算に対応している.



演習 4.37

演習 4.38

演習 4.39  $010 \rightarrow 110 \rightarrow 111$



演習 4.40  $\mathbf{n} = (0, 0, 1)$  のときだけ示せばよい.

$$\begin{aligned}
 E(R_{\mathbf{n}}(\alpha), R_{\mathbf{n}}(\alpha + \beta)) &= |R_{\mathbf{n}}(\alpha) - R_{\mathbf{n}}(\alpha + \beta)| \\
 &= \left| e^{\frac{-i\alpha}{2}} \begin{pmatrix} 1 - e^{\frac{i\beta}{2}} & 0 \\ 0 & 1 - e^{-\frac{i\beta}{2}} \end{pmatrix} |\psi\rangle \right| \\
 &= \left| \left(1 - e^{\frac{i\beta}{2}}\right) \left(1 - e^{-\frac{i\beta}{2}}\right) |\psi\rangle \right| \\
 &= \left| 1 - e^{\frac{i\beta}{2}} \right|.
 \end{aligned}$$

よって, 任意の  $\epsilon$  に対して,

$$\left| 1 - e^{i\frac{\theta n - \alpha}{2}} \right| < \frac{\epsilon}{3}$$

を満たす整数  $n$  をとってくれば,

$$E(R_{\mathbf{n}}(\alpha), R_{\mathbf{n}}(\theta)^n) = E(R_{\mathbf{n}}(\alpha), R_{\mathbf{n}}(n\theta)) = E(R_{\mathbf{n}}(\alpha), R_{\mathbf{n}}(\alpha + n\theta - \alpha)) = \left| 1 - e^{i\frac{\theta n - \alpha}{2}} \right| < \frac{\epsilon}{3}.$$

このような整数  $n$  がとってこれることを以下に示す. ある任意の角度  $\phi \in [0, 2\pi)$  を精度  $\delta$  で近似することを考える.

$$\theta_k = k\theta \pmod{2\pi}$$

とかき, 以下では角度についての等号は,  $\text{mod } 2\pi$  で考える. 任意の  $\delta$  に対して,  $2\pi/N < \delta$  を満たす  $N$  が存在する. すると,

$$|\theta_{k-j}| = |\theta_k - \theta_j| \leq \frac{2\pi}{N} < \delta$$

を満たす  $k, j = 1, 2, \dots, N$ ,  $k > j$  が存在する. ここで,  $\theta$  が無理数なので,  $\theta_{k-j} = (k-j)\theta \neq 0$  であるから, 任意の異なる  $l, l'$  に対して,

$$|\theta_{l(k-j)} - \theta_{l'(k-j)}| < \delta$$

とできる. したがって, 適当な  $l$  を選んでやれば, 任意の角度  $\phi$  を,  $\theta_{l(k-j)}$  とすることで, 任意の精度  $\delta$  で近似可能. この事実を用いてやれば, 適当な  $n$  を選ぶことで,

$$\frac{\theta n - \alpha}{2}$$

を任意の精度で 0 に近似できる. つまり, 任意の  $\epsilon$  に対して,

$$\left| 1 - e^{i\frac{\theta n - \alpha}{2}} \right| < \frac{\epsilon}{3}$$

を満たす整数  $n$  が存在する.

演習 4.41 まず,

$$\cos \alpha = \frac{3}{\sqrt{10}}, \quad \sin \alpha = -\frac{3}{\sqrt{10}}$$

なる  $\alpha$  を定義すると,

$$\frac{\theta}{2} = \alpha + \frac{\pi}{4}$$

が成り立ち,

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

なので,

$$\frac{1}{4}S - \frac{1}{4}XSX = \frac{1-i}{4}Z$$

や

$$\begin{aligned} \frac{3}{4}S + \frac{1}{4}XSX &= \frac{\sqrt{10}}{4} \begin{pmatrix} \frac{3}{\sqrt{10}} + i\frac{1}{\sqrt{10}} & 0 \\ 0 & \frac{1}{\sqrt{10}} + i\frac{3}{\sqrt{10}} \end{pmatrix} = \frac{\sqrt{10}}{4} \begin{pmatrix} \cos \alpha - i \sin \alpha & 0 \\ 0 & -\sin \alpha + i \cos \alpha \end{pmatrix} \\ &= \frac{\sqrt{10}}{4} \begin{pmatrix} e^{-i\alpha} & 0 \\ 0 & e^{i(\frac{\pi}{2} + \alpha)} \end{pmatrix} = \frac{\sqrt{10}}{4} e^{i\frac{\pi}{4}} \begin{pmatrix} e^{-i(\alpha + \frac{\pi}{4})} & 0 \\ 0 & e^{i(\alpha + \frac{\pi}{4})} \end{pmatrix} = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix} \end{aligned}$$

が成り立つ.

問題の量子回路を  $|0\rangle|0\rangle|\psi\rangle$  に作用させると,

$$\begin{aligned} |0\rangle|0\rangle|\psi\rangle &\rightarrow \frac{1}{2}(|0\rangle|0\rangle|\psi\rangle + |0\rangle|1\rangle|\psi\rangle + |1\rangle|0\rangle|\psi\rangle + |1\rangle|1\rangle|\psi\rangle) \\ &\rightarrow \frac{1}{2}(|0\rangle|0\rangle S|\psi\rangle + |0\rangle|1\rangle S|\psi\rangle + |1\rangle|0\rangle S|\psi\rangle + |1\rangle|1\rangle XSX|\psi\rangle) \\ &\rightarrow \frac{3|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle}{4} S|\psi\rangle + \frac{|0\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle}{4} XSX|\psi\rangle \\ &= |0\rangle|0\rangle \left( \frac{3}{4}S + \frac{1}{4}XSX \right) |\psi\rangle + (|0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle) \left( \frac{1}{4}S - \frac{1}{4}XSX \right) |\psi\rangle \\ &= \frac{\sqrt{10}}{4} e^{i\frac{\pi}{4}} |0\rangle|0\rangle R_Z(\theta) |\psi\rangle + \frac{1-i}{4} (|0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle) Z |\psi\rangle \end{aligned}$$

なので, 第一 q ビットと第二 q ビットが共に 0 になるとき第三 q ビットには  $R_Z(\theta)$  を適用し, そうでなければ  $Z$  を作用させることがわかった. 第一 q ビットと第二 q ビットが共に 0 になる確率は  $10/16 = 5/8$  である.

第一 q ビットと第二 q ビットを測定して, 共に 0 でない場合の終状態は, 規格化定数をのぞいて,

$$(|0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle) Z |\psi\rangle$$

なので, 第三 q ビットに  $Z$  を作用させることで第三 q ビットを  $|\psi\rangle$  というように始状態に戻せる. こうして得た第三 q ビットの  $|\psi\rangle$  を入力として, 再び問題の量子回路に作用させる. ここまでで,

$$\frac{5}{8} + \left(1 - \frac{5}{8}\right) \frac{5}{8}$$

の確率で,  $R_Z(\theta)$  を適用できている. 同じことを繰り返せば,

$$\frac{5}{8} + \left(1 - \frac{5}{8}\right) \frac{5}{8} + \left(1 - \frac{5}{8}\right) \left(1 - \frac{5}{8}\right) \frac{5}{8} + \cdots = 1$$

の確率で,  $R_Z(\theta)$  を適用させることができる.

#### 演習 4.42 (1)

$$e^{i\theta} = \frac{3+4i}{5}$$

なる  $\theta$  を考える.  $\theta$  が  $2\pi$  の有理数倍, つまり  $\theta = 2\pi p/q$  ( $p, q$  は整数) であるとする. 正の整数  $m$  を  $m = |q|$  とすると,

$$e^{im\theta} = e^{2\pi |p|} = 1 \rightarrow (3+4i)^m = 5^m.$$

(2) 帰納法を用いて, 任意の自然数  $m$  に対して,

$$(3+4i)^m = 3+4i \pmod{5}$$

であることが示せる. したがって,

$$(3+4i)^m = 0 \pmod{5}$$

なる  $m$  は存在せず,

$$(3+4i)^m = 5^m \pmod{5}$$

なる  $m$  も存在しない. ゆえに, (1) と合わせて,  $\theta$  は  $2\pi$  の無理数倍.

**演習 4.43** 演習 4.41 の回路  $U$  とする.  $U$  は  $S, H, \text{CNOT}, \text{Toffoli}$  から成る. 演習 4.41 では,  $Z = S^2$  と  $U$ , つまり  $S, H, \text{CNOT}, \text{Toffoli}$  で  $R_z(\theta)$  を作れることを述べた. (4.76) より,  $\theta$  が  $2\pi$  の無理数倍なので, 任意の  $\epsilon > 0$ ,  $\alpha \in [0, 2\pi)$  に対して,

$$E(R_z(\alpha), R_z(\theta)^n) < \epsilon$$

成る  $n$  が存在する. さらに,  $HR_z(\theta)H = R_x(\theta)$  なので, 任意の  $\epsilon > 0$ ,  $\alpha \in [0, 2\pi)$  に対して,

$$E(R_x(\alpha), R_x(\theta)^m) < \epsilon$$

成る  $m$  も存在する. ここで, 演習 4.10 より, 任意の単一 q ビットに作用するユニタリゲート  $V$  は,

$$V = R_z(\beta)R_x(\gamma)R_z(\delta)$$

とかけるので, 任意の  $\epsilon > 0$  に対して,

$$E(V, R_z(\theta)^{n_1}R_x(\theta)^{m_1}R_z(\theta)^{n_2}) \leq E(R_z(\beta), R_z(\theta)^{n_1}) + E(R_x(\gamma), R_x(\theta)^{m_1}) + E(R_z(\delta), R_z(\theta)^{n_2}) < \epsilon$$

を満たす自然数  $n_1, n_2, m_1$  が存在する. ここで (4.63) を用いた. 以上より, 任意の単一 q ビットに作用するユニタリゲート  $V$  が任意の精度  $\epsilon$  で,  $R_z(\theta), R_x(\theta)$  だけ, つまり,  $S, H, \text{CNOT}, \text{Toffoli}$  だけで近似できることが示された.

#### 演習 4.44

#### 演習 4.45

演習 4.46  $2^n \times 2^n$  の複素行列を作るのに必要な独立な実数の個数は  $2 \times 4^n$ . 演習 4.24 より,  $\rho$  は Hermite;

$$\rho = \rho^\dagger$$

で, この式を  $\rho$  の各成分と  $\rho^\dagger$  の各成分が等しいという条件式と読み換えると, その条件式の本数は  $4^n$ . このことと,  $\text{tr}\rho = 1$  なことから  $\rho$  を作るのに必要な独立な実数の個数は,

$$2 \times 4^n - 4^n - 1 = 4^n - 1.$$

演習 4.47 グラフを書けば,

$$\sum_{n=0}^{\infty} \sum_{k=0}^n f(k, n-k) = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} f(i, j)$$

であることがわかる. これを用いて,  $[A, B] = 0$  のとき,

$$e^{A+B} = \sum_{n=1}^{\infty} \frac{1}{n!} (A+B)^n = \sum_{n=0}^{\infty} \sum_{k=0}^n \frac{1}{k!(n-k)!} A^k B^{n-k} = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \frac{1}{i!j!} A^i B^j = e^A e^B.$$

これを繰り返し用いて問題の等式が示せる.

演習 4.48

$$L = O\left(\binom{n}{c}\right) = O(n^c)$$

演習 4.49

$$\begin{aligned} e^{(A+B)\Delta t} &= 1 + (A+B)\Delta t + \frac{AA+AB+BA+BB}{2}\Delta t^2 + O(\Delta t^3) \\ e^{A\Delta t} e^{B\Delta t} e^{-\frac{1}{2}[A,B]\Delta t^2} &= \left(1 + A\Delta t + \frac{A^2\Delta t^2}{2}\right) \left(1 + B\Delta t + \frac{B^2\Delta t^2}{2}\right) \left(1 - \frac{1}{2}[A,B]\Delta t^2\right) + O(\Delta t^3) \\ &= 1 + (A+B)\Delta t + \frac{AA+AB+BA+BB}{2}\Delta t^2 + O(\Delta t^3) \\ e^{\frac{A\Delta t}{2}} e^{B\Delta t} e^{\frac{A\Delta t}{2}} &= \left(1 + \frac{A\Delta t}{2} + \frac{A^2\Delta t^2}{4}\right) \left(1 + B\Delta t + \frac{B^2\Delta t^2}{2}\right) \left(1 + \frac{A\Delta t}{2} + \frac{A^2\Delta t^2}{4}\right) + O(\Delta t^3) \\ &= 1 + (A+B)\Delta t + \frac{AA+AB+BA+BB}{2}\Delta t^2 + O(\Delta t^3) \end{aligned}$$

なので,

$$e^{(A+B)\Delta t} = e^{A\Delta t} e^{B\Delta t} e^{-\frac{1}{2}[A,B]\Delta t^2} + O(\Delta t^3) = e^{\frac{A\Delta t}{2}} e^{B\Delta t} e^{\frac{A\Delta t}{2}} + O(\Delta t^3)$$

演習 4.50 (1) 式 (4.104) を繰り返し用いる.

(2) (1) と式 (4.63) より,

$$E(U_{\Delta t}^m, e^{-2miH\Delta t}) \leq mE(U_{\Delta t}, e^{-2iH\Delta t}) = m \max_{|\psi\rangle} \|U_{\Delta t} - e^{-2iH\Delta t}|\psi\rangle\| = mO(\Delta t^3) \max_{|\psi\rangle} \|O|\psi\rangle\| \leq m\alpha\Delta t^3.$$

ここで,  $O$  はあるオペレータ.

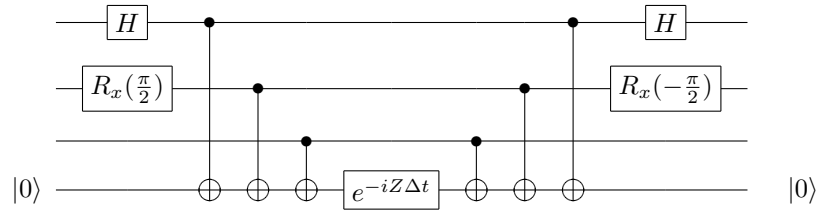
演習 4.51

$$\begin{aligned} X &= HZH \\ e^{-i\theta X} Z e^{i\theta X} &= \cos\theta Z - \sin\theta Y \rightarrow Y = e^{i\frac{\pi}{2}X} Z e^{-i\frac{\pi}{2}X} \end{aligned}$$

であるので, Hamiltonian は,

$$H = \left( H \otimes R_x \left( -\frac{\pi}{2} \right) \otimes I \right) (Z \otimes Z \otimes Z) \left( H \otimes R_x \left( \frac{\pi}{2} \right) \otimes I \right)$$

と書き換えられる. これをシミュレートする回路は以下のようなになる.



## 第 5 章

# 量子 Fourier 変換とその応用

### 演習 5.1

$$\omega = e^{i\frac{2\pi}{N}}$$

とする. 量子 Fourier 変換オペレータ  $U$  の行列表示  $U_{ij}$  は, 行列の index が 0 オリジンだとして,

$$U_{ij} = \frac{1}{\sqrt{N}} \omega^{ij}$$

なので,

$$\sum_j U_{ij} U_{jk}^\dagger = \frac{1}{N} \sum_j \omega^{ij} \bar{\omega}^{jk} = \frac{1}{N} \sum_j \omega^{ij} \omega^{-jk} = \frac{1}{N} \sum_j \omega^{j(i-k)} = \delta_{ik}$$

と  $U$  はユニタリ.

### 演習 5.2

$$\sum_{k=0}^{N-1} \frac{1}{\sqrt{N}} |k\rangle$$

演習 5.3  $N = 2^n$  とする. 式 (5.1)

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega^{jk}$$

を実装して, 離散 Fourier 変換に必要な計算量は, サイズ  $N \times N$  の行列とサイズ  $N$  のベクトルの積を求める計算量  $\Theta(N^2) = O(4^n)$  に等しい.

一方, 式 (5.14)

$$\begin{aligned} \text{QFT } |j_1 j_2 \dots j_n\rangle &= \text{QFT } |j_2 j_3 \dots j_n\rangle \frac{(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle)}{\sqrt{2}} \\ &= \text{QFT } |j_3 j_4 \dots j_n\rangle \frac{(|0\rangle + e^{2\pi i 0 \cdot j_2 j_3 \dots j_n} |1\rangle)}{\sqrt{2}} \frac{(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle)}{\sqrt{2}} \\ &\vdots \\ &= \text{QFT } |j_n\rangle \frac{(|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle)}{\sqrt{2}} \dots \frac{(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle)}{\sqrt{2}} \\ &= \frac{(|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle)}{\sqrt{2}} \frac{(|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle)}{\sqrt{2}} \dots \frac{(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle)}{\sqrt{2}} \end{aligned}$$

をみると,  $|j_1 j_2 \dots j_n\rangle$  の Fourier 変換を知りたいければ  $|j_2 j_3 \dots j_n\rangle$  の Fourier 変換を求めれば良い.  $|j_2 j_3 \dots j_n\rangle$  の Fourier 変換を知りたいければ  $|j_3 j_4 \dots j_n\rangle$  の Fourier 変換を求めれば良い. このことを再帰的に行えば, ある特定の  $|j\rangle = |j_1 j_2 \dots j_n\rangle$  の Fourier 変換を求めるのに必要な計算量は  $\Theta(\log N) = \Theta(n)$  であることがわかる. よって, 全ての  $j = j_1 j_2 \dots j_n$  に対して, Fourier 変換を求めるのに必要な計算量は  $\Theta(N \log N) = O(2^n n)$ .

演習 5.4 系 4.2 で,

$$\alpha = \frac{\pi}{2^k}, \beta = \frac{\pi}{2^{k-1}}, \gamma = \delta = 0$$

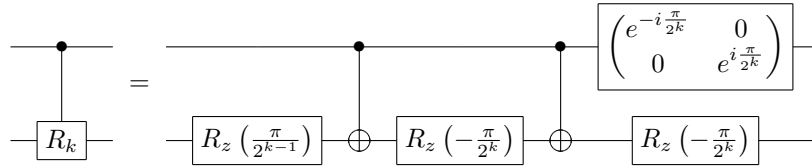
として,

$$\begin{aligned} R_k &= e^{i\frac{\pi}{2^k}} \begin{pmatrix} e^{-i\frac{\pi}{2^k}} & 0 \\ 0 & e^{i\frac{\pi}{2^k}} \end{pmatrix} \\ &= e^{i\frac{\pi}{2^k}} R_z \left( \frac{\pi}{2^{k-1}} \right) \\ &= e^{i\frac{\pi}{2^k}} R_z \left( \frac{\pi}{2^{k-1}} \right) X R_z \left( -\frac{\pi}{2^k} \right) X R_z \left( -\frac{\pi}{2^k} \right) \end{aligned}$$

となり,

$$R_z \left( \frac{\pi}{2^{k-1}} \right) R_z \left( -\frac{\pi}{2^k} \right) R_z \left( -\frac{\pi}{2^k} \right) = I$$

である. よって, 制御  $R_k$  を単一 q ビットと CNOT で分解すると,



となる.

演習 5.5  $\mathbf{x} = (x_0, x_1, \dots, x_{N-1})$  Fourier 逆変換  $\mathbf{y} = (y_0, y_1, \dots, y_{N-1})$  を,

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \bar{\omega}^{jk} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega^{-jk}$$

で定義する. すると, 量子 Fourier 逆変換は,

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{-jk} |k\rangle$$

となる. 量子 Fourier 逆変換と量子 Fourier 変換

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{jk} |k\rangle$$

を比べると,  $\omega$  の指数部分の符号だけが異なる. よって, 量子 Fourier 変換を行う量子回路で用いられている  $R_k$  を全て  $\bar{R}_k$ ;

$$\bar{R}_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\frac{2\pi i}{2^k}} \end{pmatrix}$$

に置き換えれば良い.

演習 5.6 量子 Fourier 変換回路が  $O(n^2)$  個の  $R_k$  と  $O(n)$  個の  $H$  からなることと式 (4.63) より,

$$E(U, V) \leq O(n^2)p(n) = O(n^2p(n)) \rightarrow E(U, V) = O(n^2p(n))$$

なので, 量子 Fourier 変換回路の各ゲートが多項式精度で動作可能なら, 出力状態も多項式精度が保証される.

演習 5.7

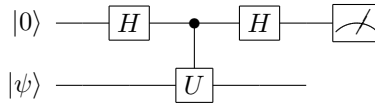
$$|j\rangle U^j |u\rangle = e^{2\pi i j \phi} |j\rangle |u\rangle = e^{2\pi i (2^{t-1}j_{t-1} + \dots + 2^0 j_0) \phi} |j_0 j_1 \dots j_{t-1}\rangle |u\rangle$$

演習 5.8 第 2 レジスタでの測定結果が  $u$  であるときに, 第 1 レジスタで

$$t = n + \left\lceil \log \left( 2 + \frac{1}{2\epsilon} \right) \right\rceil$$

個の  $q$  ビットを用いれば, 確率  $1 - \epsilon$  で  $\phi_u$  の推定値を正しく得られる. 第 2 レジスタでの測定結果が  $u$  である確率は  $|c_u|^2$  なので, 第 1 レジスタで  $t$  個の  $q$  ビットを用いれば, 確率  $|c_u|^2(1 - \epsilon)$  で  $\phi_u$  の推定値を正しく得られる.

演習 5.9 本問の場合,  $\phi$  は 0 または  $1/2$  なので第 1 レジスタは 1 つの  $q$  ビットで十分である. すると, 位相推定の量子回路は演習 4.34 と全く同じ回路になる.



演習 5.10

$$5^2 = 4, 5^3 = 20, 5^4 = 16, 5^5 = 17, 5^6 = 1 \pmod{21}$$

演習 5.11 ここで  $\equiv$  は,  $\text{mod } N$  における等号.

位数  $r$  が存在するとき, 任意の正の整数  $n$  に対して  $x^n \not\equiv 0$ . なぜなら,  $x^r \equiv 1$  なる  $r$  が存在すると,

- $n_1 < r$  を満たす任意の正の整数  $n_1$  に対して,  $x^{n_1} \not\equiv 0$ . なぜなら,  $x_1^n \equiv 0$  なる  $n_1$  が存在すると,  $n_1 < n_2$  を満たす任意の正の整数  $n_2$  に対して,  $x^{n_2} \equiv 0$  となるから.
- $n_1 > r$  を満たす任意の正の整数  $n_1$  に対して,  $x^{n_1} \equiv x^{n_1 \% r} \not\equiv 0$  ( $n_1 \% r$  は  $n_1$  を  $r$  で割ったあまり).

となるから.

したがって, 位数  $r$  が存在するとき, 任意の正の整数  $n$  に対して  $x^n$  として取りうる値は  $1, 2, \dots, N-1$ . よって,  $1 \leq n_1 < n_2 \leq N$  を満たす  $n_1, n_2$  が存在して,  $x^{n_1} \equiv x^{n_2}$ . よって,  $n_1 + r = n_2$  なる  $r$  が存在する. ここで,  $1 \leq n_1 < n_2 \leq N$  なので  $1 \leq r \leq N-1$  となり題意が示された.

演習 5.12  $x$  と  $N$  が互いに素なので, 定理 D.9 より  $x$  の逆元が存在し,

$$xy_1 \equiv xy_2 \Leftrightarrow y_1 \equiv y_2.$$

よって,  $0 \leq y_1, y_2 \leq N-1$  に対して,

$$\langle y_1 | UU^\dagger | y_2 \rangle = \langle xy_1 \text{ mod } N | xy_2 \text{ mod } N \rangle = \langle y_1 \text{ mod } N | y_2 \text{ mod } N \rangle = \langle y_1 | y_2 \rangle$$

$U$  は,  $N \leq y_1, y_2 \leq 2^L - 1$  に対しては恒等演算子として作用するよう定義されているので,

$$\langle y_1 | UU^\dagger | y_2 \rangle = \langle y_1 | II^\dagger | y_2 \rangle = \langle y_1 | y_2 \rangle.$$

以上より,  $U$  はユニタリ.



## 演習 5.13

$$\sum_{s=0}^{r-1} e^{-2\pi i s k / r} = \begin{cases} r & (k=0) \\ \frac{1-e^{-2\pi i k}}{1-e^{-2\pi i k / r}} = 0 & (k=1, 2, \dots, r-1) \end{cases}$$

なので,

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = \frac{1}{r} \sum_{s=0}^{r-1} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} |x^k \bmod N\rangle \frac{1}{r} \sum_{k=0}^{r-1} r \delta_{k0} |x^k \bmod N\rangle = |1\rangle.$$

## 演習 5.14

$$V |j\rangle |k\rangle = |j\rangle |k + x^j \bmod N\rangle$$

を計算する  $V$  が存在すれば, 第 2 レジスタを  $|0\rangle$  で初期化しても Fourier 逆変換の前の状態  $|\psi\rangle$  は,

$$|\psi\rangle = \sum_j V |j\rangle |0\rangle = \sum_j |j\rangle |x^j \bmod N\rangle$$

とできる.

コラム 5.2 にもあるように, 筆算の要領で, 各  $j = 1, 2, \dots, t-1$  に対して,  $|x^{2^j}\rangle$  を  $O(L^2)$  計算できる. したがって, 任意の  $j$  に対して,

$$|x^j \bmod N\rangle = |x^{j_t 2^{t-1}} x^{j_{t-1} 2^{t-2}} \dots x^{j_1 2^0} \bmod N\rangle$$

を  $O(L^3)$  で計算できる. また,  $|k\rangle$  と  $|x^j\rangle$  がわかっていれば,  $|k + x^j \bmod N\rangle$  も筆算の要領で  $O(L)$  で計算できる. 総じて,  $|k + x^j \bmod N\rangle$  は  $O(L^3)$  で計算可能. つまり,  $V$  を  $O(L^3)$  個のゲートで実現可能.

演習 5.15 付録 D.2 にあるように,  $\gcd(x, y)$  は  $O(L^3)$  で計算できる. 掛け算や割り算は, それぞれ筆算の要領で  $O(L^2)$  で計算できる. 以上より,  $xy/\gcd(x, y)$  は  $O(L^3)$  で計算できる.

演習 5.16  $x \geq 2$  に対して,

$$\frac{3}{2}x^2 - x(x+1) = \frac{x^2}{2} - x \geq 0$$

なので,

$$\int_x^{x+1} \frac{dy}{y^2} = \frac{1}{x(x+1)} \geq \frac{2}{3x^2}.$$

よって,

$$\frac{3}{4} = \frac{3}{2} \int_2^\infty \frac{dy}{y^2} \geq \sum_{n=2}^\infty \frac{1}{n^2} \geq \sum_q \frac{1}{q^2}.$$

## 演習 5.17

演習 5.18 91 に対する 4 の位数は 6.  $4^{6/2} \not\equiv -1 \pmod{91}$  なので,  $\gcd(4^3 - 1, 91) = 7$  となり, アルゴリズムは成功する.

演習 5.19 奇の合成数は, 小さい順に  $9, 15, 21, \dots$  よって, ある数のべきになっていない最小の合成数は 15.

演習 5.20  $N = nr$  とかく.

$$\begin{aligned}
 \hat{f}(l) &= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2\pi i l x / N} f(x) \\
 &= \frac{1}{\sqrt{nr}} \sum_{k=0}^{n-1} \sum_{x=0}^{r-1} e^{-2\pi i l (x+kr) / nr} f(x+kr) \\
 &= \frac{1}{\sqrt{nr}} \sum_{k=0}^{n-1} e^{-2\pi i l k / n} \sum_{x=0}^{r-1} e^{-2\pi i l x / nr} f(x) \\
 &= \begin{cases} \sqrt{\frac{n}{r}} \sum_{x=0}^{r-1} e^{-2\pi i l x / nr} f(x) & (l = n\mathbb{Z}) \\ 0 & (\text{otherwise}) \end{cases}
 \end{aligned}$$

演習 5.21 (1)

$$\begin{aligned}
 U_y |\hat{f}(l)\rangle &= \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i l x / r} U_y |f(x)\rangle \\
 &= e^{2\pi i l y / r} \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i l (x+y) / r} |f(x+y)\rangle \\
 &= e^{2\pi i l y / r} |\hat{f}(l)\rangle
 \end{aligned}$$

(2)

$$|f(x_0)\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{2\pi i l x_0 / r} |\hat{f}(l)\rangle$$

は  $U_y$  の固有状態を等しい振幅で重ね合わせた状態. したがって,  $|0\rangle |f(x_0)\rangle$  を初期状態として, 位相発見のアルゴリズム (日本語版の教科書 p84) を用いれば,  $f$  の周期  $r$  を得る.

## 第 6 章

# 量子探索アルゴリズム

演習 6.1

$$(2|0\rangle\langle 0| - I)(2|0\rangle\langle 0| - I)^\dagger = I.$$

演習 6.2

$$\begin{aligned} (2|\psi\rangle\langle\psi| - I) \sum_k \alpha_k |k\rangle &= \frac{2}{N} \sum_x \sum_y \sum_k \alpha_k |x\rangle \langle y|k\rangle - \sum_k \alpha_k |k\rangle \\ &= \frac{2}{N} \sum_x \sum_y \sum_k \alpha_k |x\rangle \delta_{yk} - \sum_k \alpha_k |k\rangle \\ &= \frac{2}{N} \sum_x \sum_k \alpha_k |x\rangle - \sum_k \alpha_k |k\rangle \\ &= 2\langle\alpha\rangle \sum_x |x\rangle - \sum_k \alpha_k |k\rangle \\ &= \sum_k [-\alpha_k + 2\langle\alpha\rangle] |k\rangle. \end{aligned}$$

演習 6.3  $|\alpha\rangle, |\beta\rangle$  基底で,

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2) \end{pmatrix} = \begin{pmatrix} \cos(3\theta/2) \\ \sin(3\theta/2) \end{pmatrix}$$

であることを

$$G\left(\cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle\right) = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle.$$

を見比べれば良い.

演習 6.4 P114 の手続きと全く同様.

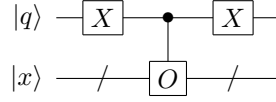
演習 6.5 考えたい探索問題  $f(x)$ , 拡張した探索問題  $f'(x, q)$  とかくと,

$$f'(x, q) = \begin{cases} f(x) & (q = 0) \\ 0 & (q = 1) \end{cases}$$

なので, 拡張したオラクル  $O'$ ;

$$|q\rangle|x\rangle \xrightarrow{O'} (-1)^{f'(x,q)}|q\rangle|x\rangle = \begin{cases} (-1)^{f(x)}|q\rangle|x\rangle & (q = 0) \\ |q\rangle|x\rangle & (q = 1) \end{cases}$$

を実現する量子回路は

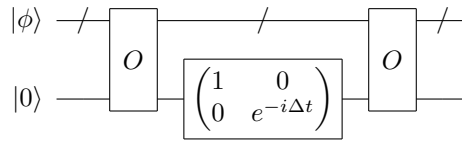


となる.

演習 6.6 点線の箱への Input を  $|a\rangle|b\rangle$  として, 点線の箱の Input への作用は

$$\begin{aligned}
 |a\rangle|b\rangle &\rightarrow |a\rangle X H X^{1-a} H X |b\rangle = \begin{cases} |a\rangle X H X H X |b\rangle & (a=0) \\ |A\rangle X H H X |b\rangle & (a=1) \end{cases} \\
 &= \begin{cases} -|a\rangle Z |b\rangle & (a=0) \\ |a\rangle |b\rangle & (a=1) \end{cases} \\
 &= \begin{cases} -|a\rangle Z |b\rangle & (a=0, b=0) \\ |a\rangle Z |b\rangle & (a=0, b=1) \\ |a\rangle |b\rangle & (a=1) \end{cases} \\
 &= I - 2|00\rangle\langle 00|
 \end{aligned}$$

演習 6.7 図 6.4 の



という回路について考える. ここで, オラクル  $O$  は,

$$|\phi\rangle|0\rangle \xrightarrow{O} \begin{cases} |\phi\rangle|1\rangle & (x=\phi) \\ |\phi\rangle|0\rangle & (\text{otherwise}) \end{cases}$$

と作用する. すると, 上記の回路の作用は,

$$|\phi\rangle|0\rangle \xrightarrow{O} \begin{cases} |\phi\rangle|1\rangle & (x=\phi) \\ |\phi\rangle|0\rangle & (\text{otherwise}) \end{cases} \rightarrow \begin{cases} e^{-i\Delta t} |\phi\rangle|1\rangle & (x=\phi) \\ |\phi\rangle|0\rangle & (\text{otherwise}) \end{cases} \xrightarrow{O} \begin{cases} e^{-i\Delta t} |\phi\rangle|0\rangle & (x=\phi) \\ |\phi\rangle|0\rangle & (\text{otherwise}) \end{cases}$$

第 1q ビットに注目すると, この回路の作用は  $\exp[-i|x\rangle\langle x|\Delta t]$ . 図 6.5 についても同様.

演習 6.8 必要なステップ数は,

$$\frac{t}{\Delta t} = O\left(\frac{\sqrt{N}}{\Delta t}\right).$$

全ステップ後の累積誤差は,

$$O\left(\frac{\sqrt{N}}{\Delta t} \Delta t^r\right).$$

累積誤差が  $O(1)$  になるには,

$$1 = O\left(\frac{\sqrt{N}}{\Delta t} \Delta t^r\right) \rightarrow O(\Delta t) = O\left(N^{-\frac{1}{2(r-1)}}\right).$$

よって, 高い成功率を得るには,

$$\frac{t}{\Delta t} = O\left(\frac{\sqrt{N}}{N^{-\frac{1}{2(r-1)}}}\right) = O\left(N^{\frac{r}{2(r-1)}}\right).$$

演習 6.9 演習 4.15 そのまま.

演習 6.10

$$\frac{t}{\Delta t} = \frac{\pi\sqrt{N}}{2\Delta t}$$

が  $O(\sqrt{N})$  かつ整数になるような  $\Delta t$  を選べば良い.

演習 6.11

$$H = \sum_{x=1}^m |x\rangle \langle x| + |\psi\rangle \langle \psi|$$

演習 6.12 (1)  $|\psi\rangle, |x\rangle$  で張られる空間の正規直交基底  $|x\rangle, |y\rangle$  として,  $|\psi\rangle = \alpha|x\rangle + \beta|y\rangle$  とかく.  $|x\rangle, |y\rangle$  基底で考える. Hamiltonian は,

$$H = |x\rangle \langle \psi| + |\psi\rangle \langle x| = \alpha I + (\beta X + \alpha Z)$$

となるので, 時間発展 op. は,

$$\begin{aligned} e^{-iHt} &= e^{-i\alpha t} e^{-i(\beta X + \alpha Z)t} \\ &= e^{-i\alpha t} [I \cos t - i(\beta X + \alpha Z) \sin t]. \end{aligned}$$

よって,

$$e^{-iHt} |\psi\rangle = e^{-i\alpha t} [\cos t |\psi\rangle - i \sin t |x\rangle]$$

となることから,  $t = 0$  で  $|\psi\rangle$  だった系は  $t = \pi$  で  $|x\rangle$  に時間発展する.

(2)

演習 6.13  $M$  の推定値

$$S = \frac{N}{k} \sum_{j=1}^k X_j$$

に対して,

$$\begin{aligned} E[S] &= \frac{N}{k} \sum_{j=1}^k E[X_j] = \frac{N}{k} \sum_{j=1}^k \frac{M}{N} = M \\ E[S^2] &= \frac{N^2}{k^2} \sum_{j,l=1}^k E[X_j X_l] = \frac{N^2}{k^2} \left( \sum_{j=1}^k E[X_j^2] + \sum_{j \neq l} E[X_j] E[X_l] \right) = \frac{N^2}{k^2} \left( k \frac{M}{N} + k(k-1) \frac{M}{N} \frac{M}{N} \right) = M^2 + \frac{M(N-M)}{k} \end{aligned}$$

なので,  $S$  の標準偏差は,

$$\Delta S = \sqrt{E[S^2] - E[S]^2} = \sqrt{\frac{M(N-M)}{k}}.$$

精度  $\sqrt{M}$  以内で  $M$  を正確に推定する確率を  $p$  にするには,  $p$  に応じて  $N$  に依らない定数  $\alpha$  をとってきて,

$$\alpha \Delta S < \sqrt{M} \rightarrow k \geq \alpha^2 (N - M)$$

なる  $k$  を選べば良い. よって,  $k = \Omega(N)$  が示された.

## 演習 6.14

演習 6.15 Cauchy-Schwarz の不等式より,

$$\left( \sum_x |\langle \psi | x \rangle| \right)^2 \leq \left( \sum_x |\langle \psi | x \rangle|^2 \right) \left( \sum_x 1 \right) = N$$

であることを用いて,

$$\begin{aligned} \sum_x \|\psi - x\|^2 &= \sum_x \|\psi\|^2 + \|x\|^2 - 2\Re \langle \psi | x \rangle \\ &= 2N - 2 \sum_x \Re \langle \psi | x \rangle \\ &\geq 2N - 2 \sum_x |\langle \psi | x \rangle| \\ &\geq 2N - 2\sqrt{N}. \end{aligned}$$

演習 6.16 教科書 P133-P134 の議論に手を加える.

まず,

$$D_k = \sum_x \|\psi_k^x - \psi_k\| \leq 4k^2$$

であることは教科書で示した通り.

$x$  の可能な値に対して一様な平均をとったときの, 誤り確率が  $1/2$  以下になる;

$$\frac{1}{N} \sum_x |\langle x | \psi_k^x \rangle|^2 \leq \frac{1}{2}$$

と仮定する. まず,  $|x\rangle$  の位相をうまく取り替えることで,  $\langle \psi_k^x | x \rangle = |\langle \psi_k^x | x \rangle|$  とできることを用いて,

$$\begin{aligned} E_k &= \sum_x \|\psi_k^x - x\|^2 \\ &= 2N - 2 \sum_x |\langle \psi_k^x | x \rangle| \\ &\leq 2N - 2 \sqrt{\sum_x |\langle \psi_k^x | x \rangle|^2} \leq 2N - \sqrt{2N}. \end{aligned}$$

最後の不等号で, 仮定を用いた. ここで, 演習 6.15 の結果より,

$$F_k = \sum_x \|\psi - x\|^2 \geq 2N - 2\sqrt{N}.$$

であるから, (6.51) 式は,  $N \neq 2$  であれば,

$$\begin{aligned} D_k &\geq \left( \sqrt{E_k} - \sqrt{F_k} \right)^2 = \left( \sqrt{2N - \sqrt{2N}} - \sqrt{2N - 2\sqrt{N}} \right)^2 \\ &= N \left( \sqrt{2 - \sqrt{\frac{2}{N}}} - \sqrt{2 - \frac{2}{\sqrt{N}}} \right)^2 \geq cN \end{aligned}$$

となる正数  $c$  が存在する.

以上より,

$$cN \leq D_k \leq 4k^2 \rightarrow k \geq \sqrt{\frac{cN}{4}}.$$

つまり、探索サイズ  $N (\neq 2)$  の問題にを解くにあたり、探索空間の元  $x$  に対して一様な平均をとったときの誤り確率が  $1/2$  以下になることを保証するならば、Oracle の呼び出し回数  $k$  は  $\Omega(N)$ 。

演習 6.17 <https://arxiv.org/abs/quant-ph/9605034>

演習 6.18 最小次数  $l$  の Boole 関数  $F(X_1, \dots, X_N)$  の一般形は、 $X_k^2 = X_k$  なことに注意して、

$$F(X_1, \dots, X_N) = \sum_{i=0}^l \sum_{j=1}^{NC_i} \prod_{k=1}^i \alpha_{ij} X_{\beta_{ijk}}$$

とかける。ここで、 $\alpha_j$  は  $F(X_1, \dots, X_N)$  を決めるための定数で、 $\beta_{ijk}$  は、1 から  $n$  までの数から  $i$  個選ぶことで得られる集合を、全てかき集めた集合族の  $j$  番目の要素の小さい方から  $k$  番目の要素である。  $F(X_1, \dots, X_N)$  を一意に定めるために  $2^N$  本の条件式を用いて、 $\sum_{i=0}^l NC_i (\leq 2^N)$  個の  $\alpha_{ij}$  を決める。条件式の数の方が、決めるべき定数  $\alpha_{ij}$  の総数より多いので、 $\alpha_{ij}$  は与えられた  $F(X_1, \dots, X_N)$  に対して一意に決まる。

演習 6.19

$$P(X) = 1 - (1 - X_0) \dots (1 - X_{N-1})$$

は、 $X_0, \dots, X_{N-1}$  の全てが 0 の時のみ 0 になる。つまり、 $P(X)$  は OR。

## 第 7 章

# 量子コンピュータ：物理的実現方法

演習 7.1

$$a^\dagger a = \frac{1}{2m\hbar\omega} (m^2\omega^2 x^2 + p^2 + im\omega [x, p]) = \frac{1}{\hbar\omega} \left( \frac{p^2}{2m} + \frac{m\omega^2 x^2}{2} \right) - \frac{1}{2}.$$

演習 7.2

$$[a, a^\dagger] = \frac{-2im\omega [x, p]}{2m\hbar\omega} = 1.$$

演習 7.3

$$[H, a] = [\hbar\omega a^\dagger a, a] = \hbar\omega [a^\dagger, a]a = -\hbar\omega a$$

であるので,

$$H|\psi\rangle = E|\psi\rangle$$

なる  $|\psi\rangle$  に対して,

$$Ea|\psi\rangle = aH|\psi\rangle = (Ha + \hbar\omega a)|\psi\rangle \rightarrow Ha|\psi\rangle = (E - \hbar\omega)a|\psi\rangle$$

を得る. これを帰納的に繰り返して,

$$Ha^n|\psi\rangle = (E - n\hbar\omega)|\psi\rangle.$$

演習 7.4 式 (7.11);

$$a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$$

より,

$$(a^\dagger)^n|0\rangle = \sqrt{n!}|n\rangle.$$

演習 7.5 式 (7.10), 正規化条件,  $[a, a^\dagger] = 1$  より,

$$\begin{aligned} |a^\dagger|n\rangle|^2 &= \langle n|aa^\dagger|n\rangle = \langle n|a^\dagger a + 1|n\rangle = n+1 \\ |a|n\rangle|^2 &= \langle n|a^\dagger a|n\rangle = n \end{aligned}$$

演習 7.6

$$a|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} a|n\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=1}^{\infty} \frac{\alpha^n}{\sqrt{(n-1)!}} |n-1\rangle = \alpha e^{-\frac{|\alpha|^2}{2}} \sum_{n=1}^{\infty} \frac{\alpha^{n-1}}{\sqrt{(n-1)!}} |n-1\rangle = \alpha|\alpha\rangle$$



演習 7.7 明らか.

演習 7.8 Kerr 物質を用いた位相シフタ  $P$  は, 系の光子の数に比例した分だけ位相をズラすオペレータ;

$$P|n\rangle = e^{i\Delta n}|n\rangle$$

なので,

$$P|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} e^{i\Delta n} |n\rangle = e^{-\frac{|\alpha e^{i\Delta}|^2}{2}} \sum_{n=0}^{\infty} \frac{(\alpha e^{i\Delta})^n}{\sqrt{n!}} |n\rangle = |\alpha e^{i\Delta}\rangle.$$

演習 7.9  $\theta = \pi/4$  のビームスプリッタ  $B$  を考えると,

$$\begin{aligned} e^{i\pi} B|01\rangle &= -\frac{|01\rangle + |10\rangle}{\sqrt{2}} \\ B|10\rangle &= \frac{|11\rangle - |01\rangle}{\sqrt{2}} \end{aligned}$$

となり, 全体の位相をのぞいて Hadamard 変換になっている.

演習 7.10 行列表示で,

$$\begin{pmatrix} \cos \beta & \sin \beta \\ -\sin \beta & \cos \beta \end{pmatrix} \begin{pmatrix} e^{i\phi} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} = e^{\frac{i\phi}{2}} R_y(-2\beta) R_z(-\phi) R_y(2\alpha)$$

演習 7.11

$$\begin{aligned} B|20\rangle &= \frac{1}{\sqrt{2}} B b^\dagger b^\dagger |00\rangle \\ &= \frac{1}{\sqrt{2}} B b^\dagger B^\dagger B b^\dagger B^\dagger B |00\rangle \\ &= \frac{1}{\sqrt{2}} \frac{-a^\dagger + b^\dagger}{\sqrt{2}} \frac{-a^\dagger + b^\dagger}{\sqrt{2}} |00\rangle \\ &= \frac{a^\dagger a^\dagger - b^\dagger a^\dagger - a^\dagger b^\dagger + b^\dagger b^\dagger}{2\sqrt{2}} |00\rangle \\ &= \frac{1}{2} |02\rangle - \frac{1}{\sqrt{2}} |11\rangle + \frac{1}{2} |20\rangle. \end{aligned}$$

演習 7.12  $b^\dagger \otimes I$  や  $I \otimes a^\dagger$  を単に  $b^\dagger$  や  $a^\dagger$  とかく.

$$\begin{aligned} B|\alpha\rangle \otimes |\beta\rangle &= B e^{-(|\alpha|^2 + |\beta|^2)} \sum_{n,m} \frac{\alpha^n \beta^m}{\sqrt{n!m!}} |n\rangle \otimes |m\rangle \\ &= B e^{-(|\alpha|^2 + |\beta|^2)} \sum_{n,m} \frac{\alpha^n \beta^m}{n!m!} (b^\dagger)^n (a^\dagger)^m |0\rangle \otimes |0\rangle \\ &= e^{-(|\alpha|^2 + |\beta|^2)} \sum_{n,m} \frac{\alpha^n \beta^m}{n!m!} (B b^\dagger B^\dagger)^n (B a^\dagger B^\dagger)^m B |0\rangle \otimes |0\rangle \\ &= e^{-(|\alpha|^2 + |\beta|^2)} \sum_{n,m} \frac{\alpha^n \beta^m}{n!m!} (-a^\dagger \sin \theta + b^\dagger \cos \theta)^n (a^\dagger \cos \theta + b^\dagger \sin \theta)^m |0\rangle \otimes |0\rangle \\ &= e^{-(|\alpha|^2 + |\beta|^2)} \sum_n \frac{\alpha^n}{n!} (-a^\dagger \sin \theta + b^\dagger \cos \theta)^n \sum_m \frac{\beta^m}{m!} (a^\dagger \cos \theta + b^\dagger \sin \theta)^m |0\rangle \otimes |0\rangle \\ &= e^{-(|\alpha|^2 + |\beta|^2)} \exp [(-a^\dagger \sin \theta + b^\dagger \cos \theta) \alpha + (a^\dagger \cos \theta + b^\dagger \sin \theta) \beta] |0\rangle \otimes |0\rangle \\ &= e^{-(|\beta \sin \theta + \alpha \cos \theta|^2 + |\beta \cos \theta - \alpha \sin \theta|^2)} \exp [(\beta \sin \theta + \alpha \cos \theta) b^\dagger + (\beta \cos \theta - \alpha \sin \theta) a^\dagger] |0\rangle \otimes |0\rangle \\ &= |\beta \sin \theta + \alpha \cos \theta\rangle \otimes |\beta \cos \theta - \alpha \sin \theta\rangle. \end{aligned}$$

## 演習 7.13

演習 7.14  $b^\dagger \otimes I$  や  $I \otimes a^\dagger$  を単に  $b^\dagger$  や  $a^\dagger$  とかく.

$$\begin{aligned}
K |\alpha\rangle |n\rangle &= e^{i\chi L a^\dagger a b^\dagger b} e^{-\frac{|\alpha|^2}{2}} \sum_m \frac{\alpha^m}{\sqrt{m!}} |m\rangle |n\rangle \\
&= e^{i\chi L n b^\dagger b} e^{-\frac{|\alpha|^2}{2}} \sum_m \frac{\alpha^m}{\sqrt{m!}} |m\rangle |n\rangle \\
&= e^{-\frac{|\alpha|^2}{2}} \sum_{m,l} \frac{1}{l!} (i\chi L n b^\dagger b)^l \frac{\alpha^m}{\sqrt{m!}} |m\rangle |n\rangle \\
&= e^{-\frac{|\alpha|^2}{2}} \sum_{m,l} \frac{1}{l!} (i\chi L n m)^l \frac{\alpha^m}{\sqrt{m!}} |m\rangle |n\rangle \\
&= e^{-\frac{|\alpha e^{i\chi L n}|^2}{2}} \sum_m \frac{(\alpha e^{i\chi L n})^m}{\sqrt{m!}} |m\rangle |n\rangle \\
&= |\alpha e^{i\chi L n}\rangle |n\rangle
\end{aligned}$$

なので,

$$\begin{aligned}
K |\alpha\rangle |\beta\rangle &= K e^{-\frac{|\beta|^2}{2}} \sum_n \frac{\beta^n}{\sqrt{n!}} |\alpha\rangle |n\rangle \\
&= e^{-\frac{|\beta|^2}{2}} \sum_n \frac{\beta^n}{\sqrt{n!}} |\alpha e^{i\chi L n}\rangle |n\rangle
\end{aligned}$$

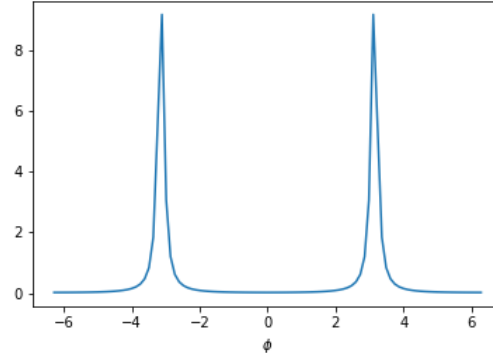
であることから,

$$\begin{aligned}
\rho_a &= \text{tr}_b [K |\alpha\rangle |\beta\rangle \langle\beta| \langle\alpha| K^\dagger] \\
&= e^{-|\beta|^2} \text{tr}_b \left[ \sum_{n,m} \frac{\beta^n}{\sqrt{n!}} \frac{\bar{\beta}^m}{\sqrt{m!}} |\alpha e^{i\chi L n}\rangle |n\rangle \langle m| \langle\alpha e^{i\chi L m}| \right] \\
&= e^{-|\beta|^2} \text{tr}_b \left[ \sum_{n,m} \delta_{nm} \frac{\beta^n}{\sqrt{n!}} \frac{\bar{\beta}^m}{\sqrt{m!}} |\alpha e^{i\chi L n}\rangle \langle\alpha e^{i\chi L m}| \right] \\
&= e^{-|\beta|^2} \sum_n \frac{|\beta|^{2n}}{n!} |\alpha e^{i\chi L n}\rangle \langle\alpha e^{i\chi L n}|
\end{aligned}$$

を得る. この和の主な寄与をもたらす  $n$  は,

$$1 = \frac{|\beta|^{2(n-1)}}{(n-1)!} \frac{n!}{|\beta|^{2n}} \rightarrow n \sim |\beta|^2.$$

## 演習 7.15



演習 7.16  $m = \pm 1$  とする.

$$I \equiv \int Y_{l_1, m_1}^* Y_{1, m} Y_{l_2, m_2} d\Omega \propto \int_0^\pi P_{l_1, m_1}(\cos \theta) \sin \theta P_{l_2, m_2}(\cos \theta) d\cos \theta \int_0^{2\pi} e^{i(-m_1+m+m_2)\phi} d\phi.$$

$I$  の  $\phi$  成分の積分に注目すると,  $I \neq 0$  であるためには,

$$\int_0^{2\pi} e^{i(-m_1+m+m_2)\phi} d\phi \neq 0 \longleftrightarrow -m_1 + m + m_2 = 0 \longleftrightarrow m_1 - m_2 = m = \pm 1$$

であることが必要.

以下では  $m = 1$  の場合だけ考えるが,  $m = -1$  の場合も同様である. 先の条件より,

$$m_1 = m_2 + 1.$$

Legendre 陪多項式についての漸化式

$$\sin \theta P_{m, l}(\cos \theta) = \frac{1}{2l+1} [P_{l+1, m+1}(\cos \theta) - P_{l-1, m+1}(\cos \theta)]$$

を用いて,  $I$  の  $\theta$  成分の積分は,

$$\begin{aligned} & \int_0^\pi P_{l_1, m_2+1}(\cos \theta) \sin \theta P_{l_2, m_2}(\cos \theta) d\cos \theta \\ &= \frac{1}{2l_2+1} \int_0^\pi P_{l_1, m_2+1}(\cos \theta) [P_{l_2+1, m_2+1}(\cos \theta) - P_{l_2-1, m_2+1}(\cos \theta)] d\cos \theta \end{aligned}$$

となる. よって, Legendre 陪多項式の直交性より,  $m = 1$  の時,  $I$  の  $\theta$  成分の積分が 0 にならないための必要十分条件は,  $m_1 - m_2 = 1$  かつ  $l_1 = l_2 \pm 1$ .

以上より,

$$I \neq 0 \longleftrightarrow m_1 - m_2 = \pm 1 \text{ かつ } l_1 - l_2 = \pm 1.$$

演習 7.17  $\omega = \delta = 0$  のとき, Jaynes-Cummings の Hamiltonian  $H$  は,

$$H = g(a^\dagger \sigma_- + a \sigma_+).$$

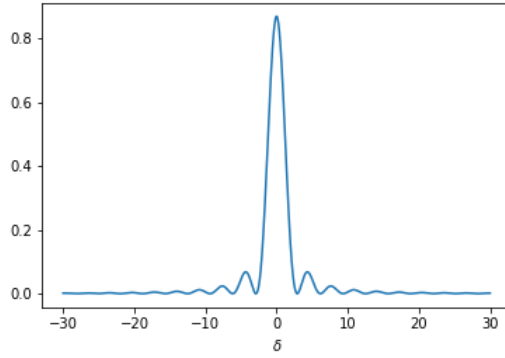
よって,

$$\begin{aligned} H |\chi_n\rangle &= g(a^\dagger \sigma_- + a \sigma_+) \frac{|n, 1\rangle + |n+1, 0\rangle}{\sqrt{2}} = g \frac{\sqrt{n+1} |n+1, 0\rangle + \sqrt{n+1} |n, 1\rangle}{\sqrt{2}} = g\sqrt{n+1} |\chi_n\rangle \\ H |\bar{\chi}_n\rangle &= g(a^\dagger \sigma_- + a \sigma_+) \frac{|n, 1\rangle - |n+1, 0\rangle}{\sqrt{2}} = g \frac{\sqrt{n+1} |n+1, 0\rangle - \sqrt{n+1} |n, 1\rangle}{\sqrt{2}} = -g\sqrt{n+1} |\bar{\chi}_n\rangle. \end{aligned}$$

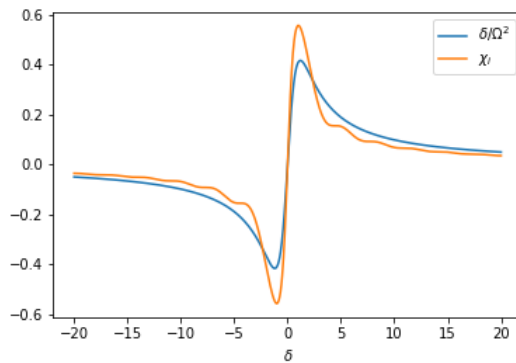
演習 7.18 時間発展演算子  $U$  は,  $\Omega = \sqrt{g^2 + \delta^2}$  を用いて,

$$\begin{aligned}
 U &= \exp[-iHt] \\
 &= e^{i\delta t} |00\rangle\langle 00| + \exp\left[i\begin{pmatrix} -\delta t & gt \\ gt & \delta t \end{pmatrix}\right] \\
 &= e^{i\delta t} |00\rangle\langle 00| + \exp[igtX - i\delta tZ] \\
 &= e^{i\delta t} |00\rangle\langle 00| + I \cos \Omega t + i\frac{g}{\Omega} X \sin \Omega t - i\frac{\delta}{\Omega} Z \sin \Omega t \\
 &= e^{i\delta t} |00\rangle\langle 00| + (|01\rangle\langle 01| + |10\rangle\langle 10|) \cos \Omega t + i\frac{g}{\Omega} \sin \Omega t (|01\rangle\langle 10| + |10\rangle\langle 01|) - i\frac{\delta}{\Omega} \sin \Omega t (|01\rangle\langle 01| - |10\rangle\langle 10|) \\
 &= e^{i\delta t} |00\rangle\langle 00| + \left(\cos \Omega t + i\frac{\delta}{\Omega} \sin \Omega t\right) |01\rangle\langle 01| + \left(\cos \Omega t + i\frac{\delta}{\Omega} \sin \Omega t\right) |10\rangle\langle 10| - i\frac{g}{\Omega} \sin \Omega t (|01\rangle\langle 10| + |10\rangle\langle 01|).
 \end{aligned}$$

演習 7.19



演習 7.20



演習 7.21  $\arg(\langle 110|U|110\rangle)$  を求めるには,  $U = \exp[-iHt]$  の  $|110\rangle\langle 110|$  成分だけ考えればよい. すると,

$$H_2^n = \begin{pmatrix} -\delta & g_a & g_b \\ g_a & \delta & 0 \\ g_b & 0 & \delta \end{pmatrix}^n = \begin{cases} \Omega'^n |110\rangle\langle 110| + \dots & (n \text{ is even}) \\ -\delta \Omega'^{n-1} |110\rangle\langle 110| + \dots & (n \text{ is odd}) \end{cases}$$

なので,

$$\langle 110|U|110\rangle = \langle 110|\exp[-iHt]|110\rangle$$

$$\begin{aligned}
&= \langle 110 | \exp[-iH_2 t] | 110 \rangle \\
&= \langle 110 | \sum_n \frac{1}{n!} (-iH_2 t)^n | 110 \rangle \\
&= \sum_{n \text{ is even}} \frac{(-1)^{\frac{n}{2}} t^n}{n!} \Omega'^n + i\delta \sum_{n \text{ is odd}} \frac{(-1)^{\frac{n-1}{2}} t^n}{n!} \Omega'^{n-1} \\
&= \sum_n \frac{(-1)^n t^{2n}}{(2n)!} \Omega'^{2n} + i \frac{\delta}{\Omega'} \sum_n \frac{(-1)^n t^{2n+1}}{(2n+1)!} \Omega'^{2n+1} \\
&= \cos \Omega' t + i \frac{\delta}{\Omega'} \sin \Omega' t
\end{aligned}$$

を得る. よって,

$$\begin{aligned}
\phi_{ab} &= \arg(\langle 110 | U | 110 \rangle) - \arg(\langle 000 | U | 000 \rangle) = \arg\left(\cos \Omega' t + i \frac{\delta}{\Omega'} \sin \Omega' t\right) - \arg(e^{i\delta t}) \\
&= \arg\left[\left(\cos \Omega' t + i \frac{\delta}{\Omega'} \sin \Omega' t\right) e^{-i\delta t}\right].
\end{aligned}$$

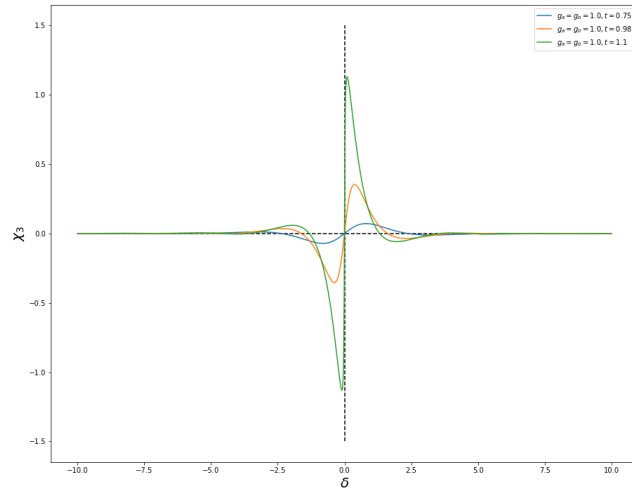
$\phi_a, \phi_b$  については,  $\Omega_i = \sqrt{g_i^2 + \delta^2}$  として, 式 (7.77) と全く同様の計算をして,

$$\begin{aligned}
\phi_a &= \arg(\langle 100 | U | 100 \rangle) - \arg(\langle 000 | U | 000 \rangle) = \arg\left[\left(\cos \Omega_a t - i \frac{\delta}{\Omega_a} \sin \Omega_a t\right) e^{-i\delta t}\right] \\
\phi_b &= \arg(\langle 010 | U | 010 \rangle) - \arg(\langle 010 | U | 010 \rangle) = \arg\left[\left(\cos \Omega_b t - i \frac{\delta}{\Omega_b} \sin \Omega_b t\right) e^{-i\delta t}\right]
\end{aligned}$$

以上より,

$$\chi_3 = \phi_{ab} - \phi_a - \phi_b = \arg\left[\frac{\cos \Omega' t + i \frac{\delta}{\Omega'} \sin \Omega' t}{\left(\cos \Omega_a t - i \frac{\delta}{\Omega_a} \sin \Omega_a t\right) \left(\cos \Omega_b t - i \frac{\delta}{\Omega_b} \sin \Omega_b t\right)} e^{i\delta t}\right]$$

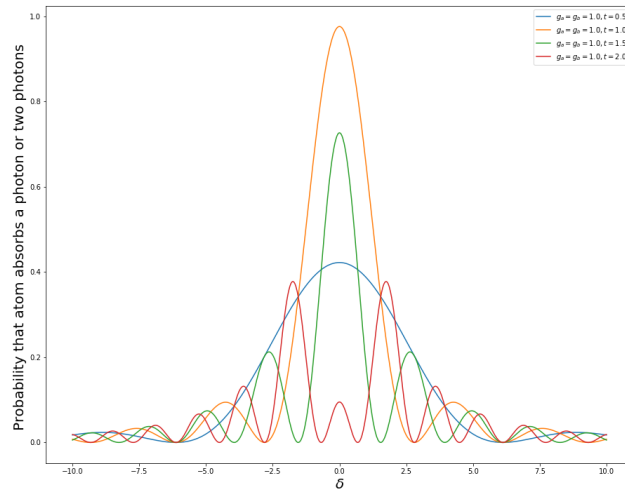
$\chi_3$  の  $\delta$  依存性を図示すると, 以下のようになる.



演習 7.22 演習 7.21 より, 光子が原子に吸収される確率は,

$$1 - |\langle 110|U|110\rangle|^2 = 1 - (\cos \Omega' t)^2 - \left( \frac{\delta}{\Omega'} \sin \Omega' t \right)^2$$

図示すると, 以下のようになる.



演習 7.23

演習 7.24

$$\mu_N B \sim 5 \times 10^{-26} J < k_B T \sim 5 \times 10^{-21} J$$

演習 7.25

$$\begin{aligned} [j_i, j_k] &= \left[ \frac{\sigma_i \otimes I + I \otimes \sigma_i}{2}, \frac{\sigma_k \otimes I + I \otimes \sigma_k}{2} \right] \\ &= \frac{[\sigma_i \otimes I, \sigma_k \otimes I] + [I \otimes \sigma_i, I \otimes \sigma_k]}{4} \\ &= i\epsilon_{ikl} \frac{\sigma_l \otimes I + I \otimes \sigma_l}{2} \\ &= i\epsilon_{ikl} j_l. \end{aligned}$$

演習 7.26

$$J^2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \quad j_z = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

演習 7.27

演習 7.28 (1)

$$[i_k, i_l] = i\epsilon_{klm} i_m.$$

(2)

$$|2, 2\rangle, |2, 1\rangle, |2, 0\rangle, |2, -1\rangle, |2, -2\rangle, |1, 1\rangle, |1, 0\rangle, |1, -1\rangle.$$

演習 7.29

$$\int_0^\infty \frac{\sin^2 \frac{\omega - \omega_0}{2} t}{(\omega - \omega_0)^2} \omega \, d\omega \sim \int_{-\infty}^\infty \frac{\sin^2 \frac{\omega - \omega_0}{2} t}{(\omega - \omega_0)^2} \omega_0 \, d\omega = \int_{-\infty}^\infty \frac{t^2 \sin^2 \frac{\omega - \omega_0}{2} t}{4 \left( \frac{\omega - \omega_0}{2} t \right)^2} \omega_0 \, d\omega = \int_{-\infty}^\infty \frac{t \sin^2 x}{2x^2} \omega_0 \, dx = \frac{\pi t \omega_0}{2}.$$

ここで,  $\sim$  では, 被積分関数の寄与が  $\omega \sim \omega_0$  で非常に大きいことを用いた. この結果を用いて,

$$\begin{aligned} \gamma_{\text{rad}} &= \frac{d}{dt} \frac{1}{(2\pi c)^2} \frac{8\pi}{3} \int_0^\infty \omega^2 p_{\text{decay}} \, d\omega \\ &= \frac{d}{dt} \frac{1}{(2\pi c)^2} \frac{8\pi}{3} \int_0^\infty \frac{\omega_0^2 |\langle 0 | \boldsymbol{\mu} | 1 \rangle|^2}{2\hbar \omega \epsilon_0 c^3} \frac{4 \sin^2 \frac{\omega - \omega_0}{2} t}{(\omega - \omega_0)^2} \omega^2 \, d\omega \\ &= \frac{\omega_0^3 |\langle 0 | \boldsymbol{\mu} | 1 \rangle|^2}{3\pi \hbar \epsilon_0 c^5}. \end{aligned}$$

演習 7.30

$$\frac{\gamma_{\text{rad}}^{\text{ed}}}{\gamma_{\text{rad}}} = \frac{|\langle 0 | \boldsymbol{\mu}_{\text{ed}} | 1 \rangle|^2}{|\langle 0 | \boldsymbol{\mu} | 1 \rangle|^2} \sim \frac{e^2 a_0^2 \omega_0^{\text{ed}}}{\mu_B^2 \omega_0} \sim \frac{10^{-58} 10^{15}}{10^{-46} 10^{10}} = 10^{-7}.$$

演習 7.31

$$H = e^{i\frac{\pi}{2}} R_x(\pi) R_y\left(\frac{\pi}{2}\right).$$

演習 7.32

演習 7.33

$$\begin{aligned} i \frac{\partial}{\partial t} |\phi(t)\rangle &= i \frac{\partial}{\partial t} e^{\frac{i\omega Z t}{2}} |\chi(t)\rangle \\ &= -\frac{\omega Z}{2} e^{\frac{i\omega Z t}{2}} |\chi(t)\rangle + i e^{\frac{i\omega Z t}{2}} \frac{\partial}{\partial t} |\chi(t)\rangle \\ &= -\frac{\omega Z}{2} e^{\frac{i\omega Z t}{2}} |\chi(t)\rangle + e^{\frac{i\omega Z t}{2}} H |\chi(t)\rangle \\ &= \left[ e^{\frac{i\omega Z t}{2}} H e^{-\frac{i\omega Z t}{2}} - \frac{\omega Z}{2} e^{\frac{i\omega Z t}{2}} \right] |\phi(t)\rangle. \end{aligned}$$

演習 7.34

演習 7.35  $H_{1,2}^D$  の球面平均は, その定数項の寄与を除いて,

$$\begin{aligned} &\int_0^\pi d\theta \int_0^{2\pi} d\phi \sin \theta [\boldsymbol{\sigma}_1 \cdot \boldsymbol{\sigma}_2 - 3(\boldsymbol{\sigma}_1 \cdot \mathbf{n})(\boldsymbol{\sigma}_2 \cdot \mathbf{n})] \\ &= \int_0^\pi d\theta \int_0^{2\pi} d\phi \sigma_{1x} \sigma_{2x} (\sin \theta - 3 \sin^3 \theta \cos^2 \phi) + \sigma_{1y} \sigma_{2y} (\sin \theta - 3 \sin^3 \theta \sin^2 \phi) + \sigma_{1z} \sigma_{2z} (\sin \theta - 3 \cos^2 \theta \sin \theta) \\ &\quad + \sin^3 \theta \sin \phi \cos \phi (\sigma_{1x} \sigma_{2y} + \sigma_{1y} \sigma_{2x}) + \sin^3 \theta \cos \theta \cos \phi (\sigma_{1x} \sigma_{2z} + \sigma_{1z} \sigma_{2x}) \\ &\quad + \sin^2 \theta \cos \theta \sin \phi (\sigma_{1y} \sigma_{2z} + \sigma_{1z} \sigma_{2y}) \\ &= 0 \end{aligned}$$

演習 7.36  $\underline{n=1}$

考えるべきは, 2 準位系で, そのエネルギーを  $\frac{\hbar\omega}{2}, -\frac{\hbar\omega}{2}$  とする. すると, 基底としてエネルギー固有状態を考えた行列表示で,  $\beta \ll 1$  とすると,

$$e^{-\beta H} \sim 1 - \beta H = 1 - \frac{\beta \hbar \omega}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$n = 2$

2 つの 2 準位系;

$$\begin{aligned} A &: -\frac{\omega_A}{4}, \frac{\omega_A}{4} \\ B &: -\frac{\omega_B}{4}, \frac{\omega_B}{4} \end{aligned}$$

を考えると,

$$e^{-\beta H} \sim 1 - \beta H = 1 - \beta \hbar \begin{pmatrix} \omega_A + \omega_B & 0 & 0 & 0 \\ 0 & \omega_B - \omega_A & 0 & 0 \\ 0 & 0 & \omega_A - \omega_B & 0 \\ 0 & 0 & 0 & -\omega_A - \omega_B \end{pmatrix} = 1 - \frac{\beta \hbar \omega_A}{4} \begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & -3 & 0 \\ 0 & 0 & 0 & -5 \end{pmatrix}$$

演習 7.37 まず,

$$H = JZ_1 \otimes Z_2$$

のとき,

$$e^{-iHt} = I \otimes I \cos Jt - iZ_1 \otimes Z_2 \sin Jt = \begin{pmatrix} e^{-iJt} & 0 & 0 & 0 \\ 0 & e^{iJt} & 0 & 0 \\ 0 & 0 & e^{iJt} & 0 \\ 0 & 0 & 0 & e^{-iJt} \end{pmatrix}.$$

次に,

$$\begin{aligned} \rho &= \exp \left[ i\pi \frac{Y_1 \otimes I}{4} \right] \frac{1}{4} [1 - \beta \hbar \omega_0 (Z_1 \otimes I + I \otimes Z_2)] \exp \left[ -i\pi \frac{Y_1 \otimes I}{4} \right] \\ &= \frac{1}{4} [1 - \beta \hbar \omega_0 (-X_1 \otimes I + I \otimes Z_2)]. \end{aligned}$$

よって,

$$e^{-iHt} \rho e^{iHt} = \frac{1}{4} \begin{pmatrix} 1 - \beta \hbar \omega_0 & 0 & \beta \hbar \omega_0 e^{-2iJt} & 0 \\ 0 & 1 + \beta \hbar \omega_0 & 0 & \beta \hbar \omega_0 e^{2iJt} \\ \beta \hbar \omega_0 e^{2iJt} & 0 & 1 - \beta \hbar \omega_0 & 0 \\ 0 & \beta \hbar \omega_0 e^{-2iJt} & 0 & 1 + \beta \hbar \omega_0 \end{pmatrix}.$$

したがって,

$$\begin{aligned} V(t) &= V_0 \operatorname{tr} [e^{-iHt} \rho e^{iHt} (iX_1 + Y_1) \otimes I] \\ &= \frac{iV_0 \beta \hbar \omega_0}{2} \operatorname{tr} \left[ \begin{pmatrix} e^{2iJt} & 0 & 0 & 0 \\ 0 & e^{-2iJt} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \right] \\ &= iV_0 \beta \hbar \omega_0 \cos Jt. \end{aligned}$$



演習 7.38 演習 4.7 と同様に,

$$XR_z(\theta)X = R_z(-\theta)$$

であることから,

$$R_x(\pi)e^{-iaZ_1t}R_x(\pi) = (-iX)R_z(2at)(-iX) = -R_z(-2at) = -e^{iaZ_1t}.$$

演習 7.39  $R_x = R_x\left(\frac{\pi}{2}\right)$ ,  $R_y = R_y\left(\frac{\pi}{2}\right)$  とする. 演習 7.38 と同様に,

$$\begin{aligned} R_x^2 e^{-ic_y \sigma_y} R_x^2 &= -e^{ic_y \sigma_y} \\ R_x^2 e^{-ic_z \sigma_z} R_x^2 &= -e^{ic_z \sigma_z} \\ R_y^2 e^{-ic_x \sigma_x} R_y^2 &= -e^{ic_x \sigma_x} \end{aligned}$$

である. このことを用いて,

$$H = \sum_k c_k \sigma_k$$

に対して,

$$\begin{aligned} e^{-iHt} R_x^2 e^{-iHt} R_x^2 &= -e^{-2ic_x \sigma_x t} \\ R_y^2 e^{-iHt} R_x^2 e^{-iHt} R_x^2 R_y^2 &= -R_y^2 e^{-2ic_x \sigma_x t} R_y^2 = e^{2ic_x \sigma_x t} \end{aligned}$$

となるから,

$$R_y^2 e^{-iHt} R_x^2 e^{-iHt} R_x^2 R_y^2 e^{-iHt} R_x^2 e^{-iHt} R_x^2 = -e^{2ic_x \sigma_x t} e^{-2ic_x \sigma_x t} = -1$$

というようなパルス列を与えると, 系の時間発展を再収束させられる.

演習 7.40

演習 7.41

$$H = aZ_1 + bZ_2 + cZ_1Z_2$$

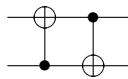
のとき,

$$\begin{aligned} e^{-iHt} R_{x1}^2 e^{-iHt} R_{x1}^2 &= -e^{-2ibZ_2t} \\ e^{-iHt} R_{x2}^2 e^{-iHt} R_{x2}^2 &= -e^{-2iaZ_1t} \\ e^{-iHt} R_{x1}^2 R_{x2}^2 e^{-iHt} R_{x1}^2 R_{x2}^2 &= e^{-2icZ_1Z_2t} \end{aligned}$$

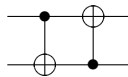
であることと演習 7.47 より,

$$\begin{aligned} e^{-i\frac{\pi}{4}} U_{CNOT} &= e^{i\frac{\pi}{4}Z_2} e^{-i\frac{\pi}{4}Z_1} R_{x2} e^{-i\frac{\pi}{2}Z_1Z_2} R_{y2} \\ &= e^{iH\frac{\pi}{8b}} R_{x1}^2 e^{iH\frac{\pi}{8b}} R_{x1}^2 e^{-iH\frac{\pi}{8a}} R_{x2}^2 e^{-iH\frac{\pi}{8a}} R_{x2}^2 e^{-iH\frac{\pi}{8c}} R_{x1}^2 R_{x2}^2 e^{-iH\frac{\pi}{8c}} R_{x1}^2 R_{x2}^2 R_{y2}. \end{aligned}$$

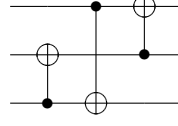
演習 7.42  $P$  は,



$P^\dagger$  は,



## 演習 7.43



演習 7.44 簡単のため  $n$  を偶数とする. Zeemann 周波数  $\omega$  の spin が  $n$  個ある系の密度行列  $\rho$  は,

$$Z = e^{\beta\hbar\omega} + e^{-\beta\hbar\omega}$$

として,

$$\rho = \frac{1}{Z^n} \begin{pmatrix} e^{\beta\hbar\omega} & 0 \\ 0 & e^{-\beta\hbar\omega} \end{pmatrix}^{\otimes n}.$$

特に  $\beta\hbar\omega \ll 1$  では,

$$\rho \sim \frac{1}{2^n} \left[ I + \beta\hbar\omega \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right]^{\otimes n}.$$

以下  $O(\beta\hbar\omega)$  まで考えとする. 少し頑張って考えると,  $\rho$  の対角成分の 0 の個数は  $2^{\frac{n}{2}+1} - 2$  個,  $\rho$  の (0,0) 成分は  $\frac{n\beta\hbar\omega}{2^n}$  になる. したがって, 式 (7.163) から式 (7.165) と全く同様の手続きを行えば,

$$\exists \tilde{P} \quad \left( \tilde{P} \rho \tilde{P}^\dagger - \frac{I^{\otimes n}}{2^n} \text{の上 } (2^{\frac{n}{2}+1} - 2) \times (2^{\frac{n}{2}+1} - 2) \text{ ブロック} \right) = \frac{n\beta\hbar\omega}{2^n} \underbrace{|00\dots 00\rangle}_{2^{\frac{n}{2}+1}-2 \text{ qubit}} \langle 00\dots 00|.$$

$n$  が偶数の時,  $\rho$  の対角成分の値に注目すると 0 が一番多いので, 上に示したものが, 論理ラベルで作れる実効的純粋状態のうち最大の qubit 数を持つものである.

演習 7.45 密度行列  $\rho$  は  $r_{ij} \in \mathbb{R}$  ( $i, j = 1, 2, 3$ ) を用いて,

$$\rho = \frac{1}{4} \left[ I \otimes I + \sum_{i,j} r_{ij} \sigma_i \otimes \sigma_j \right]$$

かける. この  $\rho$  の各係数  $r_{ij}$  を決めるには,

$$\langle \sigma_i \otimes \sigma_j \rangle = \text{tr}[\rho \sigma_i \otimes \sigma_j] = r_{ij}$$

より,  $\sigma_i \otimes \sigma_j$  を測定すれば良い. つまり 9 回の測定をすれば良い.

演習 7.46 27 回測定すれば十分.

## 演習 7.47

$$\begin{aligned} R_{x2} e^{-i\frac{\pi}{4} Z_1 Z_2} R_{y2} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix} e^{-i\frac{\pi}{4}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i & 0 & 0 \\ -i & 1 & 0 & 0 \\ 0 & 0 & 1 & -i \\ 0 & 0 & -i & 1 \end{pmatrix} \\ &= e^{-i\frac{\pi}{4}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{aligned}$$

であり,

$$\begin{aligned}
 e^{i\frac{\pi}{4}Z_2}e^{-i\frac{\pi}{4}Z_1}R_{x2}e^{-i\frac{\pi}{4}Z_1Z_2}R_{y2} &= \begin{pmatrix} e^{i\frac{\pi}{4}} & 0 & 0 & 0 \\ 0 & e^{-i\frac{\pi}{4}} & 0 & 0 \\ 0 & 0 & e^{i\frac{\pi}{4}} & 0 \\ 0 & 0 & 0 & e^{-i\frac{\pi}{4}} \end{pmatrix} \begin{pmatrix} e^{-i\frac{\pi}{4}} & 0 & 0 & 0 \\ 0 & e^{-i\frac{\pi}{4}} & 0 & 0 \\ 0 & 0 & e^{i\frac{\pi}{4}} & 0 \\ 0 & 0 & 0 & e^{i\frac{\pi}{4}} \end{pmatrix} e^{-i\frac{\pi}{4}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & 1 & 0 \end{pmatrix} \\
 &= e^{-i\frac{\pi}{4}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = e^{-i\frac{\pi}{4}} U_{CNOT}.
 \end{aligned}$$

演習 7.48

$$\begin{aligned}
 R_{x2}e^{-i\frac{\pi}{4}Z_1Z_2}R_{y2}R_{y1} &= e^{-i\frac{\pi}{4}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & 1 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix} \\
 &= \frac{e^{-i\frac{\pi}{4}}}{\sqrt{2}} \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & i & 0 & -i \\ 0 & -i & 0 & -i \\ 1 & 0 & 1 & 0 \end{pmatrix}
 \end{aligned}$$

より,  $R_{x2}e^{-i\frac{\pi}{4}Z_1Z_2}R_{y2}R_{y1}$  は,

$$\begin{aligned}
 |00\rangle &\rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\
 |01\rangle &\rightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}} \\
 |10\rangle &\rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\
 |11\rangle &\rightarrow \frac{|01\rangle + |10\rangle}{\sqrt{2}}
 \end{aligned}$$

というように Bell 状態を作る.

演習 7.49 演習 7.47 で CNOT がいかに作れるかを示したことを思い出して,

$$\begin{aligned}
 SWAP &= C(X_2)C(X_1)C(X_2) \\
 &= e^{-i\frac{3\pi}{4}}e^{i\frac{\pi}{4}Z_2}e^{-i\frac{\pi}{4}Z_1}R_{x2}e^{-i\frac{\pi}{4}Z_1Z_2}R_{y2}e^{i\frac{\pi}{4}Z_1}e^{-i\frac{\pi}{4}Z_2}R_{x1}e^{-i\frac{\pi}{4}Z_1Z_2}R_{y1}e^{i\frac{\pi}{4}Z_2}e^{-i\frac{\pi}{4}Z_1}R_{x2}e^{-i\frac{\pi}{4}Z_1Z_2}R_{y2}.
 \end{aligned}$$

演習 7.50

演習 7.51  $x_0 = 3$  の時だけ示す.  $R_{\gamma i}$  と  $R_{\gamma j}$  は  $i \neq j$  のとき可換で,  $R_x^3 = \bar{R}_x, R_y^3 = \bar{R}_y$  であることを用いて,

$$\begin{aligned}
 G &= H^{\otimes 2}PH^{\otimes 2}O = R_{x1}^2\bar{R}_{y1}R_{x2}^2\bar{R}_{y2}R_{x1}\bar{R}_{y1}R_{x2}\bar{R}_{y2}\tau R_{x1}^2\bar{R}_{y1}R_{x2}^2\bar{R}_{y2}R_{x1}\bar{R}_{y1}R_{x2}\bar{R}_{y2}\tau \\
 &= R_{x1}^2R_{x2}^2R_{x1}\bar{R}_{y1}R_{x2}\bar{R}_{y2}\tau R_{x1}^2R_{x2}^2\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau \\
 &= R_{x1}^3R_{x2}^3\bar{R}_{y1}\bar{R}_{y2}\tau R_{x1}\bar{R}_{y1}\bar{R}_{y2}\tau \\
 &= \bar{R}_{x1}\bar{R}_{x2}\bar{R}_{y1}\bar{R}_{y2}\tau R_{x1}R_{x2}\bar{R}_{y1}\bar{R}_{y2}\tau.
 \end{aligned}$$

## 第 8 章

# 量子雑音と量子情報

演習 8.1

$$\mathcal{E}(\rho) = U |\psi\rangle \langle\psi| U^\dagger = U \rho U^\dagger$$

演習 8.2 密度行列は、スペクトル分解可能;

$$\rho = \sum_i p_i |i\rangle \langle i|.$$

測定オペレータの集合  $\{M_m\}$  に対し、 $\rho$  の測定結果が  $m$  である確率は、

$$p(m) = \sum_i p(m|i) p_i = \sum_i \langle i | M_m^\dagger M_m | i \rangle p_i = \text{tr} \left[ \sum_i \langle i | M_m^\dagger M_m | i \rangle p_i \right] = \text{tr} [M_m^\dagger M_m \rho] = \text{tr} [M_m \rho M_m^\dagger].$$

測定後の系の状態  $\rho_m$  は、

$$\left\{ |i^m\rangle = \frac{M_m |i\rangle}{\sqrt{\langle i | M_m^\dagger M_m | i \rangle}}, p(i|m) \right\}$$

というアンサンブルで、

$$\rho_m = \sum_i p(i|m) |i^m\rangle \langle i^m| = \sum_i \frac{p(m|i) p_i}{p(m)} \frac{M_m |i\rangle \langle i| M_m^\dagger}{\langle i | M_m^\dagger M_m | i \rangle} = \sum_i p(i|m) |i^m\rangle \langle i^m| = \sum_i \frac{p_i M_m |i\rangle \langle i| M_m^\dagger}{p(m)} = \frac{M_m \rho M_m^\dagger}{\text{tr} [M_m \rho M_m^\dagger]}$$

演習 8.3 AB の初期状態  $\rho_A \otimes \rho_B = \rho = \sum_{a,b} p_{ab} |a\rangle \langle a| \otimes |b\rangle \langle b|$ , CD の初期状態  $|0_C\rangle \langle 0_C| \otimes |0_D\rangle \langle 0_D|$  として、

$$\begin{aligned} \mathcal{E}(\rho) &= \text{tr}_{A \otimes D} [U \rho \otimes |0_C\rangle \langle 0_C| \otimes |0_D\rangle \langle 0_D| U^\dagger] \\ &= \sum_{a,a',b,d'} p_{ab} \langle a' | \otimes \langle d' | (U |a\rangle \langle a| \otimes |b\rangle \langle b| \otimes |0\rangle \langle 0| \otimes |0\rangle \langle 0| U^\dagger) |a'\rangle \otimes |d'\rangle \\ &= \sum_{a,a',b,d'} p_{ab} \langle a' | \otimes \langle d' | U |0_C\rangle \otimes |0_D\rangle |a\rangle \langle a| \otimes |b\rangle \langle b| \langle 0_C| \otimes \langle 0_D| U^\dagger |a'\rangle \otimes |d'\rangle \\ &= \sum_{a',d'} \langle a' | \otimes \langle d' | U |0_C\rangle \otimes |0_D\rangle \rho \langle 0_C| \otimes \langle 0_D| U^\dagger |a'\rangle \otimes |d'\rangle = \sum_{a,d} E_{ad} \rho E_{ad}^\dagger. \end{aligned}$$

ただし、

$$E_{ad} = \langle a' | \otimes \langle d' | U |0_C\rangle \otimes |0_D\rangle$$

で、AD での完全性条件より、

$$\sum_{a,d} E_{ad} E_{ad}^\dagger = \sum_{a,d} \langle a' | \otimes \langle d' | U |0_C\rangle \otimes |0_D\rangle \langle 0_C| \otimes \langle 0_D| U^\dagger |a'\rangle \otimes |d'\rangle$$

$$\begin{aligned}
&= \sum_{a,d} \langle 0_C | \otimes \langle 0_D | U^\dagger | a' \rangle \otimes | d' \rangle \langle a' | \otimes \langle d' | U | 0_C \rangle \otimes | 0_D \rangle \\
&= \langle 0_C | \otimes \langle 0_D | U^\dagger U | 0_C \rangle \otimes | 0_D \rangle = I_{AB}.
\end{aligned}$$

演習 8.4 環境の初期状態  $|0\rangle$  として,

$$E_k = \langle k | U | 0 \rangle = \langle k | P_0 \otimes I + P_1 \otimes X | 0 \rangle = P_0 \langle k | 0 \rangle + P_1 \langle k | 1 \rangle.$$

なので, 量子演算は,

$$\mathcal{E}(\rho) = \sum_{k=0,1} E_k \rho E_k^\dagger = P_0 \rho P_0 + P_1 \rho P_1.$$

演習 8.5 環境の初期状態  $|0\rangle$  として,

$$E_k = \langle k | U | 0 \rangle = \frac{X}{\sqrt{2}} \langle k | 0 \rangle + \frac{Y}{\sqrt{2}} \langle k | 1 \rangle.$$

なので, 量子演算は,

$$\mathcal{E}(\rho) = \sum_{k=0,1} E_k \rho E_k^\dagger = \frac{X \rho X + Y \rho Y}{2}.$$

演習 8.6  $\mathcal{E}, \mathcal{F} : \text{Map}(\mathbb{C}^n, \mathbb{C}^n) \rightarrow \text{Map}(\mathbb{C}^n, \mathbb{C}^n)$  のとき

演算要素  $\{\mathcal{F}_k \in \text{Map}(\mathbb{C}^n, \mathbb{C}^n)\}, \{\mathcal{E}_k \in \text{Map}(\mathbb{C}^n, \mathbb{C}^n)\}$  として,

$$\mathcal{F}(\rho) = \sum_k \mathcal{F}_k \rho \mathcal{F}_k^\dagger \in \text{Map}(\mathbb{C}^n, \mathbb{C}^n)$$

なので,

$$\mathcal{E} \circ \mathcal{F}(\rho) = \mathcal{E}(\mathcal{F}(\rho)) = \sum_{k,l} \mathcal{E}_l \mathcal{F}_k \rho \mathcal{F}_k^\dagger \mathcal{E}_l^\dagger$$

となり,  $\mathcal{E} \circ \mathcal{F}$  は演算要素  $\{\mathcal{F}_k \mathcal{E}_l\}$  をもつ量子演算.

$\mathcal{E}, \mathcal{F} : \text{Map}(\mathbb{C}^n, \mathbb{C}^n) \rightarrow \text{Map}(\mathbb{C}^m, \mathbb{C}^m)$  のとき

わからない.

演習 8.7

$$\mathcal{E}_m(\rho) = \text{tr}_E(M_m U \rho \otimes \sigma U^\dagger M_m^\dagger)$$

として,  $Q$  の終状態は,

$$\frac{\mathcal{E}_m(\rho)}{\text{tr}[\mathcal{E}_m(\rho)]}$$

で,

$$\sigma = \sum_j q_j |j\rangle \langle j|$$

ならば,

$$\mathcal{E}_m(\rho) = \sum_{jk} q_j \langle e_k | M_m U \rho \otimes |j\rangle \langle j| U^\dagger M_m^\dagger | e_k \rangle = \sum_{j,k} E_{jk} \rho E_{jk}^\dagger.$$

ここで,

$$E_{jk} = \sqrt{q_j} \langle e_k | M_m U | j \rangle.$$

演習 8.8  $\{E_k\}_{k=0}^{n+1}$  は,

$$\sum_{k=0}^{n+1} E_k^\dagger E_k = I, \quad \sum_{k=0}^n E_k^\dagger E_k < I$$

を満たすとする. 正規直交基底  $\{|e_k\rangle\}_{k=0}^{n+1}$  で張られる Hilbert 空間  $E'$  と主システムの Hilbert 空間  $Q$  とする. ここで, 任意の  $|\psi\rangle \in Q$  に対して,  $U : Q \otimes E' \rightarrow Q \otimes E'$ ;

$$\begin{aligned} U |\psi\rangle |e_0\rangle &= \sum_{k=0}^{n+1} E_k |\psi\rangle |e_k\rangle \\ U |\psi\rangle |e_i\rangle &= |\psi\rangle |e_i\rangle \quad (i \neq 0) \end{aligned}$$

なるオペレータを考えると, 式 (8.38) 同様に, 任意の  $|\psi\rangle, |\phi\rangle \in Q$  に対して,

$$\langle \psi | \langle e_i | U^\dagger U | \phi \rangle | e_j \rangle = \langle \psi | \phi \rangle \langle e_i | e_j \rangle$$

が成り立つので  $U$  はユニタリ. この  $U$  によって, 主システムの終状態が,

$$\text{tr}_{E'} [U \rho \otimes |e_0\rangle \langle e_0| U^\dagger] = \sum_{i=0}^{n+1} \langle e_i | \left[ \sum_{j,k=0}^{n+1} E_j \rho E_k^\dagger \otimes |e_j\rangle \langle e_k| \right] | e_i \rangle = \sum_{i=0}^n E_i \rho E_i^\dagger$$

とオペレータ和表現でかける.

演習 8.9

$$\begin{aligned} \mathcal{E}_m(\rho) &= \text{tr}_{env} [P_m U (\rho \otimes |e_0\rangle \langle e_0|) U^\dagger P_m] \\ &= \sum_{m',k'} \langle m', k' | P_m U (\rho \otimes |e_0\rangle \langle e_0|) U^\dagger P_m | m', k' \rangle \\ &= \sum_{m',k',l,l'} \langle m', k' | m, l \rangle \langle m, l | P_m U (\rho \otimes |e_0\rangle \langle e_0|) U^\dagger P_m | m', l' \rangle \langle m', l' | m', k' \rangle \\ &= \sum_k \langle m, k | U (\rho \otimes |e_0\rangle \langle e_0|) U^\dagger | m, k \rangle \\ &= \sum_{i,k} p_i \langle m, k | U | i \rangle \langle i | \otimes | e_0 \rangle \langle e_0 | U^\dagger | m, k \rangle \\ &= \sum_{i,k,m',k',m'',k''} p_i \langle m, k | (E_{m'k'} | i \rangle \otimes | m', k' \rangle) (\langle i | E_{m''k''}^\dagger \otimes \langle m'', k'' |) | m, k \rangle \\ &= \sum_{i,k} p_i E_{mi} | i \rangle \langle i | E_{mi}^\dagger = \sum_k E_{mk} \rho E_{mk}^\dagger \end{aligned}$$

なので, 測定後の状態は,

$$\frac{\mathcal{E}_m(\rho)}{\text{tr}[\mathcal{E}_m(\rho)]}$$

演習 8.10

$$W_{jk} = \text{tr}[E_j^\dagger E_k] = \text{tr}[E_k E_j^\dagger] = \text{tr}[E_k^\dagger E_j]^* = W_{kj}^*$$

なので,  $W_{jk}$  は Hermite. ここで, 独立な  $\{E_i\}_{i=1}^{d^2}$  を選ぶことで,  $i > d^2$  に対して,

$$E_i = \sum_{j=1}^{d^2} c_j E_j$$

と書けるはずなので,

$$W_{ik} = \text{tr} \left[ E_i^\dagger E_k \right] = \sum_{j=1}^{d^2} c_j W_{jk}$$

つまり,  $\text{rank} W \leq d^2$ . したがって,  $W$  はユニタリ  $u$  で対角化可能で, 対角行列  $u^\dagger W u$  の対角成分の非ゼロ要素は  $\text{rank} W$  個;

$$\sum_{j,k} u_{ij} W_{jk} u_{kn}^\dagger = \sum_{j,k} u_{ij} \text{tr} \left[ E_j^\dagger E_k \right] u_{kn}^\dagger = \sum_{j,k,l,m} u_{ij} e_{lm}^{j*} e_{lm}^k u_{nk}^* \equiv \sum_{l,m} f_{lm}^{i*} f_{lm}^n \propto \begin{cases} \delta_{in} & (1 \leq i, n \leq \text{rank} W) \\ 0 & (\text{otherwise}) \end{cases}$$

したがって,

$$\mathcal{E}(\rho) = \sum_{k=1}^M E_k \rho E_k^\dagger$$

の  $(i, j)$  成分は,

$$\begin{aligned} \mathcal{E}(\rho)_{ij} &= \sum_{k=1}^M \sum_{l,m=1}^d e_{il}^k \rho_{lm} e_{jm}^{k*} \\ &= \sum_{p,n,k=1}^M \sum_{l,m=1}^d e_{il}^k \rho_{lm} e_{jm}^{k*} u_{np} u_{kp}^* \\ &= \sum_{p,n,k=1}^M \sum_{l,m=1}^d e_{il}^k \rho_{lm} e_{jm}^{n*} u_{np} u_{kp}^* \\ &= \sum_{p=1}^M \sum_{l,m=1}^d f_{il}^p \rho_{lm} f_{jm}^{p*} \\ &= \sum_{p=1}^{\text{rank} W} \sum_{l,m=1}^d f_{il}^p \rho_{lm} f_{jm}^{p*} \end{aligned}$$

となるので,  $f_{ij}^k$  を行列要素として持つ

$$\mathcal{F}_k : \text{Map}(\mathbb{C}^{\text{rank} W}, \mathbb{C}^{\text{rank} W}) \rightarrow \text{Map}(\mathbb{C}^{\text{rank} W}, \mathbb{C}^{\text{rank} W})$$

を定義すると,

$$\mathcal{E}(\rho) = \sum_{p=1}^{\text{rank} W} \mathcal{F}_p \rho \mathcal{F}_p^\dagger.$$

演習 8.11 演習 8.10 で,

$$W_{jk} = \text{tr} \left( E_j^\dagger E_k \right)$$

なる行列  $W$  の rank が  $dd'$  以下になるところ以外は全く同様.

演習 8.12 行列  $M$  の極分解

$$M = U|M|$$

に対して,  $U$  は直交行列なので行列式が  $\pm 1$  に限られる. そこで,

$$\begin{aligned} \det U = 1 &\rightarrow O = U, \quad S = |M| \\ \det U = -1 &\rightarrow O = -U, \quad S = -|M| \end{aligned}$$

とすることで, 行列式が 1 であるように  $O$  を取ることができて,

$$M = OS$$

と書ける.

演習 8.13 演習 4.8 より明らか.

演習 8.14 演習 8.12 で見たように,  $\det S$  は正とは限らない.

演習 8.15

$$\begin{aligned} X|\pm\rangle &= \pm|\pm\rangle \\ Y|\pm\rangle &= \mp i|\mp\rangle \\ Z|\pm\rangle &= |\mp\rangle \end{aligned}$$

なので,

$$\rho = \frac{I + \mathbf{r} \cdot \boldsymbol{\sigma}}{2}$$

に対して,

$$\langle \pm | \rho | \pm \rangle = \frac{I + \langle \pm | \mathbf{r} \cdot \boldsymbol{\sigma} | \pm \rangle}{2} = \frac{I \pm r_x}{2}.$$

したがって,

$$\mathcal{E}(\rho) = \sum_{i=\pm} |i\rangle \langle i| \rho |i\rangle \langle i| = \frac{1+r_x}{2} |+\rangle \langle +| + \frac{1-r_x}{2} |-\rangle \langle -| = \frac{I + r_x X}{2}$$

なので, この量子演算の作用を Bloch 球面上で表すと,

$$\mathbf{r} = \begin{pmatrix} r_x \\ r_y \\ r_z \end{pmatrix} \longrightarrow \mathbf{r}' = \begin{pmatrix} r_x \\ 0 \\ 0 \end{pmatrix}.$$

演習 8.16  $p \neq 0$  として,

$$E_0 = \sqrt{1-p} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

とする. 演算集合  $\{E_0\}$  で定義される量子演算はトレース非保存で,

$$\mathcal{E}(\rho) = E_0 \rho E_0^\dagger = (1-p)X\rho X = \frac{1-p}{2}I + \frac{1-p}{2}(r_x X - r_y Y - r_z Z)$$

となる. これは Bloch 球表示できない.

演習 8.17

$$\mathcal{E}(A) = \frac{A + XAX + YAY + ZAZ}{4}$$



として,

$$\mathcal{E}(I) = I, \mathcal{E}(X) = \mathcal{E}(Y) = \mathcal{E}(Z)$$

なので,

$$\rho = \frac{I + \mathbf{r} \cdot \boldsymbol{\sigma}}{2}$$

に対して,

$$\mathcal{E}(\rho) = \frac{1}{2}\mathcal{E}(I) = \frac{I}{2}.$$

演習 8.18 量子演算  $\mathcal{E}$ ;

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$$

は,

$$\sum_k E_k^\dagger E_k \leq I$$

を満たす演算要素  $\{E_k\}$  で定義される. したがって,

$$\text{tr}[\mathcal{E}(\rho^n)] = \sum_k \text{tr}[E_k \rho^n E_k^\dagger] = \sum_k \text{tr}[\rho^n E_k^\dagger E_k] \leq \text{tr}(\rho^n).$$

演習 8.19  $\rho$  を対角化する  $d$  次元 Hilbert 空間の正規直交基底  $\{|1\rangle, |2\rangle, \dots, |d\rangle\}$  とすると,

$$\frac{I}{d} = \frac{1}{d} \sum_i |i\rangle \langle i| \text{tr} \rho = \frac{1}{d} \sum_{i,j} |i\rangle \langle i| \langle j| \rho |j\rangle = \frac{1}{d} \sum_{i,j} |i\rangle \langle j| \rho |j\rangle \langle i|$$

なので,

$$\begin{aligned} \mathcal{E}(\rho) &= p \frac{I}{d} + (1-p)\rho \\ &= \frac{p}{d} \sum_{i,j} |i\rangle \langle j| \rho |j\rangle \langle i| + (1-p) \sum_{i,j} |j\rangle \langle j| \rho |i\rangle \langle i| \\ &= \frac{p}{d} \sum_{i,j} |i\rangle \langle j| \rho |j\rangle \langle i| + (1-p) \sum_i |i\rangle \langle i| \rho |i\rangle \langle i| \\ &= \frac{p}{d} \sum_{i \neq j} |i\rangle \langle j| \rho |j\rangle \langle i| + \left(1 - \frac{d-1}{d}p\right) \sum_i |i\rangle \langle i| \rho |i\rangle \langle i| \end{aligned}$$

なので, 演算要素は,

$$\left\{ \sqrt{\frac{p}{d}} |i\rangle \langle j| \middle| 1 \leq i, j \leq d, i \neq j \right\} + \left\{ \sqrt{1 - \frac{d-1}{d}p} |i\rangle \langle i| \middle| 1 \leq i \leq d \right\}.$$

演習 8.20 問題の図の回路の作用  $U$  として,

$$U \equiv C_1[X] C_2[R_y(\theta)] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \\ 0 & 0 & \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

第 1qubit の初期状態  $\rho_{\text{in}}$  を

$$\rho_{\text{in}} = \begin{pmatrix} a & b \\ b^* & c \end{pmatrix}$$

として, 初期状態は,

$$\rho_{\text{in}} \otimes |0\rangle\langle 0| = \begin{pmatrix} a & 0 & b & 0 \\ 0 & 0 & 0 & 0 \\ b^* & 0 & c & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

ゆえに, 終状態は,

$$U\rho_{\text{in}} \otimes |0\rangle\langle 0| U^\dagger = \begin{pmatrix} a & b \sin \frac{\theta}{2} & b \cos \frac{\theta}{2} & 0 \\ b^* \sin \frac{\theta}{2} & c \sin^2 \frac{\theta}{2} & c \sin \frac{\theta}{2} \cos \frac{\theta}{2} & 0 \\ b^* \cos \frac{\theta}{2} & c \sin \frac{\theta}{2} \cos \frac{\theta}{2} & c \cos^2 \frac{\theta}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

したがって, 第 1qubit の終状態  $\rho_{\text{out}}$  は,

$$\rho_{\text{out}} = \text{tr}_{\text{2nd qubit}} [U\rho_{\text{in}} \otimes |0\rangle\langle 0| U^\dagger] = \begin{pmatrix} a + c \sin^2 \frac{\theta}{2} & b \cos \frac{\theta}{2} \\ b^* \cos \frac{\theta}{2} & c \cos^2 \frac{\theta}{2} \end{pmatrix}.$$

演習 8.22 より,

$$\rho_{\text{out}} = \mathcal{E}_{\text{AD}}(\rho_{\text{in}} \otimes |0\rangle\langle 0|).$$

演習 8.21 (1)

(2)

$$\begin{aligned} \sum_{k=0}^{\infty} E_k^\dagger E_k &= \sum_{k=0}^{\infty} \sum_{l=k}^{\infty} \sum_{m=k}^{\infty} \sqrt{l C_k} \sqrt{m C_k} \sqrt{(1-\gamma)^{l-k} \gamma^k} \sqrt{(1-\gamma)^{m-k} \gamma^k} |l\rangle\langle l-k| m-k\rangle\langle m| \\ &= \sum_{k=0}^{\infty} \sum_{m=k}^{\infty} m C_k (1-\gamma)^{l-k} \gamma^k |m\rangle\langle m| \end{aligned}$$

なので, 全ての  $|n\rangle$  に対して,

$$\sum_{k=0}^{\infty} E_k^\dagger E_k |n\rangle = \sum_{k=0}^{\infty} \sum_{m=k}^{\infty} m C_k (1-\gamma)^{l-k} \gamma^k |m\rangle\langle m|n\rangle = \sum_{k=0}^{\infty} n C_k (1-\gamma)^{l-k} \gamma^k |n\rangle = |n\rangle$$

だから,

$$\sum_{k=0}^{\infty} E_k^\dagger E_k = I.$$

演習 8.22 振幅ダンピングの演算要素;

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, E_1 = \begin{pmatrix} 1 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$$

として,

$$\mathcal{E}_{\text{AD}}(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger = \begin{pmatrix} a + (1-a)\gamma & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & c(1-\gamma) \end{pmatrix}$$

演習 8.23 振幅ダンピングの演算要素;

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, E_1 = \begin{pmatrix} 1 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$$

とする. 単一 qubit の初期状態が 2 重軌道 qubit;

$$\rho = |\psi\rangle\langle\psi| = |a|^2 |01\rangle\langle 01| + ab^* |01\rangle\langle 10| + a^*b |10\rangle\langle 01| + |b|^2 |10\rangle\langle 10|$$

でかけるとする. すると,

$$\begin{aligned} (\mathcal{E}_{\text{AD}} \otimes I)(\rho) &= |a|^2 |0\rangle\langle 0| \otimes |1\rangle\langle 1| + a^*b\sqrt{1-\gamma} |1\rangle\langle 0| \otimes |0\rangle\langle 1| + ab^*\sqrt{1-\gamma} |0\rangle\langle 0| \otimes |1\rangle\langle 0| \\ &\quad + |b|^2 (1-\gamma) |1\rangle\langle 1| \otimes |0\rangle\langle 0| + \gamma |b|^2 |0\rangle\langle 0| \otimes |0\rangle\langle 0| \end{aligned}$$

となり,

$$\begin{aligned} (\mathcal{E}_{\text{AD}} \otimes \mathcal{E}_{\text{AD}})(\rho) &= |a|^2 (1-\gamma) |0\rangle\langle 0| \otimes |1\rangle\langle 1| + a^*b(1-\gamma) |1\rangle\langle 0| \otimes |0\rangle\langle 1| + ab^*(1-\gamma) |0\rangle\langle 0| \otimes |1\rangle\langle 0| \\ &\quad + |b|^2 (1-\gamma) |1\rangle\langle 1| \otimes |0\rangle\langle 0| + \gamma |b|^2 |0\rangle\langle 0| \otimes |0\rangle\langle 0| + \gamma |a|^2 |0\rangle\langle 0| \otimes |0\rangle\langle 0|. \end{aligned}$$

つまり,

$$(\mathcal{E}_{\text{AD}} \otimes \mathcal{E}_{\text{AD}})(\rho) = (1-\gamma)\rho + \gamma |0\rangle\langle 0| \otimes |0\rangle\langle 0| = E_0^{\text{dr}} \rho E_0^{\text{dr}} + E_1^{\text{dr}} \rho E_1^{\text{dr}}.$$

演習 8.24 振幅ダンピングの演算要素

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, E_1 = \begin{pmatrix} 1 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$$

とする.  $\delta = 0$  の Jaynes-Cummings 相互作用の時間発展  $U$

$$U = |0\rangle\langle 0| \otimes |0\rangle\langle 0| + \cos gt (|0\rangle\langle 0| \otimes |1\rangle\langle 1| + |1\rangle\langle 1| \otimes |0\rangle\langle 0|) - i \sin gt (|0\rangle\langle 1| \otimes |1\rangle\langle 0| + |1\rangle\langle 0| \otimes |0\rangle\langle 1|)$$

で, 初期状態は  $\rho = |\text{field}\rangle\langle\text{field}| \otimes |\text{atom}\rangle\langle\text{atom}| = |0\rangle\langle 0| \otimes |1\rangle\langle 1|$  とすると,

$$\begin{aligned} \mathcal{E}(\rho) &= \text{tr}_{\text{field}} [U \rho U^\dagger] \\ &= \text{tr}_{\text{field}} [\cos^2 gt |0\rangle\langle 0| \otimes |1\rangle\langle 1| + \sin^2 gt |1\rangle\langle 1| \otimes |0\rangle\langle 0|] \\ &= \cos^2 gt |1\rangle\langle 1| + \sin^2 gt |0\rangle\langle 0| \\ &= E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger. \end{aligned}$$

最後の等式では,  $\gamma = \sin^2 gt$  とした.

演習 8.25

$$p = \frac{e^{-\beta E_0}}{e^{-\beta E_0} + e^{-\beta E_1}}$$

を  $\beta$  について解いて,

$$\beta = \frac{\log \frac{p}{1-p}}{E_1 - E_0}$$

演習 8.26 問題の図の回路の作用  $U$  として,

$$U \equiv C_1 [R_y(\theta)] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ 0 & 0 & \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix}.$$

第 1qubit の初期状態  $\rho_{\text{in}}$  を

$$\rho_{\text{in}} = \begin{pmatrix} a & b \\ b^* & c \end{pmatrix}$$

として, 初期状態は,

$$\rho_{\text{in}} \otimes |0\rangle\langle 0| = \begin{pmatrix} a & 0 & b & 0 \\ 0 & 0 & 0 & 0 \\ b^* & 0 & c & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

ゆえに, 終状態は,

$$U \rho_{\text{in}} \otimes |0\rangle\langle 0| U^\dagger = \begin{pmatrix} a & 0 & b \cos \frac{\theta}{2} & b \sin \frac{\theta}{2} \\ 0 & 0 & 0 & 0 \\ b^* \cos \frac{\theta}{2} & 0 & c \cos^2 \frac{\theta}{2} & c \sin \frac{\theta}{2} \cos \frac{\theta}{2} \\ b^* \sin \frac{\theta}{2} & 0 & c \sin \frac{\theta}{2} \cos \frac{\theta}{2} & c \sin^2 \frac{\theta}{2} \end{pmatrix}.$$

したがって, 第 1qubit の終状態  $\rho_{\text{out}}$  は,

$$\rho_{\text{out}} = \text{tr}_{\text{2nd qubit}} [U \rho_{\text{in}} \otimes |0\rangle\langle 0| U^\dagger] = \begin{pmatrix} a & b \cos \frac{\theta}{2} \\ b^* \cos \frac{\theta}{2} & c \end{pmatrix}.$$

一方, 位相ダンピングの演算要素

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}, E_1 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{pmatrix}$$

として,

$$E_0 \rho_{\text{in}} E_0^\dagger + E_1 \rho_{\text{in}} E_1^\dagger = \begin{pmatrix} a & b \sqrt{1-\lambda} \\ b^* \sqrt{1-\lambda} & c \end{pmatrix}.$$

ゆえに,  $\lambda = \sin^2 \frac{\theta}{2}$  として,

$$\rho_{\text{out}} = E_0 \rho_{\text{in}} E_0^\dagger + E_1 \rho_{\text{in}} E_1^\dagger.$$

演習 8.27

$$u = \begin{pmatrix} \sqrt{\alpha} & \frac{\sqrt{\alpha}(1-\sqrt{1-1-\lambda})}{\sqrt{\lambda}} \\ \frac{\sqrt{1-\alpha}}{\sqrt{1-\alpha}} & -\frac{\sqrt{1-\alpha}(1+\sqrt{1-1-\lambda})}{\sqrt{\lambda}} \end{pmatrix}.$$

演習 8.28

演習 8.29 振幅ダンピング

$$\mathcal{E}(I) = E_0 E_0^\dagger + E_1 E_1^\dagger = \begin{pmatrix} 1+\gamma & 0 \\ 0 & 1-\gamma \end{pmatrix}$$

位相ダンピング, 分極解消

$$\mathcal{E}(I) = I$$

演習 8.30 初期状態  $\rho_{\text{init}}$  は,

$$\rho_{\text{init}} = \begin{pmatrix} a & b \\ b^* & 1-a \end{pmatrix}.$$

コヒーレンス劣化を考えると, 時刻  $t$  での状態は,

$$\rho(t) = \begin{pmatrix} (a - a_0)e^{-\frac{t}{T_1}} + a_0 & be^{-\frac{t}{T_2}} \\ b^*e^{-\frac{t}{T_2}} & -(a - a_0)e^{-\frac{t}{T_1}} + 1 - a_0 \end{pmatrix}. \quad (\star)$$

振幅ダンピング (AD) によるコヒーレンス劣化

式 (8.112) より,

$$\mathcal{E}_{\text{AD}}(\rho_{\text{init}}) = \begin{pmatrix} 1 - (1 - a)(1 - \gamma) & b\sqrt{1 - \gamma} \\ b^*\sqrt{1 - \gamma} & (1 - a)(1 - \gamma) \end{pmatrix}$$

で,  $\sqrt{1 - \gamma} = e^{-\frac{t}{T_2}}$  とすると,

$$\mathcal{E}_{\text{AD}}(\rho_{\text{init}}) = \begin{pmatrix} 1 - (1 - a)e^{-\frac{2t}{T_2}} & be^{-\frac{t}{T_2}} \\ b^*e^{-\frac{t}{T_2}} & (1 - a)e^{-\frac{2t}{T_2}} \end{pmatrix}$$

この式と  $(\star)$  で  $a_0 = 1$  とした式を比べて,

$$T_1 = \frac{T_2}{2}.$$

振幅ダンピング (AD) と位相ダンピング (PD) 両方によるコヒーレンス劣化

$$\mathcal{E}_{\text{PD}}(\mathcal{E}_{\text{AD}}(\rho_{\text{init}})) = \begin{pmatrix} 1 - (1 - \gamma_{\text{AD}})(1 - a) & b\sqrt{1 - \lambda_{\text{PD}}}\sqrt{1 - \gamma_{\text{AD}}} \\ b^*\sqrt{1 - \lambda_{\text{PD}}}\sqrt{1 - \gamma_{\text{AD}}} & (1 - \gamma_{\text{AD}})(1 - a) \end{pmatrix}$$

で,

$$1 - \gamma_{\text{AD}} = e^{-\frac{t}{T_1}}, \quad \sqrt{1 - \lambda_{\text{PD}}}\sqrt{1 - \gamma_{\text{AD}}} = e^{-\frac{t}{T_2}}$$

とすると  $(\star)$  で  $a_0 = 1$  とした式に一致する. このとき,

$$e^{-\frac{t}{T_2}} = \sqrt{1 - \lambda_{\text{PD}}}\sqrt{1 - \gamma_{\text{AD}}} = \sqrt{1 - \lambda_{\text{PD}}}e^{-\frac{t}{2T_1}} \leq e^{-\frac{t}{2T_1}} \rightarrow T_1 \geq \frac{T_2}{2}.$$

**演習 8.31** 考える系の Hamiltonian;

$$H = \chi a^\dagger a (b + b^\dagger) = \chi N_a (b + b^\dagger)$$

の時間発展演算子  $U$  は,

$$U = e^{-iHt} = e^{-i\chi t N_a (b + b^\dagger)}.$$

ここで,

$$[-i\chi t N_a b^\dagger, -i\chi t N_a b] = (\chi t)^2 N_a$$

であることと, Baker-Campbell-Hausdorf の公式;

$$[A, B] = \text{c number} \rightarrow e^{A+B} = e^{-\frac{\zeta}{2}} e^A e^B$$

を用いて,

$$U = e^{-i\chi t N_a (b + b^\dagger)} = e^{-\frac{(\chi t)^2}{2} N_a^2} e^{-i\chi t N_a b^\dagger} e^{i\chi t N_a b}.$$

系の初期状態  $|\psi_0\rangle = |\text{system}\rangle \otimes |\text{environment}\rangle$  を

$$|\psi_0\rangle = \sum_n c_n |n\rangle \otimes |0\rangle$$

とすると、時刻  $t$  での系の状態は、

$$\begin{aligned} U|\psi_0\rangle &= \sum_n c_n e^{-\frac{(\chi t)^2}{2} N_a^2} e^{-i\chi t N_a b^\dagger} e^{i\chi t N_a b} |n\rangle \otimes |0\rangle \\ &= \sum_n c_n e^{-\frac{(\chi t)^2}{2} N_a^2} e^{-i\chi t N_a b^\dagger} |n\rangle \otimes |0\rangle \\ &= \sum_n \sum_k c_n e^{-\frac{(\chi t)^2}{2} N_a^2} \frac{(-i\chi t N_a b^\dagger)^k}{k!} |n\rangle \otimes |0\rangle \\ &= \sum_n \sum_k c_n e^{-\frac{(\chi t)^2}{2} N_a^2} \frac{(-i\chi t n)^k}{\sqrt{k!}} |n\rangle \otimes |k\rangle \\ &= \sum_n \sum_k c_n e^{-\frac{(\chi t)^2}{2} n^2} \frac{(-i\chi t n)^k}{\sqrt{k!}} |n\rangle \otimes |k\rangle \end{aligned}$$

となる。時刻  $t$  での系の状態を密度行列  $\rho$  でかくと、

$$\rho = U |\psi_0\rangle \langle \psi_0| U^\dagger = \sum_{n,m} \sum_{k,l} c_n c_m^* e^{\frac{(\chi t)^2}{2} (n^2 + m^2)} \frac{(-i\chi t n)^k}{\sqrt{k!}} \frac{(i\chi t m)^l}{\sqrt{l!}} |n\rangle \langle m| \otimes |k\rangle \langle l|.$$

よって、時刻  $t$  での主システムの状態は、

$$\begin{aligned} \text{tr}_{\text{env}} \rho &= \sum_{n,m} \sum_k c_n c_m^* e^{-\frac{(\chi t)^2}{2} (n^2 + m^2)} \frac{(-i\chi t n)^k}{\sqrt{k!}} \frac{(i\chi t m)^k}{\sqrt{k!}} |n\rangle \langle m| \\ &= \sum_{n,m} c_n c_m^* e^{-\frac{(\chi t)^2}{2} (n^2 + m^2)} e^{\chi t m n} |n\rangle \langle m| \\ &= \sum_{n,m} c_n c_m^* e^{-\frac{(\chi t)^2}{2} (n^2 + m^2)} e^{(\chi t)^2 m n} |n\rangle \langle m| \\ &= \sum_{n,m} c_n c_m^* e^{-\frac{(\chi t)^2}{2} (m-n)^2} |n\rangle \langle m|. \end{aligned}$$

## 第 9 章

# 量子情報の距離測度

演習 9.1  $1/2, 1/4$

演習 9.2

$$D((p, 1-p), (q, 1-q)) = \frac{2|p-q|}{2} = |p-q|$$

演習 9.3  $\frac{1}{\sqrt{2}}, \frac{4\sqrt{6}+\sqrt{3}}{12}$

演習 9.4

$$\begin{aligned} D(p_x, q_x) &= \frac{1}{2} \sum_x |p_x - q_x| = \frac{1}{2} \sum_{\{x|p_x \leq q_x\}} |p_x - q_x| + \frac{1}{2} \sum_{\{x|p_x > q_x\}} |p_x - q_x| \\ &= \frac{1}{2} \sum_{\{x|p_x \leq q_x\}} q_x - p_x + \frac{1}{2} \sum_{\{x|p_x > q_x\}} p_x - q_x \\ &= \frac{1}{2} \left( 1 - \sum_{\{x|p_x > q_x\}} q_x \right) - \frac{1}{2} \left( 1 - \sum_{\{x|p_x > q_x\}} p_x \right) + \frac{1}{2} \sum_{\{x|p_x > q_x\}} p_x - q_x \\ &= \sum_{\{x|p_x > q_x\}} p_x - q_x = \max_S \left( \sum_{x \in S} p_x - \sum_{x \in S} q_x \right). \end{aligned}$$

$D(p_x, q_x) = D(q_x, p_x)$  なので,

$$D(p_x, q_x) = \max_S \left( \sum_{x \in S} p_x - \sum_{x \in S} q_x \right) = \max_S \left( \sum_{x \in S} q_x - \sum_{x \in S} p_x \right) = \max_S \left| \sum_{x \in S} p_x - \sum_{x \in S} q_x \right|.$$

演習 9.5 演習 9.4 参照.

演習 9.6  $\frac{1}{2}, \frac{\sqrt{13}}{12}$

演習 9.7  $\rho - \sigma$  は Hermite なので, 対角化可能で, 固有状態は互いに直交する.  $\rho - \sigma$  の固有値を  $\lambda_i$  とすると,

$$\rho - \sigma = \sum_i \lambda_i |i\rangle \langle i| = \sum_{\{i|\lambda_i > 0\}} \lambda_i |i\rangle \langle i| + \sum_{\{i|\lambda_i < 0\}} \lambda_i |i\rangle \langle i| = \sum_{\{i|\lambda_i > 0\}} \lambda_i |i\rangle \langle i| - \sum_{\{i|-\lambda_i > 0\}} -\lambda_i |i\rangle \langle i| = Q - S.$$

ここで,

$$Q = \sum_{\{i|\lambda_i > 0\}} \lambda_i |i\rangle \langle i|, \quad S = \sum_{\{i|-\lambda_i > 0\}} -\lambda_i |i\rangle \langle i|$$

で,  $Q, S$  の固有空間のそれぞれの任意の元は互いに直交する.

演習 9.8 式 (9.22) より, ある直交射影オペレータ  $P$  が存在して,

$$\begin{aligned} D\left(\sum_i p_i \rho_i, \sigma\right) &= \operatorname{tr}\left(P\left(\sum_i p_i \rho_i - \sigma\right)\right) \\ &= \sum_i p_i \operatorname{tr}(P \rho_i) - \sum_i p_i \operatorname{tr}(P \sigma) \\ &= \sum_i p_i (\operatorname{tr}(P(\rho_i - \sigma))) \\ &\leq \sum_i p_i D(\rho_i, \sigma) \end{aligned}$$

演習 9.9

演習 9.10 厳密に収縮的な  $\mathcal{E}$  が 2 つの不動点を持つとすると,

$$\mathcal{E}(\rho) = \rho, \mathcal{E}(\sigma) = \sigma$$

となるが,

$$D(\rho, \sigma) = D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) < D(\rho, \sigma)$$

と矛盾.

演習 9.11 同時凸性より,

$$\begin{aligned} D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) &= D(p\rho_0 + (1-p)\mathcal{E}'(\rho), p\rho_0 + (1-p)\mathcal{E}'(\sigma)) \\ &\leq pD(\rho_0, \rho_0) + (1-p)D(\mathcal{E}'(\rho), \mathcal{E}'(\sigma)) \\ &= (1-p)D(\mathcal{E}'(\rho), \mathcal{E}'(\sigma)) \\ &\geq (1-p)D(\rho, \sigma) \\ &< D(\rho, \sigma). \end{aligned}$$

演習 9.12

$$\rho = \frac{I + \mathbf{r} \cdot \boldsymbol{\sigma}}{2}, \sigma = \frac{I + \mathbf{s} \cdot \boldsymbol{\sigma}}{2}$$

として,

$$\mathcal{E}(\rho) = \frac{I + (1-p)\mathbf{r} \cdot \boldsymbol{\sigma}}{2}, \mathcal{E}(\sigma) = \frac{I + (1-p)\mathbf{s} \cdot \boldsymbol{\sigma}}{2}$$

なので,

$$D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) = (1-p) \frac{|\mathbf{r} - \mathbf{s}|}{2} < \frac{|\mathbf{r} - \mathbf{s}|}{2} = D(\rho, \sigma)$$

演習 9.13 ビット反転チャンネルの量子演算は,

$$\rho = \frac{I + \mathbf{r} \cdot \boldsymbol{\sigma}}{2}, \sigma = \frac{I + \mathbf{s} \cdot \boldsymbol{\sigma}}{2}$$

として,

$$\begin{aligned} \mathcal{E}(\rho) &= \frac{I + (1-p)X\rho X}{2} = \frac{I + r_1X + (2p-1)r_2Y + (2p-1)r_3Z}{2} \\ \mathcal{E}(\sigma) &= \frac{I + s_1X + (2p-1)s_2Y + (2p-1)s_3Z}{2} \end{aligned}$$



なので,

$$D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) = \sqrt{(r_1 - s_1)^2 + (2p - 1)^2(r_2 - s_2)^2 + (2p - 1)^2(r_3 - s_3)^2}.$$

よって,

$$D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq D(\rho, \sigma).$$

等号は, 実数  $t$  として,

$$\mathbf{r} = \mathbf{s} = t \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

の時に成立する. 不動点の集合は, 実数  $t$  として,

$$\mathbf{r} = t \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

演習 9.14 正值オペレータ  $A$  はスペクトル分解可能で,

$$A = \sum_i \lambda_i |i\rangle \langle i|$$

とかけ, ユニタリ  $U$  を用いて

$$\sqrt{UAU^\dagger} = \sqrt{\sum_i \lambda_i U |i\rangle \langle i| U^\dagger} = \sum_i \sqrt{\lambda_i} U |i\rangle \langle i| U^\dagger = U \sqrt{A} U^\dagger$$

が成立する. このことを用いて,

$$\begin{aligned} F(U\rho U^\dagger, U\sigma U^\dagger) &= \text{tr} \sqrt{\sqrt{U\rho U^\dagger} U \sigma U^\dagger \sqrt{U\rho U^\dagger}} \\ &= \text{tr} \sqrt{U \sqrt{\rho} U^\dagger U \sigma U^\dagger U \sqrt{\rho} U^\dagger} \\ &= \text{tr} \sqrt{U \sqrt{\rho} \sigma \sqrt{\rho} U^\dagger} \\ &= \text{tr} U \sqrt{\sqrt{\rho} \sigma \sqrt{\rho}} U^\dagger \\ &= \text{tr} \sqrt{\sqrt{\rho} \sigma \sqrt{\rho}} \\ &= F(\rho, \sigma) \end{aligned}$$

演習 9.15 定理 9.4 と同様.

演習 9.16

$$\begin{aligned} \langle m | A \otimes B | m \rangle &= \sum_{i,j} \langle i_R | \langle i_Q | A \otimes B | j_R \rangle | j_Q \rangle \\ &= \sum_{i,j} \langle i_R | A | j_R \rangle \langle i_Q | B | j_Q \rangle \\ &= \sum_{i,j} \langle j_R | A^\dagger | i_R \rangle^* \langle i_Q | B | j_Q \rangle \\ &= \text{tr} [A^\top B] \end{aligned}$$

演習 9.17  $0 \leq F(\rho, \sigma) \leq 1$  なので,

$$0 \leq A(\rho, \sigma) = \arccos F(\rho, \sigma) \leq \frac{\pi}{2}$$

で, 左の等号の成立は,

$$F(\rho, \sigma) = 1 \leftrightarrow \rho = \sigma$$

演習 9.18 定理 9.6 と  $\arccos$  の単調性より示せる.

演習 9.19 定理 9.7 より,

$$F\left(\sum_i p_i \rho_i, \sum_i p_i \sigma_i\right) \geq \sum_i p_i F(\rho_i, \sigma_i)$$

演習 9.20 演習 9.19 で, 全ての  $i$  に対して,

$$\sigma_i = \sigma$$

とすれば,

$$F\left(\sum_i p_i \rho_i, \sigma\right) \geq \sum_i p_i F(\rho_i, \sigma).$$

演習 9.21 POVM として,

$$\{E_1 = |\psi\rangle\langle\psi|, E_2 = I - |\psi\rangle\langle\psi|\}$$

を考える. すると, 定理 9.1 より,

$$\begin{aligned} D(|\psi\rangle, \sigma) &\geq \frac{1}{2} |\operatorname{tr}(|\psi\rangle\langle\psi| E_1) - \operatorname{tr}(\sigma E_1)| + \frac{1}{2} |\operatorname{tr}(|\psi\rangle\langle\psi| E_2) - \operatorname{tr}(\sigma E_2)| \\ &= \frac{1}{2} (1 - \operatorname{tr}(\sigma E_1) + \operatorname{tr}(\sigma E_2)) = 1 - \operatorname{tr}(\sigma E_1) = 1 - \langle\psi|\sigma|\psi\rangle = 1 - F(|\psi\rangle, \sigma)^2. \end{aligned}$$

演習 9.22 ある  $\rho$  が存在して,

$$\begin{aligned} E(VU, \mathcal{F} \circ \mathcal{E}) &= d(VU\rho U^\dagger V^\dagger, (\mathcal{F} \circ \mathcal{E})(\rho)) \\ &\leq d(VU\rho U^\dagger V^\dagger, \mathcal{F}(U\rho U^\dagger)) + d(\mathcal{F}(U\rho U^\dagger), (\mathcal{F} \circ \mathcal{E})(\rho)) \\ &\leq d(VU\rho U^\dagger V^\dagger, \mathcal{F}(U\rho U^\dagger)) + d(U\rho U^\dagger, \mathcal{E}(\rho)) \\ &\leq E(V, \mathcal{F}) + E(U, \mathcal{E}). \end{aligned}$$

演習 9.23  $0 \leq F \leq 1$  に注意して,

$$\begin{aligned} \bar{F} = 1 &\longleftrightarrow \sum_j p_j \left(1 - F(\rho_j, \mathcal{E}(\rho_j))\right)^2 = 0 \\ &\longleftrightarrow 1 - F(\rho_j, \mathcal{E}(\rho_j))^2 = 0 \\ &\longleftrightarrow F(\rho_j, \mathcal{E}(\rho_j)) = 1 \\ &\longleftrightarrow \rho_j = \mathcal{E}(\rho_j). \end{aligned}$$

## 第 10 章

# 量子誤り訂正

$F_2$  は集合  $0, 1$  に通常の 2 進法の加法と乗法を入れた体.

演習 10.1 明らか.

演習 10.2

$$\begin{aligned}\mathcal{E}(\rho) &= (1 - 2p)\rho + 2pP_+\rho P_+ + 2pP_-\rho P_- \\ &= (1 - 2p)\rho + p(|0\rangle\langle 0| + |1\rangle\langle 1|)\rho(|0\rangle\langle 0| + |1\rangle\langle 1|) + p(|0\rangle\langle 1| + |1\rangle\langle 0|)\rho(|0\rangle\langle 1| + |1\rangle\langle 0|) \\ &= (1 - 2p)\rho + P\rho + pX\rho X \\ &= (1 - p)\rho + P\rho + pX\rho X.\end{aligned}$$

演習 10.3 第 3qubit にビット反転が生じた後の状態,  $|\psi\rangle = a|001\rangle + b|110\rangle$  として,  $Z_1Z_2, Z_2Z_3$  を測定すると,

$$\begin{aligned}Z_1Z_2|\psi\rangle &= |\psi\rangle \\ Z_2Z_3|\psi\rangle &= -|\psi\rangle\end{aligned}$$

より, 測定値はそれぞれ  $(1, -1)$ , 測定後の状態  $|\psi\rangle$  となる. 同様に, 第 1qubit, 第 2qubit にビット反転が生じた場合,  $Z_1Z_2, Z_2Z_3$  の測定値は, それぞれ  $(-1, 1)$ ,  $(-1, -1)$ . また, どの qubit にもビット反転が起らないのならば,  $Z_1Z_2, Z_2Z_3$  の測定値は, それぞれ  $(1, 1)$ .

演習 10.4 (1)  $P_0, P_1$  に対応する測定結果が得られればビット反転していない,  $P_{2j}, P_{2j+1}$  に対応する測定結果が得られれば第  $j$  ビットが反転した, と診断できる. (2) 計算基底でないと, error detection により量子状態を壊してしまう. (3) ビット反転が単一 qubit に起こる確率を  $p$  とする. 始状態が純粋状態  $|\psi\rangle$  として, 誤り訂正後の状態  $\rho$  は, (10.11) 式と同様に,

$$\rho = [(1 - p)^3 + 3p(1 - p)^2] |\psi\rangle\langle\psi| + (\text{positive operator})$$

であり, (9.121) より最小忠実度  $F$  は純粋状態について考えれば十分なことから,

$$F = \sqrt{\langle\psi|\rho|\psi\rangle} \geq \sqrt{(1 - p)^3 + 3p(1 - p)^2}.$$

演習 10.5  $X_{1:6} \equiv X_1X_2\dots X_6, X_{4:9} \equiv X_4X_5\dots X_9$  として,

- 位相反転しない場合

$$\begin{aligned}X_{1:6} \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} &= \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \\ X_{4:9} \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} &= \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}\end{aligned}$$

- 第 1qubit が位相反転した場合

$$X_{1:6} \frac{(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} = - \frac{(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

$$X_{4:9} \frac{(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} = \frac{(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

- 第 2qubit が位相反転した場合

$$X_{1:6} \frac{(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} = - \frac{(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

$$X_{4:9} \frac{(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} = - \frac{(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

- 第 3qubit が位相反転した場合

$$X_{1:6} \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}} = \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$

$$X_{4:9} \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}} = - \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$

となり, シンドローム測定としての役割を果たす.

#### 演習 10.6

$$Z_1 Z_2 Z_3 \frac{|000\rangle - |111\rangle}{\sqrt{2}} = \frac{|000\rangle + |111\rangle}{\sqrt{2}}.$$

#### 演習 10.7

$$\alpha_{00} = (1-p)^3, \alpha_{11} = \alpha_{22} = \alpha_{33} = p(1-p)^2, \alpha_{ij} = 0 \ (i \neq j)$$

として,

$$PE_i^\dagger E_j P = \alpha_{ij} P$$

を満たすので, 3qubit ビット反転符号は, 誤り訂正可能.

#### 演習 10.8 計算すると,

$$\alpha_{ij} = \delta_{ij}$$

となり,  $\alpha_{ij}$  は Hermite なので, 量子誤り訂正条件を満たす.

#### 演習 10.9 $I = E_1, P_i = E_{2i}, Q_i = E_{2i+1}$ として, 計算すると,

$$\alpha_{ij} = \begin{pmatrix} 1 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 \\ 1/2 & 1/2 & 0 & 1/4 & 1/4 & 1/4 & 1/4 \\ 1/2 & 0 & 1/2 & 1/4 & 1/4 & 1/4 & 1/4 \\ 1/2 & 1/4 & 1/4 & 1/2 & 0 & 1/4 & 1/4 \\ 1/2 & 1/4 & 1/4 & 0 & 1/2 & 1/4 & 1/4 \\ 1/2 & 1/4 & 1/4 & 1/4 & 1/4 & 1/2 & 0 \\ 1/2 & 1/4 & 1/4 & 1/4 & 1/4 & 0 & 1/2 \end{pmatrix}$$

となり,  $\alpha_{ij}$  は Hermite なので, 量子誤り訂正条件を満たす.

演習 10.10 定理 10.1 の証明と全く同様にやれば良い。

演習 10.11 分極解消チャンネルで  $p = 1$  として, その演算要素は,

$$\left\{ \frac{1}{2}I, \frac{1}{2}X, \frac{1}{2}Y, \frac{1}{2}Z \right\}.$$

演習 10.12 分極解消チャンネル

$$\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$$

に対して,  $\langle 0|X|0\rangle = \langle 0|Y|0\rangle = 0$ ,  $\langle 0|Z|0\rangle = 1$  を用いて,

$$F(|0\rangle, \mathcal{E}(|0\rangle\langle 0|)) = \sqrt{\langle 0|\mathcal{E}(\rho)|0\rangle} = \sqrt{1 - \frac{2p}{3}}.$$

演習 10.13 規格化された純粋状態  $|\psi\rangle = a|0\rangle + b|1\rangle$  に対して, 演習 8.22 より,

$$\mathcal{E}_{AD}(|\psi\rangle\langle\psi|) = \begin{pmatrix} 1 - |b|^2(1-\gamma) & ab^*\sqrt{1-\gamma} \\ a^*b\sqrt{1-\gamma} & |b|^2(1-\gamma) \end{pmatrix}$$

なので,

$$\begin{aligned} F(|\psi\rangle\langle\psi|, \mathcal{E}_{AD}(|\psi\rangle\langle\psi|)) &= \sqrt{\langle\psi|\mathcal{E}_{AD}(|\psi\rangle\langle\psi|)|\psi\rangle} \\ &= \sqrt{|a|^4 - |a|^2|b|^2(1-\gamma) + 2|a|^2|b|^2\sqrt{1-\gamma} + |b|^4(1-\gamma)} \\ &= \sqrt{2\left(1-\gamma-\sqrt{1-\gamma}\right)|a|^4 + \left(1-3(1-\gamma)+2\sqrt{1-\gamma}\right)|a|^2 + 1-\gamma}. \end{aligned}$$

$(1-\gamma-\sqrt{1-\gamma}) \leq 0$  より,  $F(|\psi\rangle\langle\psi|, \mathcal{E}_{AD}(|\psi\rangle\langle\psi|))$  の  $0 \leq |a|^2 \leq 1$  における最小値の候補は,  $|a|^2 = 0, 1$  の時に絞られる. 実際最小値は,  $|a|^2 = 0$  のときの  $\sqrt{1-\gamma}$ . (9.121) 式にあるように, 最小忠実度を考えるのには, 純粋状態を考えれば十分なので, 振幅ダンピングの最小忠実度は  $\sqrt{1-\gamma}$ .

演習 10.14

$$G = \begin{pmatrix} I_{k \times k} \\ I_{k \times k} \\ \vdots \\ I_{k \times k} \end{pmatrix}.$$

演習 10.15 生成行列  $G = (\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k)$ ,  $G' = (\mathbf{g}_1 + \mathbf{g}_2, \mathbf{g}_2, \dots, \mathbf{g}_k)$  を用いて,  $\mathbf{x} = (x_1, \dots, x_k)^\top$  を符号化することを考えると,

$$\begin{aligned} G\mathbf{x} &= \sum_{i=1}^k x_i \mathbf{g}_i \\ G'\mathbf{x} &= (x_1 + x_2) \mathbf{g}_1 + \sum_{i=2}^k x_i \mathbf{g}_i. \end{aligned}$$

よって,

$$\{G\mathbf{x} | \mathbf{x} \in F_2^k\} = \{G'\mathbf{x} | \mathbf{x} \in F_2^k\}.$$

## 演習 10.16 パリティ検査行列

$$H = \begin{pmatrix} \mathbf{y}_1^\top \\ \mathbf{y}_1^\top \\ \vdots \\ \mathbf{y}_{n-k}^\top \end{pmatrix}, \quad H' = \begin{pmatrix} \mathbf{y}_1^\top \\ \mathbf{y}_1^\top + \mathbf{y}_2^\top \\ \vdots \\ \mathbf{y}_{n-k}^\top \end{pmatrix}$$

として,

$$\text{Ker } H = \{ \mathbf{x} \in F_2^k \mid \mathbf{y}_i^\top \mathbf{x} = 0 \ (i = 1, 2, \dots, n-k) \} = \text{Ker } H'.$$

演習 10.17  $G$  の列ベクトルに直交する線型独立なベクトル  $\mathbf{y}_i$  を 4 本取ってきて,  $\mathbf{y}_i$  を転置した横ベクトルたちを行ベクトルとして持つのが, パリティ検査行列  $H$ . 例えば次のようなものが考えられる.

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

演習 10.18  $G$  の各列  $\mathbf{g}_i$ ,  $H$  の各行  $\mathbf{h}_i$  として,

$$(HG)_{ij} = \mathbf{h}_i^\top \mathbf{g}_j = 0.$$

演習 10.19 パリティ検査行列の標準形  $H = (A \mid I_{n-k})$  の  $A$  の各列

$$\mathbf{a}_i = \begin{pmatrix} a_{1,i} \\ a_{2,i} \\ \vdots \\ a_{n-k,i} \end{pmatrix}$$

は互いに線型独立である. したがって,  $\text{Ker } H$  の基底  $\{\mathbf{g}_j\}_{j=1}^k$  として, 第  $j$  成分だけが 1 でそれ以外の成分が 0 のベクトル  $\mathbf{e}_j$  を用いて,

$$\mathbf{g}_j = \begin{pmatrix} \mathbf{e}_j \\ -a_{1,j} \\ -a_{2,j} \\ \vdots \\ -a_{n-k,j} \end{pmatrix}$$

をとることができる. よって, 生成行列は,

$$G = (\mathbf{g}_1, \dots, \mathbf{g}_k) = \begin{pmatrix} I_k \\ -A \end{pmatrix}.$$

演習 10.20 パリティ検査行列  $H = (\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_k)$ , 符号化された状態  $\mathbf{x} = (x_1, \dots, x_k)^\top$  とする.

ある  $\mathbf{x}$  に対して,  $\text{wt } \mathbf{x} \leq d-1$  と仮定すると, ある  $l \leq d-1$  なる  $l$  を用いて,

$$H\mathbf{x} = \sum_{i=i_1, i_2, \dots, i_l} \mathbf{h}_i$$

となるが,  $\mathbf{h}_{i_1}, \dots, \mathbf{h}_{i_l}$  は互いに線型独立なので,  $H\mathbf{x} = \mathbf{0}$  になりえず, 矛盾. よって, 全ての  $\mathbf{x}$  に対して,  $\text{wt } \mathbf{x} \geq d$ .

ある  $(i_1, \dots, i_{d-1}, i_d)$  の組に対して,  $\mathbf{h}_{i_1}, \dots, \mathbf{h}_{i_{d-1}}, \mathbf{h}_{i_d}$  が線型従属になり, どの  $d$  本も線型独立なので,

$$\mathbf{h}_{i_d} = \mathbf{h}_{i_1} + \dots + \mathbf{h}_{i_{d-1}}.$$

よって, 成分  $i = i_1, i_2, \dots, i_d$  が 1 になる  $\mathbf{x}$ , つまり  $\text{wt } \mathbf{x} = d$  となる  $\mathbf{x}$  が,

$$H\mathbf{x} = \sum_{i=i_1, i_2, \dots, i_d} \mathbf{h}_i = \mathbf{h}_{i_d} + \mathbf{h}_{i_d} = \mathbf{0}$$

を満たす. つまり,  $\text{wt } \mathbf{x} = d$  を満たす,  $H$  で定義された符号  $\mathbf{x}$  が存在.

以上より,

$$d(H) = d.$$

演習 10.21 演習 10.20 より,

$$d-1 = (H \text{ の任意のベクトルの組が線型独立になるときのそのベクトルの本数の最大値}) \leq \text{rank}(H) = n-k.$$

演習 10.22 Hamming code のどの 2 列を見ても線型独立だが, ある 3 列を見ると線形従属なので, 演習 10.20 より, Hamming code の距離は 3.

演習 10.23  $n > 4t > 0$  のとき,

$$x \log \frac{2t}{n} + (n-x) \log \frac{n-2t}{n}$$

は  $x$  について単調減少なので,

$$\left(\frac{2t}{n}\right)^x \left(\frac{n-2t}{n}\right)^{n-x}$$

も  $x$  について単調減少. すると,  $n > 4t > 0$  のとき,

$$\frac{2^{nH\left(\frac{2t}{n}\right)}}{\sum_{j=0}^t {}_nC_j} = \frac{1}{\sum_{j=0}^t {}_nC_j \left(\frac{2t}{n}\right)^{2t} \left(\frac{n-2t}{n}\right)^{n-2t}} \geq \frac{1}{\sum_{j=0}^{2t} {}_nC_j \left(\frac{2t}{n}\right)^{2t} \left(\frac{n-2t}{n}\right)^{n-2t}} \geq \frac{1}{\sum_{j=0}^{2t} {}_nC_j \left(\frac{2t}{n}\right)^j \left(\frac{n-2t}{n}\right)^{n-j}} = 1$$

が成立するので, 任意の  $n(> 4t > 0)$  に対して,

$$2^{nH\left(\frac{2t}{n}\right)} \geq 2^{n-k} \geq \sum_{j=0}^t {}_nC_j$$

なる  $k$  が存在する. つまり,

$$\left\{ \begin{array}{l} \frac{k}{n} \geq 1 - H\left(\frac{2t}{n}\right) \\ \sum_{j=0}^t {}_nC_j 2^k \leq 2^n \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \frac{k}{n} \geq 1 - H\left(\frac{2t}{n}\right) \\ t \text{ ビット以下の誤りから護る } [n, k] \text{ 符号が存在.} \end{array} \right.$$

を満たす  $k$  が存在する.

演習 10.24

$$C \subseteq C^\perp \longleftrightarrow \forall_{x \in F_2^k} G[C]x \in C^\perp \longleftrightarrow \forall_{x \in F_2^k} H[C^\perp]G[C]x = G^\top[C]G[C]x = 0 \longleftrightarrow G^\top[C]G[C] = O.$$

演習 10.25  $x \in C^\perp$  のとき,

$$\forall_{y \in C} x \cdot y = 0$$

なので,

$$\sum_{y \in C} (-1)^{x \cdot y} = |C|.$$

一方,  $x \notin C^\perp$  のとき,  $C$  の生成行列  $G[C] = (g_1, g_2, \dots, g_k)$  として,  $x \cdot g_i = 0$  となる  $g_i$  が存在するので, ある  $l \geq 1$  が存在して,

$$\begin{aligned} x \cdot g_1 &= \dots = x \cdot g_l = 1 \\ x \cdot g_{l+1} &= \dots = x \cdot g_k = 0 \end{aligned}$$

と書いても, 一般性を失わない. 任意の  $C$  の符号語  $y$  が  $y = G[C]a = \sum_i a_i g_i$  とかけるので,

$$\sum_{y \in C} (-1)^{x \cdot y} = \sum_{a_1, a_2, \dots, a_k=0,1} (-1)^{\sum_i a_i x \cdot g_i} = \sum_{a_1, a_2, \dots, a_l=0,1} (-1)^{a_1 + a_2 + \dots + a_l} = \prod_{i=1}^k \sum_{a_i=0,1} (-1)^{a_i} = 0.$$

演習 10.26 始状態  $|x\rangle|0\rangle$  の  $|x\rangle$  を第 1 レジスタ,  $|0\rangle$  を第 2 レジスタと呼ぶ. パリティ検査行列  $H$  の  $(i, j)$  成分が  $H_{ij}$  が 1 となる  $(i, j)$  に対に対して, 第 1 レジスタの第  $i$  qubit を制御ビットとして, 第 2 レジスタの第  $j$  qubit を反転させるゲートを考えれば良い.

演習 10.27

演習 10.28

$$H[C_1] \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} = O$$

なので,

$$G[C_1] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

演習 10.29 任意の  $g \in S$  に対して,  $|\psi_1\rangle, |\psi_2\rangle \in V_S$  は,

$$g|\psi_1\rangle = |\psi_1\rangle, g|\psi_2\rangle = |\psi_2\rangle$$

であることと,  $g$  の線形性より,

$$g(c_1|\psi_1\rangle + c_2|\psi_2\rangle) = c_1|\psi_1\rangle + c_2|\psi_2\rangle.$$

よって,  $V_S$  の任意の 2 つの要素の線型結合もまた  $V_S$  の要素. 後半の主張については明らか.

演習 10.30

$$-I \notin S \iff (\pm iI)^2 \notin S \iff (\pm iI) \notin S.$$

演習 10.31

←) 明らか.

→) 任意の  $S$  の元が, 互いに可換な  $S$  の生成元での積でかけるので,  $S$  の要素も互いに可換.



演習 10.32 計算すれば良い.

演習 10.33  $r(g)$  の各成分と  $g$  は, ある係数  $c$  を用いて

$$g = c \prod_{i=1}^n X_i^{r_i} Z_i^{r_{n+i}}$$

で対応づけられる. よって,

$$\begin{aligned} [g, g'] = 0 &\longleftrightarrow \prod_{i=1}^n X_i^{r_i} Z_i^{r_{n+i}} X_i^{r'_i} Z_i^{r'_{n+i}} - \prod_{i=1}^n X_i^{r'_i} Z_i^{r'_{n+i}} X_i^{r_i} Z_i^{r_{n+i}} = 0 \\ &\longleftrightarrow \prod_{i=1}^n (-1)^{r'_i r_{n+i}} X_i^{r_i} X_i^{r'_i} Z_i^{r_{n+i}} Z_i^{r'_{n+i}} - \prod_{i=1}^n (-1)^{r_i r'_{n+i}} X_i^{r'_i} X_i^{r_i} Z_i^{r'_{n+i}} Z_i^{r_{n+i}} = 0 \\ &\longleftrightarrow \prod_{i=1}^n (-1)^{r'_i r_{n+i}} = \prod_{i=1}^n (-1)^{r_i r'_{n+i}} \\ &\longleftrightarrow \sum_{i=1}^n r'_i r_{n+i} + r_i r'_{n+i} = 0 \\ &\longleftrightarrow r(g) \Lambda r(g')^\top = 0. \end{aligned}$$

演習 10.34 示すべきは

$$-I \in S \longleftrightarrow \exists_i g_i^2 = -I \text{ または } g_i = -I$$

$\longleftarrow$ ) 明らか.

$\longrightarrow$ )

演習 10.35  $G_n$  は反 Hermite または Hermite を要素にもち, 任意の  $g \in S \subset G_n$  に対して

$$g^2 = \pm I^{\otimes n}$$

なので,

$$-I^{\otimes n} \in S \subset G_n \longrightarrow \forall g = \bigotimes_{i=1,2,\dots,n} g_i \in S \subset G_n \quad g^2 = \bigotimes_{i=1,2,\dots,n} g_i^2 = I^{\otimes n} \text{ かつ } g \neq -I^{\otimes n}$$

であるので,  $\{g_i\}_{i=1}^n$  のうちの偶数個が, 2 乗すると  $-I$  になる反 Hermite であり, 残りが 2 乗すると  $I$  になる Hermite になることが言える. よって,

$$g = \bigotimes_{i=1,2,\dots,n} g_i$$

は Hermite.

演習 10.36 量子回路を考えれば明らか.

演習 10.37

$$UY_1U^\dagger = iUX_1U^\dagger UZ_1U^\dagger = iX_1X_2Z_1 = Y_1Z_2$$

演習 10.38  $\Sigma = X_1, X_2, Z_1, Z_2$  として,

$$U\Sigma U^\dagger = V\Sigma V^\dagger \longleftrightarrow [U^\dagger V, \Sigma] = 0$$

とすると,  $i, j = 0, 1, 2, 3$  に対して,

$$[U^\dagger V, \sigma_i \otimes \sigma_j] = 0$$

なので,  $U^\dagger V$  は任意のオペレータと可換. つまり,  $U^\dagger V = I$ . ゆえに  $U = V$ .

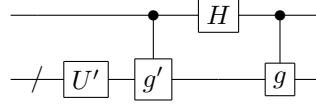
演習 10.39 計算すれば良い.

演習 10.40 (1) グローバルな位相を考えないので,  $G_1$  の要素  $g$  として  $g = X, Y, Z$  だけを考慮して,  $UgU \in G_1$  なる  $U$  が Hadamard ゲート  $H$  と位相ゲート  $S$  でかけることを言えば良い. たとえば  $U = H$  とすると,

$$HXH^\dagger = Z, HYH^\dagger = Y, HZH = X$$

なので, グローバル位相を無視すれば  $HG_1H \in G_1$ .  $U = S$  としても同様.

(2)

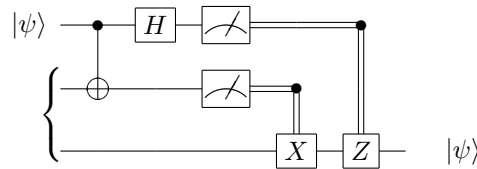


の作用を, 始状態  $|0\rangle \otimes |\psi\rangle + |1\rangle \otimes |\phi\rangle$  として考えると,

$$\begin{aligned} |0\rangle \otimes |\psi\rangle + |1\rangle \otimes |\phi\rangle &\rightarrow |0\rangle \otimes U'|\psi\rangle + |1\rangle \otimes U'|\phi\rangle \\ &\rightarrow |0\rangle \otimes U'|\psi\rangle + |1\rangle \otimes g'U'|\phi\rangle \\ &\rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes U'|\psi\rangle + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes g'U'|\phi\rangle \\ &\rightarrow \frac{|0\rangle \otimes U'|\psi\rangle + |1\rangle \otimes gU'|\psi\rangle}{\sqrt{2}} + \frac{|0\rangle \otimes g'U'|\phi\rangle - |1\rangle \otimes gg'U'|\phi\rangle}{\sqrt{2}} \\ &\rightarrow \frac{(I + X_1 \otimes g)(|0\rangle \otimes U'|\psi\rangle)}{\sqrt{2}} + \frac{(I - X_1 \otimes g)(Z_1 \otimes g')(|0\rangle \otimes U'|\psi\rangle)}{\sqrt{2}} \\ &= \frac{(I + UZ_1U^\dagger)(|0\rangle \otimes U'|\psi\rangle)}{\sqrt{2}} + \frac{(I - UZ_1U^\dagger)UX_1U^\dagger(|0\rangle \otimes U'|\psi\rangle)}{\sqrt{2}} \end{aligned}$$

演習 10.41 計算すれば良い.

演習 10.42



Alice と Bob に分け与える EPR 対を  $|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$  とする. また, Bob に届けたい状態  $|\psi\rangle = |+\rangle$  とする. 上記の量子回路の各ゲートの作用を固定部分群形式で追っていく.

1. 始状態  $|+\rangle |\beta_{00}\rangle$   
 $\langle X \otimes X \otimes I, I \otimes X \otimes X, I \otimes Z \otimes Z \rangle$
2. CNOT 作用後  
 $\langle X \otimes X \otimes I, I \otimes X \otimes X, Z \otimes Z \otimes Z \rangle$

3.  $H$  作用後

$$\langle Z \otimes X \otimes I, I \otimes X \otimes X, X \otimes Z \otimes Z \rangle$$

4. 生成元のうち 1 つだけ  $I \otimes Z \otimes I$  と反可換になるように生成元を取り替える

$$\langle Z \otimes X \otimes I, Z \otimes I \otimes X, X \otimes Z \otimes Z \rangle$$

5. 2qubit 目の測定 ( $M_2$ )

$$\text{if } M_2 = 0, \langle I \otimes Z \otimes I, Z \otimes I \otimes X, X \otimes Z \otimes Z \rangle$$

$$\text{if } M_2 = 1, \langle -I \otimes Z \otimes I, Z \otimes I \otimes X, X \otimes Z \otimes Z \rangle$$

6.  $I \otimes I \otimes X^{M_2}$  作用後

$$\text{if } M_2 = 0, \langle I \otimes Z \otimes I, Z \otimes I \otimes X, X \otimes Z \otimes Z \rangle$$

$$\text{if } M_2 = 1, \langle -I \otimes Z \otimes I, Z \otimes I \otimes X, -X \otimes Z \otimes Z \rangle$$

7. 1qubit 目の測定 ( $M_1$ ) をして,  $I \otimes I \otimes Z^{M_1}$  作用後

$$\text{if } (M_1, M_2) = (0, 0), \langle I \otimes Z \otimes I, Z \otimes I \otimes X, Z \otimes I \otimes I \rangle$$

$$\text{if } (M_1, M_2) = (0, 1), \langle -I \otimes Z \otimes I, Z \otimes I \otimes X, -Z \otimes I \otimes I \rangle$$

$$\text{if } (M_1, M_2) = (1, 0), \langle I \otimes Z \otimes I, -Z \otimes I \otimes X, -Z \otimes I \otimes I \rangle$$

$$\text{if } (M_1, M_2) = (1, 1), \langle -I \otimes Z \otimes I, -Z \otimes I \otimes X, -Z \otimes I \otimes I \rangle$$

終状態の固定部分群の生成元は  $|+\rangle$  を安定化させる.

演習 10.43  $g \in S, |\psi\rangle \in V_S$  とする. すると, 任意の  $h \in S$  に対して,

$$hg|\psi\rangle = h|\psi\rangle = |\psi\rangle = g|\psi\rangle \longrightarrow g^{-1}hg|\psi\rangle = |\psi\rangle \longrightarrow g^{-1}hg \in S$$

なので,  $g \in N(S)$ . つまり,  $S \subset N(S)$ .

演習 10.44  $\longrightarrow$ )

$$g \in N(S) \longrightarrow \forall s \in S \quad gs = sg \longrightarrow gS = Sg \longrightarrow g \in N(S)$$

$\longleftarrow$ )  $g \in N(S)$  とする.  $-I \notin S$  なので,  $S$  の要素はだから,  $\forall s \in S \quad gs = sg$ . よって,  $g \in Z(S)$ .

演習 10.45

演習 10.46  $S = \langle X_1 X_2, X_2 X_3 \rangle$  とすると,  $V_S$  は  $|+++ \rangle$  と  $|- - - \rangle$  で張られる.

演習 10.47  $i = 1, 2, \dots, 8$  に対して,  $g_i |0_L\rangle = |0_L\rangle$ ,  $g_i |1_L\rangle = |1_L\rangle$  を確かめれば良い.

演習 10.48 計算すれば良い.

演習 10.49 例えば,  $X_1 Z_2 \notin N(S) - S$  か調べる.

$$\{X_1 Z_2, g2\} = \{X_1 Z_2, X_2 Z_3 Z_4 X_5\} = \{X_1 Z_2, X_2\} Z_3 Z_4 X_5 = (X_1 Z_2 X_2 + X_2 X_1 Z_2) Z_3 Z_4 X_5 = 0$$

であり,  $l = 1, 2, 3, 4, 5$  に対しても同様に  $\{X_1 Z_2, g_l\} = 0$  なので,  $X_1 Z_2 \in G_n - N(S)$ . よって,  $X_1 Z_2 \notin N(S) - S$ .

同様のことを任意の 1 qubit 誤りの積  $\sigma_j \sigma_k$  について調べれば良い.

演習 10.50

$$2(1 + 3n) \leq 2^n$$

を満たす最大の自然数  $n = 5$ .

演習 10.51

演習 10.52 計算すれば良い.

演習 10.53  $G_z = [000|A_2^\top 0I]$  より, 明らか.

演習 10.54  $G$  の検査行列の標準形

$$\begin{pmatrix} I & A_1 & A_2 & B & 0 & C \\ 0 & 0 & 0 & D & I & E \end{pmatrix}$$

とかく.

$G$  の生成元  $g_i (i = 1, \dots, r)$  と  $G_x = [0E^\top I|C^\top 00]$  の生成元  $g_j^x$  について.

$$r(g_i)\Lambda r(g_j^x) = \dots = 2C_{ij} = 0$$

であることと, 演習 10.33 より,  $g_i (i = 1, \dots, r)$  と  $g_j^x$  は可換. 独立性は明らか.

$G$  の生成元  $g_i (i = r + 1, \dots, n - k)$  と  $G_x = [0E^\top I|C^\top 00]$  の生成元  $g_j^x$  についても上と同様.

$G_z = [000|A_2^\top 0I]$  の生成元  $g_j^z$  と  $G_x = [0E^\top I|C^\top 00]$  の生成元  $g_j^x$  について.

$$r(g_i^z)\Lambda r(g_j^x) = \dots = \delta_{ij}$$

なので,  $g_i^z$  と  $g_j^x$  は,  $i = j$  のとき反可換,  $i \neq j$  のとき可換. 独立性は明らか.

演習 10.55  $G_x$  の検査行列は,

$$( \ 000 \mid 110 \mid 1 \mid 000 \mid 000 \mid 0 \ )$$

より,  $\bar{X} = X_4 X_5 X_7$ .

演習 10.56  $|\psi\rangle \in V_S, g \in S$  として,  $g$  と  $\bar{X}$  は可換なので,

$$g\bar{X}|\psi\rangle = \bar{X}g|\psi\rangle = \bar{X}|\psi\rangle.$$

$\bar{Z}$  についても同様.

演習 10.57 5 qubit

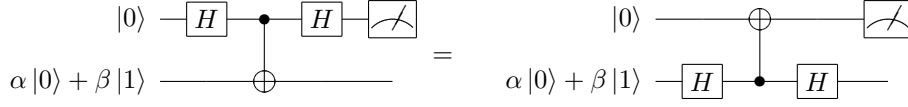
$$\left( \begin{array}{c|c} 10001 & 11011 \\ 01001 & 00110 \\ 00101 & 11000 \\ 00011 & 10111 \end{array} \right)$$

9 qubit

$$\left( \begin{array}{c|c} 101111001 & \\ 010101111 & \\ \hline & 101000000 \\ & 100100000 \\ & 000010001 \\ & 000001001 \\ & 010000100 \\ & 000000010 \end{array} \right)$$

演習 10.58 説明通りに操作することは, 演習 4.34 に示した.

図 10.14 の回路の等価性:



について示す. 演習 4.34 より, 左辺の回路の終状態は,  $|\psi_{in}\rangle = \alpha|0\rangle + \beta|1\rangle$  として,

$$|0\rangle \otimes |+\rangle \langle +|\psi_{in}\rangle + |1\rangle \otimes |-\rangle \langle -|\psi_{in}\rangle$$

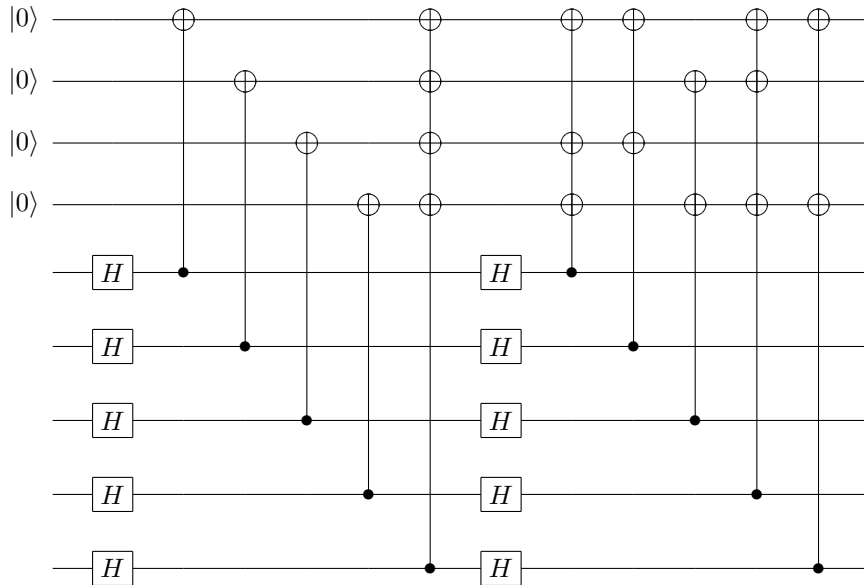
一方, 右辺の回路の終状態は,

$$\frac{\alpha + \beta}{\sqrt{2}} |0\rangle |+\rangle + \frac{\alpha - \beta}{\sqrt{2}} |1\rangle |-\rangle = |0\rangle \otimes |+\rangle \langle +|\psi_{in}\rangle + |1\rangle \otimes |-\rangle \langle -|\psi_{in}\rangle.$$

よって, 示せた. 図 10.15 の回路の等価性についても同様に示せる.

演習 10.59 明らか.

演習 10.60 演習 10.57 で求めた, 検査行列の標準形をみて, シンドローム回路を作ると以下ようになる.



演習 10.61  $E_j (j = 0, \dots, 21)$  は単一 qubit 誤り.

演習 10.62

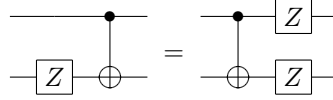
演習 10.63

$$\begin{aligned} \bar{U} |0_L\rangle &= \bar{U} \bar{Z} |0_L\rangle = \bar{X} \bar{U} |0_L\rangle \\ \bar{U} |1_L\rangle &= -\bar{U} \bar{Z} |1_L\rangle = -\bar{X} \bar{U} |1_L\rangle \end{aligned}$$

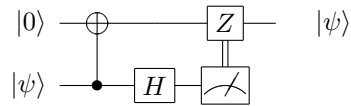
より,  $\bar{U} |0_L\rangle$  は  $\bar{X}$  の固有値 1 の固有状態,  $\bar{U} |1_L\rangle$  は  $\bar{X}$  の固有値 -1 の固有状態. よって,

$$\begin{aligned} \bar{U} |0_L\rangle &\propto \frac{|0_L\rangle + |1_L\rangle}{\sqrt{2}} \\ \bar{U} |1_L\rangle &\propto \frac{|0_L\rangle - |1_L\rangle}{\sqrt{2}}. \end{aligned}$$

演習 10.64



演習 10.65  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  とかく.



上の回路の作用は,

$$\begin{aligned}
 \alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle &\longrightarrow \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \\
 &\longrightarrow \frac{\alpha}{\sqrt{2}}|0\rangle|0\rangle + \frac{\alpha}{\sqrt{2}}|0\rangle|1\rangle + \frac{\beta}{\sqrt{2}}|1\rangle|0\rangle - \frac{\beta}{\sqrt{2}}|1\rangle|1\rangle \\
 &\longrightarrow Z(\alpha|0\rangle - \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle
 \end{aligned}$$

演習 10.66 明らか.

演習 10.67 明らか.

## 第 11 章

# エントロピーと情報

演習 11.1 2 値エントロピー  $H(p, 1-p)$  とすると,

$$H(p, 1-p) \leq H\left(\frac{1}{2}, \frac{1}{2}\right)$$

演習 11.2 まず, 関数方程式

$$f(x+y) = f(x) + f(y)$$

を満たす連続関数が, 定数  $a$  を用いて,  $f(x) = ax$  であることを言う. 関数方程式より,

$$\begin{aligned} f(x) &= -f(-x) \\ f(n) &= nf(1) \quad (n \in \mathbb{N}) \end{aligned}$$

なので, 任意の整数  $m$  に対して,

$$f(m) = f(1)m.$$

また, 任意の自然数  $n$ , 任意の整数  $m$  に対して,

$$f\left(\frac{m}{n}\right) = \frac{1}{n}f(m) = \frac{m}{n}f(1)$$

つまり, 任意の有理数  $x$  に対して,

$$f(x) = f(1)x.$$

$f$  は連続なので, 任意の実数  $x$  に対して,

$$f(x) = f(1)x.$$

$a > 1, x, y < 0$  に対して,  $I$  が,

$$I(a^{x+y}) = I(a^x) + I(a^y)$$

を満たすとなると, 上に示したことから,

$$I(a^x) = I(a)x$$

が言えるので,  $0 < p = a^x \leq 1$  として,

$$I(p) = I(a) \log_a p.$$

演習 11.3 演習 11.4 で示す,  $H_{bin}(p)$  の凹性と,

$$0 = \frac{dH_{bin}(p)}{dp} = \log \frac{1-p}{p} \longrightarrow p = \frac{1}{2}$$

より,  $H_{bin}(p)$  の最大値は,

$$H_{bin}\left(\frac{1}{2}\right) = 1.$$

演習 11.4

$$\frac{d^2 H_{bin}(p)}{d^2 p} = -\frac{1}{p(1-p)} < 0.$$

演習 11.5

$$\begin{aligned} H(p_{X,Y}(x,y)||p_X(x)p_Y(y)) &= -H(p_{X,Y}(x,y)) - \sum_{x,y} p_{X,Y}(x,y) \log [p_X(x)p_Y(y)] \\ &= -H(p_{X,Y}(x,y)) - \sum_{x,y} p_{X,Y}(x,y) \log p_X(x) - \sum_{x,y} p_{X,Y}(x,y) \log p_Y(y) \\ &= -H(p_{X,Y}(x,y)) - \sum_x p_Y(y) \log p_X(x) - \sum_y p_Y(y) \log p_Y(y) \\ &= -H(X,Y) + H(X) + H(Y) \end{aligned}$$

であることと定理 11.1 より,

$$H(X,Y) \leq H(X) + H(Y)$$

が成立し, 等号成立は,

$$p_{X,Y}(x,y) = p_X(x)p_Y(y).$$

演習 11.6 (11.23) 式より,

$$H(X,Y) = H(Y) - \sum_{x,y} p_{X,Y}(x,y) \log p_{X|Y}(x|y).$$

また,

$$\begin{aligned} H(X,Y,Z) &= - \sum_{x,y,z} p_{X,Y,Z}(x,y,z) \log p_{X,Y,Z}(x,y,z) \\ &= - \sum_{x,y,z} p_{X,Y,Z}(x,y,z) \log [p_{X|Y,Z}(x|y,z)p_{Y,Z}(y,z)] \\ &= H(Y,Z) - \sum_{x,y,z} p_{X,Y,Z}(x,y,z) \log p_{X|Y,Z}(x|y,z). \end{aligned}$$

ゆえに,

$$\begin{aligned} &H(X,Y,Z) - H(Y,Z) - H(X,Y) + H(Y) \\ &= - \sum_{x,y,z} p_{X,Y,Z}(x,y,z) \log p_{X|Y,Z}(x|y,z) + \sum_{x,y} p_{X,Y}(x,y) \log p_{X|Y}(x|y) \\ &= \sum_{x,y,z} p_{X,Y,Z}(x,y,z) \log \frac{p_{X|Y}(x|y)}{p_{X|Y,Z}(x|y,z)} \end{aligned}$$



$$\begin{aligned}
&\leq \frac{1}{\ln 2} \sum_{x,y,z} p_{X,Y,Z}(x,y,z) \left( \frac{p_{X|Y}(x|y)}{p_{X|Y,Z}(x|y,z)} - 1 \right) \\
&= \frac{1}{\ln 2} \left( \sum_{x,y,z} p_{Y,Z}(y,z) p_{X|Y}(x|y) - 1 \right) \\
&= \frac{1}{\ln 2} \left( \sum_{x,y} p_Y(y) p_{X|Y}(x|y) - 1 \right) \\
&= \frac{1}{\ln 2} \left( \sum_x p_X(x) - 1 \right) = 0.
\end{aligned}$$

等号成立は,

$$p_{X|Y}(x|y) = p_{X|Y,Z}(x|y,z)$$

つまり,  $Z \rightarrow Y \rightarrow X$  が Markov chain をなすとき.

演習 11.7

演習 11.8

$$H(X, Y : Z) = 1, H(X : Z) = H(Y : Z) = 0.$$

演習 11.9

$$H(X_1 : Y_1) = H(X_2 : Y_2) = H(X_1, X_2 : Y_1, Y_2) = 1.$$

演習 11.10

$$\begin{aligned}
X \rightarrow Y \rightarrow Z \text{ が Markov chain をなす} &\longrightarrow P_{Z|X,Y}(z|x,y) = p_{Z|Y}(z|y) \\
&\longrightarrow \frac{p_{X,Y,Z}(x,y,z)}{p_{X,Y}(x,y)} = \frac{p_{Y,Z}(y,z)}{p_Y(y)} \\
&\longrightarrow \frac{p_{X,Y,Z}(x,y,z)}{p_{Y,Z}(y,z)} = \frac{p_{X,Y}(x,y)}{p_Y(y)} \\
&\longrightarrow P_{X|Y,Z}(x|y,z) = p_{X|Y}(x|y) \\
&\longrightarrow Z \rightarrow Y \rightarrow X \text{ が Markov chain をなす}
\end{aligned}$$

演習 11.11

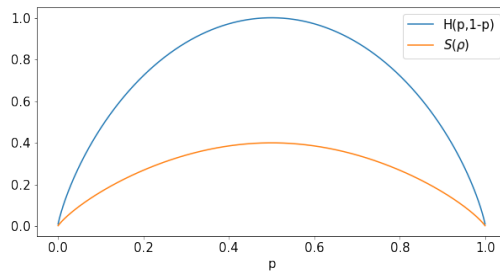
$$0, 0, H_{bin}\left(\frac{3+\sqrt{5}}{6}\right).$$

演習 11.12

$$D = \sqrt{1 - 2p(1-p)}$$

として,

$$S(\rho) = H\left(\frac{1+\sqrt{D}}{2}, \frac{1-\sqrt{D}}{2}\right) \leq H(p, 1-p).$$



演習 11.13 定理 11.8(5) において,

$$\rho = \sum_i p_i |i\rangle \langle i|, \rho_i = \sigma$$

とすると,

$$S(\rho \otimes \sigma) = S(\rho) + S(\sigma).$$

また,

$$\begin{aligned} \rho &= \sum_i p_i |i\rangle \langle i| \\ \sigma &= \sum_j q_j |\tilde{j}\rangle \langle \tilde{j}| \end{aligned}$$

とすると,

$$\rho \otimes \sigma = \sum_{i,j} p_i q_j (|i\rangle \otimes |\tilde{j}\rangle) (\langle i| \otimes \langle \tilde{j}|)$$

なので,

$$S(\rho \otimes \sigma) = - \sum_{ij} p_i q_j \log [p_i q_j] = - \sum_i p_i \log p_i - \sum_j q_j \log q_j = S(\rho) + S(\sigma).$$

演習 11.14

$|AB\rangle$  が純粋状態,  $S(B|A) < 0 \longleftrightarrow S(A) > 0 \longleftrightarrow A$  が純粋状態でない

演習 11.15 測定後の状態  $\rho'$  は,

$$\rho' = M_1 \rho M_1^\dagger + M_2 \rho M_2^\dagger = \text{tr}[\rho] |0\rangle \langle 0| = |0\rangle \langle 0|$$

より,  $S(\rho') = 0$  であるから,  $S(\rho) \geq S(\rho')$ .

演習 11.16  $\rho^{AB}$  は混合状態として.

$$\rho^{AB} = \sum \lambda_i |i^{AB}\rangle \langle i^{AB}|$$

とかくと,

$$\rho^A = \sum \lambda_i \rho_i^A, \rho^B = \sum \lambda_i \rho_i^B$$

となる. また,  $AB$  の純粋化  $ABR$  は,  $R$  の正規直交基底  $\{|i^R\rangle\}$  として,

$$|ABR\rangle = \sum_i \sqrt{\lambda_i} |i^{AB}\rangle |i^R\rangle$$

$$\rho^{ABR} = \sum_{ij} \sqrt{\lambda_i \lambda_j} |i^{AB}\rangle \langle j^{AB}| \otimes |i^R\rangle \langle j^R|$$

とかけるので,

$$\begin{aligned} \rho^{AR} &= \sum_{ij} \sqrt{\lambda_i \lambda_j} \text{tr}_B [|i^{AB}\rangle \langle j^{AB}|] \otimes |i^R\rangle \langle j^R| \\ \rho^R &= \sum_i \lambda_i |i^R\rangle \langle i^R| \end{aligned}$$

を得る.

以上より,

$$\begin{aligned} S(A, B) &= S(B) - S(A) \\ \longleftrightarrow \rho^{AR} &= \rho^A \otimes \rho^R \\ \longleftrightarrow \sum_{ij} \lambda_i \lambda_j \rho_i^A \otimes |j^R\rangle \langle j^R| &= \sum_{ij} \sqrt{\lambda_i \lambda_j} \text{tr}_B [|i^{AB}\rangle \langle j^{AB}|] \otimes |i^R\rangle \langle j^R| \\ \longleftrightarrow \text{tr}_B [|i^{AB}\rangle \langle j^{AB}|] &= \delta_{ij} \rho_i^A \quad \text{かつ} \quad \sum_{ij} \lambda_i \lambda_j \rho_i^A \otimes |j^R\rangle \langle j^R| = \sum_i \lambda_i \rho_i^A \otimes |i^R\rangle \langle i^R| \\ \longleftrightarrow \text{tr}_B [|i^{AB}\rangle \langle j^{AB}|] &= \delta_{ij} \text{tr}_B [|i^{AB}\rangle \langle i^{AB}|] \quad \text{かつ} \quad \sum_{ij} \lambda_i \lambda_j \rho_i^A \otimes |j^R\rangle \langle j^R| = \sum_{ij} \lambda_i \lambda_j \rho_j^A \otimes |j^R\rangle \langle j^R| \\ \longleftrightarrow \{\rho_i^B\} &\text{が互いに直交する台を持つ} \quad \text{かつ} \quad \exists \rho \forall i \in \{i \mid \lambda_i > 0\} \rho_i = \rho \end{aligned}$$

最後の行の 2 つ目の主張については, 演習 11.18 で示す.

演習 11.17

演習 11.18 示すべきは,

$$\sum_{ij} p_i p_j \rho_i \otimes |j\rangle \langle j| = \sum_j p_j \rho_j \otimes |j\rangle \langle j| \longleftrightarrow \exists \rho \forall i \in \{i \mid p_i > 0\} \rho_i = \rho$$

→)

$$\sum_{ij} p_i p_j \rho_i \otimes |j\rangle \langle j| = \sum_j p_j \rho_j \otimes |j\rangle \langle j| = \sum_{ij} p_i p_j \rho_j \otimes |j\rangle \langle j|$$

であり, 両辺の系 B に対する部分トレースを取ると,

$$\sum_{ij} p_i p_j (\rho_i - \rho_j) = 0$$

なので,  $p_i > 0$  なる任意の  $i$  の状態  $\rho_i$  は全て等しい.

←) 明らか.

演習 11.19

$$S\left(\frac{I}{d}\right) = S\left(\sum_i p_i U_i \rho U_i^\dagger\right) \geq \sum_i p_i S(U_i \rho U_i^\dagger) = \sum_i p_i S(\rho) = S(\rho)$$

で等号は,

$$\rho = \frac{I}{d}$$

で成立. ここで, ユニタリ  $U$  に対して,

$$S(U\rho U^\dagger) = -\text{tr}[U\rho U^\dagger \log U\rho U^\dagger] = -\text{tr}[U\rho U^\dagger U(\log \rho)U^\dagger] = -\text{tr}[\rho \log \rho] = S(\rho)$$

が成り立つことを用いた.

#### 演習 11.20

演習 11.21  $[\rho, \sigma] = 0$  とすると, これらは同時対角化可能で,

$$\rho = \sum_i p_i |i\rangle \langle i|, \sigma = \sum_i q_i |i\rangle \langle i|$$

とすると, von Neumann エントロピーの凹性より,  $0 \leq \lambda \leq 1$  に対して,

$$\begin{aligned} H(\{\lambda p_i + (1-\lambda)q_i\}) &= -\sum_i (\lambda p_i + (1-\lambda)q_i) \log(\lambda p_i + (1-\lambda)q_i) \\ &= S(\lambda\rho + (1-\lambda)\sigma) \\ &\geq \lambda S(\rho) + (1-\lambda)S(\sigma) \\ &= \lambda H(\{p_i\}) + (1-\lambda)H(\{q_i\}) \end{aligned}$$

と, Shannon エントロピーの凹性を示せた.

演習 11.22  $[\rho, \sigma] = 0$  とすると, これらは同時対角化可能で,

$$\rho = \sum_i p_i |i\rangle \langle i|, \sigma = \sum_i q_i |i\rangle \langle i|$$

とすると,

$$f(p) = S(p\rho + (1-p)\sigma) = -\sum_i [(p_i - q_i)p + q_i] \log[(p_i - q_i)p + q_i]$$

なので,

$$f''(p) = -\sum_i \frac{(p_i - q_i)^2}{p_i p + (1-p)q_i} \leq 0.$$

演習 11.23 (11.96) 式で  $B_1 = B_2 = B$  とすれば良い.

演習 11.24  $ABC$  の純粋化  $ABCR$  として,

$$S(A, B) = S(C, R), S(A, B, C) = S(R)$$

なので, (11.108) 式より,

$$S(R) + S(B) \leq S(C, R) + S(B, C).$$

#### 演習 11.25

演習 11.26 強い劣加法性から,

$$S(A) + S(B) - S(A, B) + S(A) + S(C) - S(A, C) = S(A : B) + S(A : C) \leq 2S(A).$$

たとえば,  $|AB\rangle$  として, EPR 状態

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

を取ると,

$$S(A : B) = 2 > S(A) = 1.$$

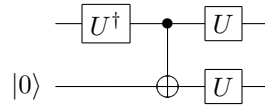
## 第 12 章

# 量子情報理論

演習 12.1  $\langle \psi | \phi \rangle = 0$  であれば,

$$U|0\rangle = |\psi\rangle, U|1\rangle = |\phi\rangle$$

なるユニタリ  $U$  が存在して,



という回路を用いれば,  $|\psi\rangle|\psi\rangle, |\phi\rangle|\phi\rangle$  という状態を作り出せる.

演習 12.2

$$\begin{aligned} \text{tr} \left[ \sum_y \left( \sqrt{E_y} \otimes U_y \right) (\sigma \otimes |0\rangle\langle 0|) \left( \sqrt{E_y} \otimes U_y^\dagger \right) \right] &= \text{tr} \left[ \sum_y \left( \sqrt{E_y} \sigma \sqrt{E_y} \right) \otimes |y\rangle\langle y| \right] \\ &= \sum_y \text{tr} \left[ \sqrt{E_y} \sigma \sqrt{E_y} \otimes |y\rangle\langle y| \right] \\ &= \sum_y \text{tr} [\sigma E_y] = \text{tr} \sigma = \text{tr} [\sigma \otimes |0\rangle\langle 0|]. \end{aligned}$$

演習 12.3

演習 12.4

演習 12.5 定理 12.2(1) より, ある  $\epsilon$  を固定して,

$$\forall \delta > 0 \exists n_0 \in \mathbb{N} \forall n \geq n_0 \quad P(X \in T(n, \epsilon)) \geq 1 - \delta$$

である. 1 情報記号のデータ圧縮に必要なビット数  $A(n, \epsilon)$  として,

$$\begin{aligned} A(n, \epsilon) &= H(X)P(X \in T(n, \epsilon)) + \frac{\log d^n}{n} P(X \notin T(n, \epsilon)) \\ &\leq RP(X \in T(n, \epsilon)) + \log d (1 - P(X \in T(n, \epsilon))) \\ &\leq R + \delta \log d \end{aligned}$$

なので,

$$\forall \delta > 0 \exists n_0 \in \mathbb{N} \forall n \geq n_0 \quad |A(n, \epsilon) - R| \leq \delta \log d.$$

## 演習 12.6

$$C_X = p^{4-\text{wt } X} (1-p)^{\text{wt } X}$$

演習 12.7 コラム 12.4 で,  $V = I$  とすれば良い.

演習 12.8 定理 12.6 の証明の式 (12.51) で式 (9.141) を用いて,

$$\bar{F} \geq F(\rho^{\otimes n}, D^n \circ C^n)$$

すれば良い.

演習 12.9 (1)  $X$  の確率分布関数を

$$p_X(0) = q, \quad p_X(1) = 1 - q$$

とすると  $Y$  の確率分布関数は

$$p_Y(0) = q(1-p), \quad p_Y(1) = (1-q)(1-p), \quad p_Y(e) = p$$

となるので,

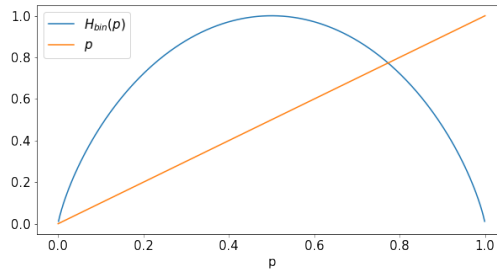
$$\begin{aligned} H(X : Y) &= H(Y) - H(Y|X) \\ &= H(Y) - \sum_x p_X(x) H(Y|X=x) \\ &= H(Y) - H_{\text{bin}}(p) \\ &= -q(1-p) \log q(1-p) - (1-q)(1-p) \log(1-p)(1-q) - p \log p + p \log p + (1-p) \log(1-p) \\ &= (1-p) H_{\text{bin}}(q) \leq (1-p) H_{\text{bin}}(1/2) = 1-p \end{aligned}$$

を得るので, 消去チャンネルの容量は  $1-p$ .

(2)

$$p = H_{\text{bin}}(p)$$

を満たす非ゼロの  $p$  を  $p_0$  とする.  $p \leq p_0$  であれば,  $p \leq H_{\text{bin}}(p)$  なので,  $1 - H_{\text{bin}}(p) \leq 1 - p$ .



## 演習 12.10

$$X \xrightarrow{\mathcal{N}_1} Y \xrightarrow{\mathcal{N}_2} Z$$

として,

$$C(\mathcal{N}_1 \circ \mathcal{N}_2) = \max_{p_X(x)} H(X : Z)$$

$$C(\mathcal{N}_1) = \max_{p_X(x)} H(X:Y)$$

$$C(\mathcal{N}_2) = \max_{p_Y(y)} H(Y:Z)$$

であることと、定理 11.5 より、

$$C(\mathcal{N}_1 \circ \mathcal{N}_2) \leq \min(C(\mathcal{N}_1), C(\mathcal{N}_2))$$

を得る。

#### 演習 12.11

$$\chi(\mathcal{E}) = \max_{\rho} \max_{\{p_j, \rho_j\} \text{ subject to } \rho = \sum_j p_j \rho_j} \left[ S(\mathcal{E}(\rho)) - \sum_j p_j S(\mathcal{E}(\rho_j)) \right]$$

とかけること注目する。

まず、 $\rho$  を固定する。

$$\rho_j = \sum_k q_j^k |\psi_j^k\rangle \langle \psi_j^k|$$

とすると、エントロピーの凹性と  $\mathcal{E}$  の線型性より、

$$S(\mathcal{E}(\rho_j)) \geq \sum_k q_j^k S(\mathcal{E}(|\psi_j^k\rangle \langle \psi_j^k|))$$

を得る。式 (11.79) より、この等号成立条件が  $\rho_j$  が純粋状態の時であることから、

$$\max_{\{p_j, \rho_j\} \text{ subject to } \rho = \sum_j p_j \rho_j} \left[ S(\mathcal{E}(\rho)) - \sum_j p_j S(\mathcal{E}(\rho_j)) \right]$$

を実現するアンサンブル  $\{p_j, \rho_j\}$  は純粋状態だけからなることがわかる。

次に、 $\rho = \sum_j p_j \rho_j$  を動かす。任意の  $\rho$  は、独立な純粋状態  $\rho_1, \rho_2, \dots, \rho_{d^2}$  の線形和でかけることから、 $\max$  を取るべきアンサンブルとしては、高々  $d^2$  個の純粋状態だけからなるアンサンブルを考えれば十分。

#### 演習 12.12

演習 12.13  $\mathcal{E}$  が  $\mathcal{E}_1, \mathcal{E}_2$  を用いて、

$$\mathcal{E} = p\mathcal{E}_1 + (1-p)\mathcal{E}_2$$

とかけるとする。入力  $\rho$  に対する  $\mathcal{E}, \mathcal{E}_1, \mathcal{E}_2$  の w 行列を  $W, W_1, W_2$  とすると、

$$W = pW_1 + (1-p)W_2$$

を得る。よって、エントロピーの凹性より、

$$S(\rho, p\mathcal{E}_1 + (1-p)\mathcal{E}_2) = S(pW_1 + (1-p)W_2) \geq pS(W_1) + (1-p)S(W_2) = pS(\rho, \mathcal{E}_1) + (1-p)S(\rho, \mathcal{E}_2).$$

#### 演習 12.14

演習 12.15 1 つの例として、強い劣加法性

$$S(\rho^{R''E_1''E_2''}) + S(\rho^{E_1''}) \leq S(\rho^{R''E_1''}) + S(\rho^{E_1''E_2''})$$

から関係式を導いてみる. 上の強い劣加法性から, 定理 12.10 の第 2 不等号が導かれたことを思い出すと,

$$S(\rho'') - S(\rho') \leq S(\rho, \mathcal{E}_2 \circ \mathcal{E}_1) - S(\rho, \mathcal{E}_1) = S(\rho^{E_1'' E_2''}) - S(\rho^{E_1''}).$$

ここで,  $\rho^{E_1'' E_2''}, \rho^{E_1''}$  を  $\mathcal{E}_1, \mathcal{E}_2$  の演算要素  $\{E_i\}, \{F_i\}$  で書くことを考える. 量子演算を作用させる前の  $QE_1'' E_2''$  の状態  $\rho^Q \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 0|$  とすると,

$$\rho^{QE_1'' E_2''} = \sum_{i,j,k,l} F_i E_j \rho^Q E_k^\dagger F_l^\dagger \otimes |j\rangle\langle k| \otimes |i\rangle\langle l|$$

なので,

$$\begin{aligned} \rho^{E_1'' E_2''} &= \text{tr}_Q \rho^{QE_1'' E_2''} = \sum_{i,j,k,l} \text{tr}_Q [F_i E_j \rho^Q E_k^\dagger F_l^\dagger] |j\rangle\langle k| \otimes |i\rangle\langle l| \\ \rho^{E_1''} &= \text{tr}_{QE_2} \rho^{QE_1'' E_2''} = \sum_{i,j,k} \text{tr}_Q [F_i E_j \rho^Q E_k^\dagger F_i] |j\rangle\langle k| \end{aligned}$$

他の組み合わせについては, arXiv:quant-ph/0011036 に示してある.

演習 12.16 定理 12.10 の第 1 等号の成立条件で示した.

演習 12.17 示すべきは,

$$\forall t \in \mathbb{R} \quad \sum_{j=1}^d \max(x_j - t, 0) \leq \sum_{j=1}^d \max(y_j - t, 0) \iff \forall k \in \{1, 2, \dots, d\} \quad \sum_{j=1}^k x_j^\downarrow \leq \sum_{j=1}^k y_j^\downarrow$$

$\implies$   $k = 1, 2, \dots, d$  に対して  $t = y_k^\downarrow$  とすれば,

$$\sum_{j=1}^k (y_j^\downarrow - y_k^\downarrow) = \sum_{j=1}^d \max(y_j^\downarrow - y_k^\downarrow, 0) \geq \sum_{j=1}^d \max(x_j^\downarrow - y_k^\downarrow, 0) \geq \sum_{j=1}^k \max(x_j^\downarrow - y_k^\downarrow, 0) \geq \sum_{j=1}^k (x_j^\downarrow - y_k^\downarrow)$$

より

$$\sum_{j=1}^k y_j^\downarrow \geq \sum_{j=1}^k x_j^\downarrow$$

を得る.

$\longleftarrow$  任意の実数  $t$  をとってくると,

1.  $\exists i \in \{1, 2, \dots, d-1\} \quad x_i^\downarrow \geq t \geq x_{i+1}^\downarrow$
2.  $t \geq x_1^\downarrow$
3.  $x_d^\downarrow \geq t$

のいずれかを満たし, いずれの場合でも

1.  $\sum_{j=1}^d \max(x_j - t, 0) = \sum_{j=1}^i (x_j^\downarrow - t) \leq \sum_{j=1}^i (y_j^\downarrow - t) \leq \sum_{j=1}^i \max(y_j^\downarrow - t, 0) \leq \sum_{j=1}^d \max(y_j - t, 0)$
2.  $\sum_{j=1}^d \max(x_j - t, 0) = 0 \leq \sum_{j=1}^d \max(y_j - t, 0)$
3.  $\sum_{j=1}^d \max(x_j - t, 0) = \sum_{j=1}^d (x_j^\downarrow - t) \leq \sum_{j=1}^d (y_j^\downarrow - t) \leq \sum_{j=1}^d \max(y_j - t, 0)$

のように,

$$\sum_{j=1}^d \max(x_j - t, 0) \leq \sum_{j=1}^d \max(y_j - t, 0)$$

が示せた.



演習 12.18  $x^1, x^2 \prec y$ ,  $0 \leq \lambda \leq 1$  とすると,  $k = 1, 2, \dots, d$  に対して,

$$\sum_{j=1}^k \lambda x_j^{1\downarrow} + (1-\lambda)x_j^{2\downarrow} \leq \sum_{j=1}^k y_j^\downarrow$$

であり,

$$\sum_{j=1}^d \lambda x_j^{1\downarrow} + (1-\lambda)x_j^{2\downarrow} \leq \sum_{j=1}^d y_j^\downarrow$$

であるので,  $\lambda x_j^1 + (1-\lambda)x_j^2 \prec y$  なので,  $\{x|x \prec y\}$  は凸集合.

演習 12.19 示すべきは,  $x \prec y$  ならば  $x' \prec y'$ , つまり  $l = 1, 2, \dots, d-1$  に対して,

$$\sum_{i=1}^l x_i'^\downarrow \leq \sum_{i=1}^l y_i'^\downarrow$$

が成立し,  $l = d-1$  で等号が成立すること.

次のような  $k$  を定める;

$$y_1^\downarrow \leq y_2^\downarrow \leq \dots \leq y_k^\downarrow \leq (1-t)y_1^\downarrow + ty_j^\downarrow \leq y_{k+1}^\downarrow \leq y_{k+2}^\downarrow \leq \dots \leq y_j^\downarrow \leq \dots \leq y_d^\downarrow$$

また,  $l = 1, 2, \dots, d-1$  として,

$$\sum_{i=1}^l x_i'^\downarrow = \sum_{i=1}^{l+1} x_i^\downarrow - x_1^\downarrow \leq \sum_{i=1}^{l+1} y_i^\downarrow - ty_1^\downarrow - (1-t)y_j^\downarrow$$

が成立.

$l \leq k-1$  のとき

$$\sum_{i=1}^l y_i'^\downarrow = \sum_{i=2}^{l+1} y_i^\downarrow$$

なので,

$$\sum_{i=1}^l x_i'^\downarrow \leq \sum_{i=1}^{l+1} y_i^\downarrow - ty_1^\downarrow - (1-t)y_j^\downarrow = \sum_{i=1}^l y_i'^\downarrow + (1-t)y_1^\downarrow - (1-t)y_j^\downarrow \leq \sum_{i=1}^l y_i'^\downarrow + y_{k+1}^\downarrow - y_j^\downarrow \leq \sum_{i=1}^l y_i'^\downarrow.$$

$k \leq l \leq j-1$  のとき

$$\sum_{i=1}^l y_i'^\downarrow = \sum_{i=2}^l y_i^\downarrow + (1-t)y_1^\downarrow + ty_j^\downarrow$$

なので,

$$\sum_{i=1}^l x_i'^\downarrow \leq \sum_{i=1}^{l+1} y_i^\downarrow - ty_1^\downarrow - (1-t)y_j^\downarrow = \sum_{i=1}^l y_i'^\downarrow - y_j^\downarrow + y_{l+1}^\downarrow \leq \sum_{i=1}^l y_i'^\downarrow$$

$j \leq l$  のとき

$$\sum_{i=1}^l y_i'^\downarrow = \sum_{i=2}^{j-1} y_i^\downarrow + \sum_{i=j+1}^{l+1} y_i^\downarrow + (1-t)y_1^\downarrow + ty_j^\downarrow = \sum_{i=2}^{l+1} y_i^\downarrow + (1-t)y_1^\downarrow - (1-t)y_j^\downarrow$$

なので,

$$\sum_{i=1}^l x_i'^{\downarrow} \leq \sum_{i=1}^{l+1} y_i^{\downarrow} - t y_1^{\downarrow} - (1-t) y_j^{\downarrow} = \sum_{i=1}^l y_i'^{\downarrow}$$

$l = d-1$  のとき

$$\sum_{i=1}^{d-1} x_i'^{\downarrow} = \sum_{i=1}^d y_i^{\downarrow} - t y_1^{\downarrow} - (1-t) y_j^{\downarrow} = \sum_{i=1}^l y_i'^{\downarrow}$$

演習 12.20  $\rho_\psi$  の台を Alice の状態空間とすれば良い.

演習 12.21

$$\begin{aligned} \text{tr}_B |\psi\rangle \langle \psi| &= 0.4 |0\rangle \langle 0| + 0.4 |1\rangle \langle 1| + 0.1 |2\rangle \langle 2| + 0.1 |3\rangle \langle 3| \\ \text{tr}_B |\phi\rangle \langle \phi| &= 0.5 |0\rangle \langle 0| + 0.25 |1\rangle \langle 1| + 0.25 |2\rangle \langle 2| \end{aligned}$$

より,  $\text{tr}_B |\psi\rangle \langle \psi| \not\prec \text{tr}_B |\phi\rangle \langle \phi|$  なので, 定理 12.25 より  $|\psi\rangle$  から  $|\phi\rangle$  への変換は LOCC ではできない.

演習 12.22

演習 12.23 教科書の議論より, LOCC により,  $|\psi\rangle = \sum_x \sqrt{x} |x_A\rangle |x_B\rangle$  から  $S(\rho_\psi)$  個の Bell 状態が作れることがわかっていて, ここで,  $\rho_\psi = \text{tr}_A |\psi\rangle \langle \psi|$ . LOCC によって  $S(< S(\rho_\psi))$  の Bell 状態から  $|\psi\rangle$  が作れるとすると,  $S(\rho_\psi)$  個の Bell 状態が作れる. つまり, LOCC によって,  $S(< S(\rho_\psi))$  の Bell 状態から  $S(\rho_\psi)$  個の Bell 状態が作れる事になるが, これは演習 12.24 より矛盾. したがって, 教科書にあるもつれの希釈手続きが最適である.

演習 12.24 純粋状態  $|\psi\rangle, |\phi\rangle$  は,

$$|\psi\rangle = \sum_{i=1}^{\text{Sch}(\lambda_\psi)} \sqrt{\lambda_{\psi i}} |i\rangle_A |i\rangle_B, \quad |\phi\rangle = \sum_{i=1}^{\text{Sch}(\lambda_\phi)} \sqrt{\lambda_{\phi i}} |\tilde{i}\rangle_A |\tilde{i}\rangle_B$$

とかける. ここで,

$$\begin{aligned} \sum_{i=1}^{\text{Sch}(\lambda_\psi)} \lambda_{\psi i}^{\downarrow} &= \sum_{i=1}^{\text{Sch}(\lambda_\phi)} \lambda_{\phi i}^{\downarrow} = 1 \\ \forall i \in \{1, 2, \dots, \text{Sch}(\lambda_\psi)\} \quad \lambda_{\psi i}^{\downarrow} &> 0 \\ \forall i \in \{1, 2, \dots, \text{Sch}(\lambda_\phi)\} \quad \lambda_{\phi i}^{\downarrow} &> 0 \end{aligned}$$

である. 定理 12.25 より, LOCC により  $|\psi\rangle \rightarrow |\phi\rangle$  という変換が可能であるとする,  $\lambda_\psi \prec \lambda_\phi$ . もし,  $\text{Sch}(\lambda_\psi) < \text{Sch}(\lambda_\phi)$  とすると,

$$0 = \sum_{i=1}^{\text{Sch}(\lambda_\psi)} \lambda_{\psi i}^{\downarrow} - \sum_{i=1}^{\text{Sch}(\lambda_\phi)} \lambda_{\phi i}^{\downarrow} = \sum_{i=1}^{\text{Sch}(\lambda_\psi)} (\lambda_{\psi i}^{\downarrow} - \lambda_{\phi i}^{\downarrow}) + \sum_{i=\text{Sch}(\lambda_\psi)+1}^{\text{Sch}(\lambda_\phi)} \lambda_{\phi i}^{\downarrow} > 0$$

と矛盾. したがって, LOCC による  $|\psi\rangle \rightarrow |\phi\rangle$  という変換によって, Schmidt 数は増加しない.

$d$  次元状態空間上の純粋状態  $|\psi\rangle, |\phi\rangle$  が,

$$\begin{aligned} |\psi\rangle &= \left( \frac{|00\rangle + |11\rangle}{\sqrt{2}} \right)^{\otimes k} |\text{AB がもつれてない 2qubit 状態}\rangle^{\otimes d-k} \\ |\phi\rangle &= \left( \frac{|00\rangle + |11\rangle}{\sqrt{2}} \right)^{\otimes l} |\text{AB がもつれてない 2qubit 状態}\rangle^{\otimes d-l} \end{aligned}$$

とする.  $|\psi\rangle, |\phi\rangle$  はそれぞれ Alice と Bob が  $k, l$  個の Bell 状態を共有している. ここで,  $k < l$  とすると,  $\text{Sch}(\lambda_\psi) = 2^k < \text{Sch}(\lambda_\phi) = 2^l$  なので,  $|\psi\rangle \rightarrow |\phi\rangle$  という変換は LOCC によってできない. つまり, Alice と Bob の共有する Bell 状態の数は, LOCC で増加しない.

演習 12.25 秘密鍵  $n!/2$ , 公開鍵  $2n$ .

演習 12.26  $(b_k, b'_k) = (0, 0)$  のとき, Bob は  $|\psi_{a_k 0}\rangle = |a_k\rangle$  を  $Z$  の固有状態を基底とした測定を行い, 測定値  $a'_k$  は確率 1 で  $a_k$  と等しくなる.  $(b_k, b'_k) = (1, 0)$  のとき, Bob は  $|\psi_{a_k 1}\rangle = |a_k\rangle$  を  $Z$  の固有状態を基底とした測定を行い, 測定値  $a'_k$  は確率  $1/2$  で  $a_k$ , 確率  $1/2$  で  $\bar{a}_k$  というようにランダムに得られる.  $(b_k, b'_k) = (0, 1), (b_k, b'_k) = (1, 1)$  のときも同様.

演習 12.27 (1)

$$\epsilon = \mu - 2\delta \geq 0$$

とする.  $2n$  ビットのうち  $\mu n$  ビットが誤っていると.  $2n$  ビットから  $n$  ビットの検査ビットを選んだ時に, 検査ビット中の誤りが  $\delta n$  より小さくなる確率  $p$  は,

$$p = \sum_{i=0}^{\delta n-1} \frac{\mu n C_i \times 2n-\mu n C_{n-i}}{2n C_n}.$$

ここで,

$$a_i \equiv \mu n C_i \times 2n-\mu n C_{n-i}$$

とすると,  $i = 0, 1, \dots, \delta n - 2$  に対して,

$$\frac{a_{i+1}}{a_i} = \frac{\frac{n+1}{i+1} - 1}{\frac{n+1}{\mu n-i} - 1} > 1$$

より,  $a_i$  は単調増加なので,

$$p = \sum_{i=0}^{\delta n-1} \frac{a_i}{2n C_n} < \delta n \frac{a_{\delta n}}{2n C_n} < \delta n \frac{\mu n C_{\delta n} \times 2n-\mu n C_{n-\delta n}}{2n C_n}$$

を得る.

(2)

$$\frac{b}{a} = t, an = s$$

とすると,

$$2^{anH(\frac{b}{a})} = [t^t(1-t)^{1-t}]^{-s}$$

$${}_{an}C_{bn} = {}_sC_{st}$$

とかける. スターリングの公式より,

$$\frac{\sqrt{2\pi}}{e^2} \frac{s^{s+\frac{1}{2}}}{(st)^{st+\frac{1}{2}}(s(1-t))^{s(1-t)+\frac{1}{2}}} \leq \frac{s!}{(st)!(s-st)!} = {}_sC_{st} \leq \frac{e}{2\pi} \frac{s^{s+\frac{1}{2}}}{(st)^{st+\frac{1}{2}}(s(1-t))^{s(1-t)+\frac{1}{2}}}.$$

よって,

$$\frac{2^{anH(\frac{b}{a})}}{{}_{an}C_{bn}} = \frac{[t^t(1-t)^{(1-t)}]^{-s}}{{}_sC_{st}}$$

$$\begin{aligned}
&\geq \frac{2\pi}{e} \frac{(st)^{st+\frac{1}{2}}(s(1-t))^{s(1-t)+\frac{1}{2}}}{s^{s+\frac{1}{2}}[t^t(1-t)^{1-t}]^s} \\
&= \frac{2\pi}{e} \left( \frac{st \cdot s(1-t)}{s} \right)^{\frac{1}{2}} \left( \frac{(st)^t(s(1-t))^{1-t}}{st^t(1-t)^{1-t}} \right)^s = \frac{2\pi}{e} \sqrt{st(1-t)}
\end{aligned}$$

よって、任意の  $t$  に対して、

$$s > \frac{e^2}{4\pi^2 t(1-t)}$$

を満たす程十分大きな  $s$  を取れば、

$$\frac{2^{anH(\frac{b}{a})}}{anC_{bn}} \geq 1.$$

もう一方の不等号についても同様に示せる.

(3) 問題文で与えられた不等式と (2) で示した不等式より、

$$\begin{aligned}
p &< \delta n \frac{\mu n C_{\delta n} \times 2^{n-\mu n} C_{n-\delta n}}{2^n C_n} \\
&< \delta n(2n+1) \frac{2^{\mu n(1-2(\frac{\mu}{\delta}-\frac{1}{2})^2)} 2^{(2-\mu)n(1-2(\frac{2-\mu}{1-\delta}-\frac{1}{2})^2)}}{2^{\frac{n}{2}}} \\
&= \delta n(2n+1) 2^{\frac{3n}{2}} 2^{-2n(\mu(\frac{\mu}{\delta}-\frac{1}{2})^2 + (2-\mu)(\frac{2-\mu}{1-\delta}-\frac{1}{2})^2)} \\
&= \delta n(2n+1) 2^{\frac{3n}{2}} 2^{-\frac{n}{2} \left[ \mu \frac{\epsilon^2}{\delta^2} + (2-\mu) \frac{(2\epsilon+3(1-\delta))^2}{(1-\delta)^2} \right]} \\
&< \delta n(2n+1) 2^{\frac{3n}{2}} 2^{-\frac{n}{2} \left[ \mu \frac{\epsilon^2}{\delta^2} + (2-\mu) \frac{4\epsilon^2}{(1-\delta)^2} \right]} \\
&< \delta n(2n+1) 2^{\frac{3n}{2}} 2^{-\frac{n}{2} [\mu \epsilon^2 + (2-\mu) 4\epsilon^2]} \\
&< \delta n(2n+1) 2^{-\frac{n}{2} [3+(8-3\mu)\epsilon^2]} = 2^{-O(\epsilon^2 n)}.
\end{aligned}$$

演習 12.28  $(a', b) = (0, 1)$  のとき, Bob が状態  $|\psi\rangle$  を  $Z$  基底で測定して, 固有値  $+1$  の方を得る. このとき  $|\psi\rangle = |0\rangle$  つまり  $a = a' = 0$ .  $(a', b) = (1, 1)$  のときも同様に示せる

演習 12.29

演習 12.30  $\ln(1-x)$  の Taylor 展開

$$\ln(1-x) = -x + O(x^2)$$

を用いて、

$$\begin{aligned}
S(\rho_{\max}) &= -(1-2^{-s}) \log(1-2^{-s}) - 2^{-s} \log \frac{2^{-s-2n}}{1-2^{-2n}} \\
&= \frac{1-2^{-s}}{\ln 2} (2^{-s} + O(2^{-2s})) + 2^{-s} (s+2n) + 2^{-s} (-2^{-n} + O(2^{-2n})) \\
&= \left( 2n + s + \frac{1}{\ln 2} \right) 2^{-s} + O(2^{-2s}).
\end{aligned}$$

最後の等号では  $s < n$  を用いた.

演習 12.31 Eve がチャンネル全ての制御ができるとすると, Alice が Bob に送信した情報を、

$$F(\rho, |\beta_{00}\rangle^{\otimes n}) > 1 - 2^{-s}$$

を満たすように

$$\rho = \sum_x p_x \rho_x$$

と書き換えることができてしまう.  $\rho$  を Alice と Bob が  $\text{POVM}\{E_y\}$  によって測定して得た結果  $Y$  と Eve が持っている  $\rho$  に関する情報  $X$  の相互情報量は, Holevo 限界, エントロピーの非負性, 演習 12.30 より,

$$H(X : Y) \leq S(\rho) - \sum_x p_x S(\rho_x) \leq S(\rho) < \left(2n + s + \frac{1}{\ln 2}\right) 2^{-s} + O(2^{-2s}).$$

演習 12.32 例えば, ビット反転については,

$$\Pi_{bf} = \frac{I \otimes I - Z \otimes Z}{2}, I - \Pi_{bf} = \frac{I \otimes I + Z \otimes Z}{2}$$

とかけるので.

演習 12.33

演習 12.34

演習 12.35

演習 12.36 明らか.

## 第 D 章

# 整数論

演習 D.1

演習 D.2

演習 D.3

演習 D.4

演習 D.5

演習 D.6

演習 D.7

演習 D.8

演習 D.9

演習 D.10

演習 D.11

演習 D.12

演習 D.13

演習 D.14

演習 D.15

演習 D.16

演習 D.17

演習 D.18

演習 D.19

$$q_1 p_0 - p_1 q_0 = -1$$

$$q_n p_{n-1} - p_n q_{n-1} = (a_n q_{n-1} + q_{n-2}) p_{n-1} - (a_n p_{n-1} + p_{n-2}) q_{n-1} = (-1)(q_{n-1} p_{n-2} - p_{n-1} q_{n-2})$$

なので, 帰納法より,

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n.$$

$p_n, q_n$  の最大公約数  $g_n$  として,  $p_n = g_n p'_n$  などと書くと,

$$g_n g_{n-1} (q'_n p'_{n-1} - p'_n q'_{n-1}) = (-1)^n.$$

ここで,

$$\begin{aligned} \frac{q'_n p'_{n-1} - p'_n q'_{n-1}}{p'_n p'_{n-1}} &= \frac{q'_n}{p'_n} - \frac{q'_{n-1}}{p'_{n-1}} = \frac{q_n}{p_n} - \frac{q_{n-1}}{p_{n-1}} \begin{cases} > 0 & (n : \text{even}) \\ < 0 & (n : \text{odd}) \end{cases} \\ \rightarrow q'_n p'_{n-1} - p'_n q'_{n-1} &\begin{cases} > 0 & (n : \text{even}) \\ < 0 & (n : \text{odd}) \end{cases} \end{aligned}$$

であるから,

$$g_n g_{n-1} = 1$$

となり,  $g_n, g_{n-1}$  は正の整数なので,

$$g_n = g_{n-1} = 1$$

を得る.

## 第 F 章

# Lieb の定理の証明

演習 F.1  $A \leq B$  とすると, 任意の状態  $|\psi\rangle$  に対して,

$$\langle\psi|X^\dagger(B-A)X|\psi\rangle \geq 0$$

なので,

$$X^\dagger B X \geq X^\dagger A X.$$

演習 F.2 明らか.

演習 F.3 明らか.

演習 F.4 (1)

(2)  $A$  は Hermite なので,

$$A = \sum_i \lambda_i |i\rangle \langle i|$$

として,

$$\begin{aligned} \|A\| &= \max |\langle u|A|u\rangle| \text{ subject to } \langle u|u\rangle = 1 \\ &= \max \left| \sum_i \lambda_i |c_i|^2 \right| \text{ subject to } \sum_i |c_i|^2 = 1 \\ &= |\lambda| \end{aligned}$$

演習 F.5  $AB, BA$  の固有多項式  $f_{AB}(x), f_{BA}(x)$  とかく.

$A$  が正則ならば,

$$f_{AB}(x) = \det(xI - AB) = \det(A^{-1}xIA - A^{-1}ABA) = \det(xI - BA) = f_{BA}(x).$$

$A$  が非正則とする. 上に示した通り,  $A(y) = A + yI$  として,  $\det A(y) \neq 0$  なる  $y$  に対して,

$$f_{A(y)B}(x) = f_{BA(y)}(x)$$

である. ここで,  $\det A(y)$  は  $y$  に関する  $n$  次なので,  $\det A(y) = 0$  なる  $y$  は高々  $n$  個であることと固有多項式の連続性より, 上式で  $\det A(y) = 0$  なる  $y$  を避けるように,  $y \rightarrow 0$  として,

$$f_{AB}(x) = f_{BA}(x).$$



演習 F.6 演習 F.4, F.5 より,  $AB$  が Hermite ならば,  $AB$  の絶対値最大の固有値  $\lambda$  として,

$$\lambda = \|AB\| \leq \|BA\|.$$

演習 F.7  $A$  が正オペレータのとき,

$$\begin{aligned} A \leq I &\longleftrightarrow \forall |\psi\rangle \quad \langle \psi | I - A | \psi \rangle \geq 0 \\ &\longleftrightarrow \forall |\psi\rangle \quad 0 \leq \langle \psi | A | \psi \rangle \leq \langle \psi | \psi \rangle \\ &\longleftrightarrow \forall |u\rangle : \text{単位ベクトル} \quad 0 \leq \langle u | A | u \rangle \leq 1 \\ &\longleftrightarrow \|A\| \leq 1. \end{aligned}$$

演習 F.8  $A, B$  が正オペレータのとき,  $\text{tr} AB \geq 0$  なので,

$$\text{tr} X^\dagger A X = \text{tr} A X X^\dagger \geq 0.$$