量子計算ミニマム

筒井翔一朗

2022 年 1 月 7 日

目次

1 Notation

Qubit

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

Kronecker 積

$$A \otimes B \equiv \begin{pmatrix} a_{11}B & \dots & a_{1N}B \\ \vdots & \ddots & \vdots \\ a_{N1}B & \dots & a_{NN}B \end{pmatrix} \tag{2}$$

Pauli ゲート

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{3}$$

Hadamard ゲート

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{4}$$

一般位相ゲート

$$R_l = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{2\pi}{2^l}} \end{pmatrix} \tag{5}$$

整数 k の 2 進数表記

$$(k)_2 = i_1 i_2 \cdots, \quad i_n = 0, 1 \tag{6}$$

例

$$(0)_2 = 0 \tag{7}$$
$$(1)_2 = 1 \tag{8}$$
$$(2)_2 = 10 \tag{9}$$
$$(3)_2 = 11 \tag{10}$$
$$(4)_2 = 100 \tag{11}$$
$$(5)_2 = 101 \tag{12}$$
$$(6)_2 = 110 \tag{13}$$
$$(7)_2 = 111 \tag{14}$$
$$(8)_2 = 1000 \tag{15}$$
$$(9)_2 = 1001 \tag{16}$$
$$(10)_2 = 1010 \tag{17}$$
$$(11)_2 = 1011 \tag{18}$$
$$(12)_2 = 1100 \tag{19}$$
$$(13)_2 = 1101 \tag{20}$$

小数を含む 2 進数表記

$$(k)_2 = k_1 \cdots k_{l-1}.k_l \cdots k_n = \cdots + k_{l-1} 2^0 + \frac{k_l}{2^1} + \frac{k_{l+1}}{2^2} + \cdots + \frac{k_n}{2^{n-l+1}} \tag{21}$$

2　基本的な計算結果

X ゲートは

$$X\,|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \tag{22}$$
$$X\,|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \tag{23}$$

のように 0,1 を反転させるので、NOT の役割をする。

アダマールゲートによる演算。

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{24}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{25}$$

量子状態と測定確率。規格化された状態

$$|\psi\rangle = \frac{\alpha}{\sqrt{|\alpha|^2 + |\alpha|^2}}|0\rangle + \frac{\beta}{\sqrt{|\alpha|^2 + |\alpha|^2}}|1\rangle \tag{26}$$

があったとする。この状態を測定して $|0\rangle$ が観測される確率は

$$P_0 = |\,|0\rangle\langle 0|\,|\psi\rangle\,|^2 = |\,\langle 0|\,|\psi\rangle\,|^2 = \frac{|\alpha|^2}{|\alpha|^2 + |\beta|^2} \tag{27}$$

である。

10 進数と 2 進数の関係。$(k)_2 = k_1k_2\cdots k_n$ のとき

$$k = k_1 2^{n-1} + k_2 2^{n-2} + \cdots + k_n 2^0 \tag{28}$$

例えば、

$$9 = 1\times 2^3 + 0\times 2^2 + 0\times 2^1 + 1\times 2^0 \tag{29}$$

3 測定について

ここでは有限次元の Hilbert 空間のみ考える。半正定値行列のセット $\{F_i\}$ で

$$\sum_i F_i = I \tag{30}$$

を満たすようなものを positive operator-valued measure (POVM) と呼ぶ。量子状態 ρ を測定して、出力 i が得られる確率は

$$\mathrm{tr}(\rho F_i) \tag{31}$$

で与えられる。

例として、純粋状態

$$\rho = |\psi\rangle\langle\psi|, \quad |\psi\rangle = \frac{\alpha}{|\alpha|^2 + |\alpha|^2}|0\rangle + \frac{\beta}{|\alpha|^2 + |\alpha|^2}|1\rangle \tag{32}$$

と、POVM

$$F_0 = \frac{1+Z}{2} = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \quad F_1 = \frac{1-Z}{2} = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}, \tag{33}$$

を考える。測定によって出力 0 が得られる確率は

$$\mathrm{tr}(\rho F_0) = \mathrm{tr}(|\psi\rangle\langle\psi|\,F_0) = \langle\psi|\,F_0\,|\psi\rangle = \frac{\alpha^2}{|\alpha|^2 + |\alpha|^2} \tag{34}$$

出力 1 が得られる確率は

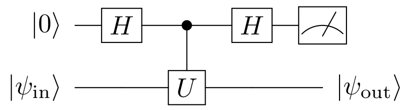
$$\mathrm{tr}(\rho F_1) = \mathrm{tr}(|\psi\rangle\langle\psi|\,F_1) = \langle\psi|\,F_1\,|\psi\rangle = \frac{\beta^2}{|\alpha|^2 + |\alpha|^2} \tag{35}$$

である。これはいわゆる Born の規則である。

4　基本的な量子アルゴリズム

4.1　アダマールテスト

U をユニタリー演算子とする。以下のゲート



を考える。control U gate を式で表すと、

$$|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes U \tag{36}$$

であることに注意して、この回路を式で書くと、測定の直前の状態は

$$\begin{aligned}
&(H\otimes I)(|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes U)(H\otimes I)|0\rangle|\psi_{\mathrm{in}}\rangle && (37)\\
=&(H\otimes I)(|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes U)\frac{|0\rangle|\psi_{\mathrm{in}}\rangle+|1\rangle|\psi_{\mathrm{in}}\rangle}{\sqrt{2}} && (38)\\
=&(H\otimes I)\left(\frac{|0\rangle|\psi_{\mathrm{in}}\rangle}{\sqrt{2}}+\frac{|1\rangle U|\psi_{\mathrm{in}}\rangle}{\sqrt{2}}\right) && (39)\\
=&\frac{1}{\sqrt{2}}(H\otimes I)\left(|0\rangle|\psi_{\mathrm{in}}\rangle+|1\rangle U|\psi_{\mathrm{in}}\rangle\right) && (40)\\
=&\frac{1}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|\psi_{\mathrm{in}}\rangle+\frac{|0\rangle-|1\rangle}{\sqrt{2}}U|\psi_{\mathrm{in}}\rangle\right) && (41)\\
=&\frac{|0\rangle+|1\rangle}{2}|\psi_{\mathrm{in}}\rangle+\frac{|0\rangle-|1\rangle}{2}U|\psi_{\mathrm{in}}\rangle && (42)\\
=&|0\rangle\frac{I+U}{2}|\psi_{\mathrm{in}}\rangle+|1\rangle\frac{I-U}{2}|\psi_{\mathrm{in}}\rangle && (43)
\end{aligned}$$

となる。第一の qubit が $|0\rangle$ である確率は

$$\begin{aligned}
p_0&=\left|(|0\rangle\langle 0|\otimes I)\left(|0\rangle\frac{I+U}{2}|\psi_{\mathrm{in}}\rangle+|1\rangle\frac{I-U}{2}|\psi_{\mathrm{in}}\rangle\right)\right|^2 && (44)\\
&=\left||0\rangle\frac{I+U}{2}|\psi_{\mathrm{in}}\rangle\right|^2 && (45)\\
&=\left(\langle\psi_{\mathrm{in}}|\frac{I+U^\dagger}{2}\langle 0|\right)\left(|0\rangle\frac{I+U}{2}|\psi_{\mathrm{in}}\rangle\right) && (46)\\
&=\langle\psi_{\mathrm{in}}|\frac{I+U+U^\dagger+U^\dagger U}{4}|\psi_{\mathrm{in}}\rangle && (47)\\
&=\langle\psi_{\mathrm{in}}|\frac{2I+U+U^\dagger}{4}|\psi_{\mathrm{in}}\rangle && (48)\\
&=\frac{1+\mathrm{Re}\langle\psi_{\mathrm{in}}|U|\psi_{\mathrm{in}}\rangle}{2} && (49)
\end{aligned}$$

となり、第一の qubit が $|1\rangle$ である確率は

$$p_1 = \left| (|1\rangle\langle 1| \otimes I) \left(|0\rangle \frac{I+U}{2} |\psi_{\rm in}\rangle + |1\rangle \frac{I-U}{2} |\psi_{\rm in}\rangle \right) \right|^2 \tag{50}$$

$$= \left| |1\rangle \frac{I-U}{2} |\psi_{\rm in}\rangle \right|^2 \tag{51}$$

$$= \left(\langle\psi_{\rm in}| \frac{I-U^\dagger}{2} \langle 1| \right) \left(|1\rangle \frac{I-U}{2} |\psi_{\rm in}\rangle \right) \tag{52}$$

$$= \langle\psi_{\rm in}| \frac{I-U-U^\dagger+U^\dagger U}{4} |\psi_{\rm in}\rangle \tag{53}$$

$$= \langle\psi_{\rm in}| \frac{2I-U-U^\dagger}{4} |\psi_{\rm in}\rangle \tag{54}$$

$$= \frac{1-{\rm Re}\langle\psi_{\rm in}| U |\psi_{\rm in}\rangle}{2} \tag{55}$$

となる。従って、この回路では演算子 U の $\langle\psi_{\rm in}|$ における期待値を推定することができる。

測定の結果、第一番目の qubit が $|0\rangle, |1\rangle$ だった場合、残りの状態はそれぞれ、

$$|\psi_{\rm out}\rangle = |\psi_0\rangle = \frac{I+U}{2} |\psi_{\rm in}\rangle, \quad |\psi_{\rm out}\rangle = |\psi_1\rangle = \frac{I-U}{2} |\psi_{\rm in}\rangle \tag{56}$$

となる。

4.2 量子フーリエ変換

x_j を 2^n 成分ベクトルとする。これは規格化 $\sum_{j=0}^{2^n-1} |x_j|^2 = 1$ されているとする。この離散フーリエ変換

$$y_k = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} x_j e^{i\frac{2\pi jk}{2^n}} \tag{57}$$

を量子回路を用いて計算する方法について述べる。

整数 j に対してその 2 進数表記をラベルに持つような量子状態を考え、次のように書く。

$$|(j)_2\rangle = |i_1 i_2 \cdots\rangle \tag{58}$$

例えば

$$|(6)_2\rangle = |110\rangle = |1\rangle \otimes |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{59}$$

である。この約束のもと、次のような状態を考える

$$|x\rangle\rangle \equiv \sum_{j=0}^{2^n-1} x_j |(j)_2\rangle, \quad |y\rangle\rangle \equiv \sum_{j=0}^{2^n-1} y_j |(j)_2\rangle \tag{60}$$

$|y\rangle\rangle$ を x_j で表すと

$$|y\rangle\rangle = \sum_{k=0}^{2^n-1} y_k |(k)_2\rangle \tag{61}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \sum_{k=0}^{2^n-1} x_j e^{i\frac{2\pi jk}{2^n}} |(k)_2\rangle \tag{62}$$

$$= \sum_{j=0}^{2^n-1} x_j \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{i\frac{2\pi jk}{2^n}} |(k)_2\rangle \right) \tag{63}$$

となる。もし、あるユニタリー変換で、

$$U|(j)_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{i\frac{2\pi jk}{2^n}} |(k)_2\rangle \tag{64}$$

となるようなものがあったとすると、

$$U|x\rangle\rangle = |y\rangle\rangle \tag{65}$$

となる。$|y\rangle\rangle$ の係数を読み取ることで、フーリエ変換の結果を知ることができる。

以下で、そのような U を具体的に構成する。ビット数は n で固定する。

$$\sum_{k=0}^{2^n-1} e^{i\frac{2\pi jk}{2^n}} |(k)_2\rangle = \sum_{k_1=0,1} \cdots \sum_{k_n=0,1} e^{i\frac{2\pi j(k_1 2^{n-1}+\cdots+k_0 2^0)}{2^n}} |k_1 \cdots k_n\rangle \tag{66}$$

$$= \sum_{k_1=0,1} \cdots \sum_{k_n=0,1} e^{i2\pi j(k_1 2^{-1}+\cdots+k_0 2^{-n})} |k_1 \cdots k_n\rangle \tag{67}$$

$$= \left(\sum_{k_1=0,1} e^{i2\pi jk_1 2^{-1}} |k_1\rangle \right) \otimes \cdots \otimes \left(\sum_{k_n=0,1} e^{i2\pi jk_n 2^{-n}} |k_n\rangle \right) \tag{68}$$

$$= \left(|0\rangle + e^{i2\pi j 2^{-1}} |1\rangle \right) \otimes \cdots \otimes \left(|0\rangle + e^{i2\pi j 2^{-n}} |1\rangle \right) \tag{69}$$

ここで、$j2^{-l}$ という因子の 2 進数表記について考える。

$$(j)_2 = j_1 j_2 \cdots j_n \tag{70}$$

とすると、

$$j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0 \tag{71}$$

であるから

$$j2^{-l} = j_1 2^{n-l-1} + j_2 2^{n-l-2} + \cdots + j_n 2^{-l} \tag{72}$$

である。よって、これを 2 進数表記すると

$$(j2^{-1})_2 = (\text{整数部分}).j_n \tag{73}$$
$$(j2^{-2})_2 = (\text{整数部分}).j_{n-1}j_n \tag{74}$$
$$\vdots \tag{75}$$
$$(j2^{-l})_2 = (\text{整数部分}).j_{n-l+1}\cdots j_{n-1}j_n \tag{76}$$
$$\vdots \tag{77}$$
$$(j2^{-n})_2 = (\text{整数部分}).j_1\cdots j_{n-1}j_n \tag{78}$$
$$\tag{79}$$

となる。また、一般に

$$e^{i2\pi j_1\cdots j_{l-1}.j_l\cdots j_n} = e^{i2\pi\left(\cdots+j_{l-2}2^1+j_{l-1}+\frac{j_l}{2^1}\cdots+\frac{j_n}{2^{n-l+1}}\right)} \tag{80}$$
$$= \cdots e^{i2\pi j_{l-2}2^1} e^{i2\pi j_{l-1}} e^{i2\pi\frac{j_l}{2^1}} \cdots e^{i2\pi\frac{j_n}{2^{n-l+1}}} \tag{81}$$
$$= e^{i2\pi\frac{j_l}{2^1}} \cdots e^{i2\pi\frac{j_n}{2^{n-l+1}}} \tag{82}$$
$$= e^{i2\pi\left(\frac{j_l}{2^1}\cdots+\frac{j_n}{2^{n-l+1}}\right)} \tag{83}$$
$$= e^{i2\pi 0.j_l\cdots j_n} \tag{84}$$

のように整数部分は効いてこないことに注意すると、

$$\sum_{k=0}^{2^n-1} e^{i\frac{2\pi jk}{2^n}} |(k)_2\rangle = \left(|0\rangle + e^{i2\pi j2^{-1}}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{i2\pi j2^{-n}}|1\rangle\right) \tag{85}$$
$$= \left(|0\rangle + e^{i2\pi 0.j_n}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{i2\pi 0.j_1\cdots j_n}|1\rangle\right) \tag{86}$$

を得る。よって、求めるべきユニタリー変換 U とは

$$U|(j)_2\rangle = \frac{1}{\sqrt{2^n}}\left(|0\rangle + e^{i2\pi 0.j_n}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{i2\pi 0.j_1\cdots j_n}|1\rangle\right) \tag{87}$$

となるようなものである。

まず、Hadamard ゲートが状態に対して

$$H|j\rangle = \frac{|0\rangle + (-1)^j|1\rangle}{\sqrt{2}} \tag{88}$$

と作用することを思い出す。ここで、2 進小数を導入すると

$$e^{i2\pi 0.0} = 1, \quad e^{i2\pi 0.1} = e^{\frac{i2\pi}{2}} = -1 \tag{89}$$

であるから、

$$H|j\rangle = \frac{|0\rangle + e^{i2\pi 0.j}|1\rangle}{\sqrt{2}} \tag{90}$$

と表すことができる。このことを用い、まず第一番目の bit に Hadamard ゲートを作用させると

$$(H\otimes I\otimes\cdots)|j_1j_2\cdots j_n\rangle = \left(\frac{|0\rangle + e^{i2\pi 0.j_1}|1\rangle}{\sqrt{2}}\right)|j_2\cdots j_n\rangle \tag{91}$$

となる。次に、2 番目の bit を制御ゲートとする位相ゲート R_2 を一番目のゲートに作用させる。3 番目以降の bit は関与しないから、1,2 番目の bit だけに注目して計算してみる。

$$(I \otimes |0\rangle\langle 0| + R_2 \otimes |1\rangle\langle 1|)\left(\frac{|0\rangle + e^{i2\pi 0.j_1}|1\rangle}{\sqrt{2}}\right)|0\rangle = \frac{|00\rangle + e^{i2\pi 0.j_1}|10\rangle}{\sqrt{2}} = \frac{|00\rangle + e^{i2\pi 0.j_1 0}|10\rangle}{\sqrt{2}} \tag{92}$$

$$(I \otimes |0\rangle\langle 0| + R_2 \otimes |1\rangle\langle 1|)\left(\frac{|0\rangle + e^{i2\pi 0.j_1}|1\rangle}{\sqrt{2}}\right)|1\rangle = \left(\frac{|0\rangle + e^{i\frac{2\pi}{2^2}}e^{i2\pi 0.j_1}|1\rangle}{\sqrt{2}}\right)|1\rangle = \frac{|01\rangle + e^{i2\pi 0.j_1 1}|11\rangle}{\sqrt{2}} \tag{93}$$

この結果をまとめると、

$$(I \otimes |0\rangle\langle 0| + R_2 \otimes |1\rangle\langle 1|)\left(\frac{|0\rangle + e^{i2\pi 0.j_1}|1\rangle}{\sqrt{2}}\right)|j_2\rangle = \frac{|0\rangle + e^{i2\pi 0.j_1 j_2}|1\rangle}{\sqrt{2}}|j_2\rangle \tag{94}$$

となる。まったく同様の計算により、

$$C_{n,1}(R_n)\cdots C_{3,1}(R_3)C_{2,1}(R_2)H_1|j_1 j_2 j_3\cdots j_n\rangle = \frac{|0\rangle + e^{i2\pi 0.j_1 j_2 j_3\cdots j_n}|1\rangle}{\sqrt{2}}|j_2 j_3\cdots j_n\rangle \tag{95}$$

となる。以下、残った $|j_2 j_3\cdots j_n\rangle$ の部分に同様な操作を施す。

$$C_{n-1,2}(R_n)\cdots C_{3,2}(R_4)C_{2,2}(R_3)H_2|\bullet j_2 j_3\cdots j_n\rangle = \frac{|0\rangle + e^{i2\pi 0.j_2 j_3\cdots j_n}|1\rangle}{\sqrt{2}}|j_3\cdots j_n\rangle \tag{96}$$

$$C_{n-1,3}(R_n)\cdots C_{3,3}(R_5)C_{2,3}(R_4)H_3|\bullet\bullet j_3\cdots j_n\rangle = \frac{|0\rangle + e^{i2\pi 0.j_3\cdots j_n}|1\rangle}{\sqrt{2}}|j_4\cdots j_n\rangle \tag{97}$$

$$\vdots \tag{98}$$

これらをすべて合わせると、

$$|j_1 j_2\cdots j_n\rangle \to \frac{1}{\sqrt{2^n}}\left(|0\rangle + e^{i2\pi 0.j_1\cdots j_n}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{i2\pi 0.j_n}|1\rangle\right) \tag{99}$$

を得る。最後に SWAP ゲートで状態の入れ替えを行えば完了である。

4.3 位相推定アルゴリズム

ユニタリー演算子 U が固有値 $e^{i\lambda_l}$ をもち、対応する固有状態が $|\psi_l\rangle$ であるとする。固有値の位相は $0 \le \lambda_l \le 2\pi$ として一般性を失わないから、$\lambda_l/2\pi$ は次のように 2 進展開できる:

$$\frac{\lambda_l}{2\pi} = \frac{j_1^{(l)}}{2^1} + \cdots + \frac{j_n^{(l)}}{2^n} \tag{100}$$

ただし、展開が無限次になる場合は、n 桁で打ち切って近似しているものと考える。これを次のように表す。

$$\lambda_l = (2\pi)0.j_1^{(l)}\cdots j_n^{(l)} \tag{101}$$

一般の量子状態 $|\psi\rangle$ を U の固有状態で展開したときの係数を c_l と表すことができる。

$$|\psi\rangle = \sum_l c_l|\psi_l\rangle \tag{102}$$

このとき、$|\psi\rangle$ と n 桁の補助量子ビット $|00\ldots0\rangle$ を

$$V|00\ldots0\rangle|\psi\rangle=\sum_l c_l\left|j_1^{(l)}\cdots j_n^{(l)}\right\rangle|\psi_l\rangle \tag{103}$$

のように変換するアルゴリズムを量子位相推定と呼ぶ。例えば、補助ビットが $|0\cdots0\rangle$ となる確率は

$$\begin{aligned}
&\left|\,|0\cdots0\rangle\langle0\cdots0|\otimes I\sum_l c_l\left|j_1^{(l)}\cdots j_n^{(l)}\right\rangle|\psi_l\rangle\right|^2 && (104)\\
=&\left|\sum_l c_l|0\cdots0\rangle\langle0\cdots0|\left|j_1^{(l)}\cdots j_n^{(l)}\right\rangle|\psi_l\rangle\right|^2 && (105)\\
=&\sum_{ll'}c_lc_{l'}^*\langle\psi_{l'}|\left\langle j_1^{(l')}\cdots j_n^{(l')}\right||0\cdots0\rangle\langle0\cdots0||0\cdots0\rangle\langle0\cdots0|\left|j_1^{(l)}\cdots j_n^{(l)}\right\rangle|\psi_l\rangle && (106)\\
=&\sum_{ll'}c_lc_{l'}^*\delta_{ll'}\left\langle j_1^{(l')}\cdots j_n^{(l')}\right||0\cdots0\rangle\langle0\cdots0|\left|j_1^{(l)}\cdots j_n^{(l)}\right\rangle && (107)\\
=&\sum_l|c_l|^2\left\langle j_1^{(l)}\cdots j_n^{(l)}\right||0\cdots0\rangle\langle0\cdots0|\left|j_1^{(l)}\cdots j_n^{(l)}\right\rangle && (108)\\
=&\sum_l|c_l|^2\left|\langle0\cdots0|\left|j_1^{(l)}\cdots j_n^{(l)}\right\rangle\right|^2 && (109)
\end{aligned}$$

まず準備として、ひとつの補助ビットと U の固有状態のテンソル積状態を考え、それに Hadamard ゲートと制御 U^{2^k} ゲートを作用させる。

$$\begin{aligned}
C_1(U_2^{2^k})H_1|0\rangle|\psi_l\rangle&=C_1(U_2^{2^k})\frac{|0\rangle+|1\rangle}{\sqrt2}|\psi_l\rangle && (110)\\
&=\frac{|0\rangle}{\sqrt2}|\psi_l\rangle+\frac{|1\rangle}{\sqrt2}U^{2^k}|\psi_l\rangle && (111)\\
&=\frac{|0\rangle+e^{2^ki\lambda_l}|1\rangle}{\sqrt2}|\psi_l\rangle && (112)
\end{aligned}$$

ここで、

$$\begin{aligned}
2^0\lambda_l&=(2\pi)2^00.j_1^{(l)}\cdots j_n^{(l)}=(2\pi)0.j_2^{(l)}\cdots j_n^{(l)} && (113)\\
2^1\lambda_l&=(2\pi)2^10.j_1^{(l)}\cdots j_n^{(l)}=(2\pi)j_1^{(l)}.j_2^{(l)}\cdots j_n^{(l)} && (114)\\
2^2\lambda_l&=(2\pi)2^20.j_1^{(l)}\cdots j_n^{(l)}=(2\pi)j_1^{(l)}j_2^{(l)}.j_3^{(l)}\cdots j_n^{(l)} && (115)\\
&\vdots && (116)\\
2^k\lambda_l&=(2\pi)2^k0.j_1^{(l)}\cdots j_n^{(l)}=(2\pi)j_1^{(l)}\cdots j_k^{(l)}.j_{k+1}^{(l)}\cdots j_n^{(l)} && (117)
\end{aligned}$$

であるから、

$$\begin{aligned}
C_1(U_2^{2^k})H_1|0\rangle|\psi_l\rangle&=\frac{|0\rangle+e^{2^ki\lambda_l}|1\rangle}{\sqrt2}|\psi_l\rangle && (118)\\
&=\frac{|0\rangle+e^{(2\pi i)j_1^{(l)}\cdots j_k^{(l)}.j_{k+1}^{(l)}\cdots j_n^{(l)}}|1\rangle}{\sqrt2}|\psi_l\rangle && (119)\\
&=\frac{|0\rangle+e^{(2\pi i)0.j_{k+1}^{(l)}\cdots j_n^{(l)}}|1\rangle}{\sqrt2}|\psi_l\rangle && (120)
\end{aligned}$$

を得る。この結果を用いると、

$$\prod_{k=1}^{n} C_k(U_2^{2^{k-1}})H_k \left|00\cdots0\right\rangle \left|\psi_l\right\rangle \tag{121}$$

$$=\frac{1}{\sqrt{2^n}}\left(\left|0\right\rangle + e^{(2\pi i)0.j_1^{(l)}\cdots j_n^{(l)}}\left|1\right\rangle\right)\left(\left|0\right\rangle + e^{(2\pi i)0.j_2^{(l)}\cdots j_n^{(l)}}\left|1\right\rangle\right)\cdots\left(\left|0\right\rangle + e^{(2\pi i)0.j_n^{(l)}}\left|1\right\rangle\right)\left|\psi_l\right\rangle \tag{122}$$

となるが、これは $\left|j_1 j_2 \cdots j_n\right\rangle$ に量子フーリエ変換を施してできる状態に他ならない。従って、

$$\mathrm{QFT}^\dagger \prod_{k=1}^{n} C_k(U_2^{2^{k-1}})H_k \left|00\cdots0\right\rangle \left|\psi_l\right\rangle = \left|j_1^{(l)} j_2^{(l)} \cdots j_n^{(l)}\right\rangle \left|\psi_l\right\rangle \tag{123}$$

である。よって、$V = \mathrm{QFT}^\dagger \prod_{k=1}^{n} C_k(U_2^{2^{k-1}})H_k$ とすれば良いことが分かった。

5　誤り訂正

5.1　線形符号による古典誤り訂正

最も素朴な誤り訂正の方法は多数決である。例えば、0 というデータがあったとき、これを 000 という風に冗長化したデータを作っておけば、何らかの要因によってビットが部分的に反転してしまい 010 になったとしても、反転前のデータは 000 であろうと推定できる。

k ビットの情報 v（成分が 0 or 1 の k 成分ベクトル）があったとし、これを $n = dk$ ビットのベクトルに冗長化することを考える。冗長化後のベクトルを v', v から v' への変換を G とする。

$$v' = Gv \tag{124}$$

G は $n \times k$ 行列である。この操作を符号化、G を生成行列と呼ぶ。G として冒頭の多数決方式を採用したものを線形符号と呼ぶ。例えば、

$$v = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad G = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \tag{125}$$

と取れば、

$$v' = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{126}$$

となる。

次に、エラーが起きたかどうかを判定する方法を考える。n ビットのベクトルのうち、Gv の形に表されるもの全体の集合を W とする。W の元を符号語と呼ぶ。例えば $(k=2,\, d=3)$

$$v = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{127}$$

は符号語だが、

$$v = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{128}$$

ではない。

各列ベクトルが独立で、$H_c G \equiv 0 \pmod 2$ を満たすような $(n-k)\times n$ 行列 H_c があったとする。これを検査行列と呼ぶ。任意の符号語 w について

$$H_c w = H_c G v = 0 \tag{129}$$

が成り立つ。また逆に、$H_c w = 0$ ならば、w は符号語であることも示せるらしい。このようにして、符号語の 2 通りの特徴付けを得た。

- G を用いた見方: ベクトルが適切に水増しされている。
- H_c を用いた見方: ブロック内の隣接するビットが等しい。

$w \in W$ のときに限りゼロになるようなベクトル $s = H_c w$ を w のシンドローム、その成分をシンドローム値と呼ぶ。ひとつでも 0 でないシンドローム値があれば、w にはエラーが起きていることになる。シンドローム値がすべて 0 のときは、w にはエラーがないか、エラー自身が $H_c e = 0$ を満たしているかのどちらかである。

（例 $k=3, n=9$）線形符号 G に対する検査行列は以下を取ればよい。

$$H_c = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \tag{130}$$

実際

$$\begin{pmatrix}1&1&0&0&0&0&0&0&0\\0&1&1&0&0&0&0&0&0\\0&0&0&1&1&0&0&0&0\\0&0&0&0&1&1&0&0&0\\0&0&0&0&0&0&1&1&0\\0&0&0&0&0&0&0&1&1\end{pmatrix}\begin{pmatrix}1&0&0\\1&0&0\\1&0&0\\0&1&0\\0&1&0\\0&1&0\\0&0&1\\0&0&1\\0&0&1\end{pmatrix}=\begin{pmatrix}2&0&0\\2&0&0\\0&2&0\\0&2&0\\0&0&2\\0&0&2\end{pmatrix}\equiv\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\\0&0&0\\0&0&0\\0&0&0\end{pmatrix} \tag{131}$$

となり OK である。符号語 w に対して H_cw を計算すると、

$$H_cw=\begin{pmatrix}1&1&0&0&0&0&0&0&0\\0&1&1&0&0&0&0&0&0\\0&0&0&1&1&0&0&0&0\\0&0&0&0&1&1&0&0&0\\0&0&0&0&0&0&1&1&0\\0&0&0&0&0&0&0&1&1\end{pmatrix}\begin{pmatrix}0\\0\\0\\1\\1\\1\\0\\0\\0\end{pmatrix}=\begin{pmatrix}0\\0\\2\\2\\0\\0\end{pmatrix}\equiv\begin{pmatrix}0\\0\\0\\0\\0\\0\end{pmatrix} \tag{132}$$

となる。もしエラーが混入していると、

$$H_cw=\begin{pmatrix}1&1&0&0&0&0&0&0&0\\0&1&1&0&0&0&0&0&0\\0&0&0&1&1&0&0&0&0\\0&0&0&0&1&1&0&0&0\\0&0&0&0&0&0&1&1&0\\0&0&0&0&0&0&0&1&1\end{pmatrix}\left(\begin{pmatrix}0\\0\\0\\1\\1\\1\\0\\0\\0\end{pmatrix}+\begin{pmatrix}0\\0\\0\\1\\0\\0\\0\\0\\0\end{pmatrix}\right)=\left(\begin{pmatrix}0\\0\\2\\2\\0\\0\end{pmatrix}+\begin{pmatrix}0\\0\\1\\0\\0\\0\end{pmatrix}\right)\equiv\begin{pmatrix}0\\0\\1\\0\\0\\0\end{pmatrix} \tag{133}$$

となる。

5.2 量子誤り訂正

現在知られている量子誤り訂正は、線形符号を量子計算版とでもいうべきものである。具体例から考える。1 ビットの情報を 3 ビットに冗長化することを考える。ここでは、符号化前の量子状態もあらかじめ 3bit で用意しておき、情報は 1bit 目に格納しておくことにする。よって符号化 G として

$$|000\rangle \to |000\rangle \tag{134}$$
$$|100\rangle \to |111\rangle \tag{135}$$

となるようなものを用意できれば良い。これは CNOT ゲート

$$\Lambda_{1,2}(X) = P_0 \otimes I \otimes I + P_1 \otimes X \otimes I \tag{136}$$
$$\Lambda_{1,3}(X) = P_0 \otimes I \otimes I + P_1 \otimes I \otimes X \tag{137}$$

で実現できる。実際、

$$\Lambda_{1,2}(X)\Lambda_{1,3}(X)\left|000\right\rangle = \left|000\right\rangle \tag{138}$$
$$\Lambda_{1,2}(X)\Lambda_{1,3}(X)\left|100\right\rangle = \left|111\right\rangle \tag{139}$$

となる。

次にシンドロームを調べる方法を考える。

$$M_0^{(1)} = \frac{I + Z_1 Z_2}{2}, \quad M_1^{(1)} = \frac{I - Z_1 Z_2}{2} \tag{140}$$

という 2 つの演算子を考えると、これらは POVM をなし、

$$M_0^{(1)}\left|000\right\rangle = \frac{1+1}{2}\left|000\right\rangle = \left|000\right\rangle \tag{141}$$
$$M_0^{(1)}\left|100\right\rangle = \frac{1-1}{2}\left|100\right\rangle = 0 \tag{142}$$
$$M_0^{(1)}\left|010\right\rangle = \frac{1-1}{2}\left|010\right\rangle = 0 \tag{143}$$
$$M_0^{(1)}\left|110\right\rangle = \frac{1+1}{2}\left|110\right\rangle = \left|110\right\rangle \tag{144}$$

$$M_1^{(1)}\left|000\right\rangle = \frac{1-1}{2}\left|000\right\rangle = 0 \tag{145}$$
$$M_1^{(1)}\left|100\right\rangle = \frac{1+1}{2}\left|100\right\rangle = \left|100\right\rangle \tag{146}$$
$$M_1^{(1)}\left|010\right\rangle = \frac{1+1}{2}\left|010\right\rangle = \left|010\right\rangle \tag{147}$$
$$M_1^{(1)}\left|110\right\rangle = \frac{1-1}{2}\left|110\right\rangle = 0 \tag{148}$$

より、

$$\mathrm{tr}(\left|ij0\right\rangle\left\langle ij0\right| M_0^1) = \delta_{ij}, \tag{149}$$
$$\mathrm{tr}(\left|ij0\right\rangle\left\langle ij0\right| M_1^1) = 1 - \delta_{ij} \tag{150}$$

となるから、M_1^1 の期待値が、1,2 番のビットに関するシンドローム値を与えることが分かる。全く同様にして、

$$M_0^{(2)} = \frac{I + Z_2 Z_3}{2}, \quad M_1^{(2)} = \frac{I - Z_2 Z_3}{2} \tag{151}$$

も測定すれば、すべてのシンドローム値が得られる。古典的な誤り訂正の場合、シンドローム値は 0 か 1 であったが、量子計算の場合はそれ以外の中途半端な値を取りうる。例えば、$\left|\psi\right\rangle = (\left|000\right\rangle + \left|010\right\rangle)/\sqrt{2}$ のとき、

$$M_0^{(1)}\left|\psi\right\rangle \frac{1}{\sqrt{2}}(\left|000\right\rangle + \left|010\right\rangle) = \frac{\left|000\right\rangle}{\sqrt{2}} \tag{152}$$

より、

$$\mathrm{tr}(\left|\psi\right\rangle\left\langle\psi\right| M_0^{(1)}) = \frac{1}{2} \tag{153}$$

となる。

以下では簡単のため、このような位相を変化させるエラーはなく、ビット反転を引き起こすエラーのみを考える。そのようなエラーを引き起こす操作は

$$E = X_1^{e_1} X_2^{e_1} X_3^{e_1} \tag{154}$$

と書ける。ただし、$e_1, e_2, e_3 = 0, 1$ である。仮に、$|000\rangle$ がオリジナルのデータで、これに、$e_1 = 1, e_2 = e_3 = 0$ のエラーが乗ったとすると、

$$E\,|000\rangle = X_1\,|000\rangle = |100\rangle \tag{155}$$

となる。この状態のシンドローム値を完全に調べると、1 番目のビットに反転があることが分かるから、状態に再度 X_1 を作用させればもとの状態を復元することができる。

$$R\,|100\rangle = X_1\,|100\rangle = |000\rangle \tag{156}$$

これでエラー訂正が完了した。

5.3 スタビライザー符号

6 Summary