量子アルゴリズム
Shorの素因数分解アルゴリズム

計算アルゴリズム論

今井浩

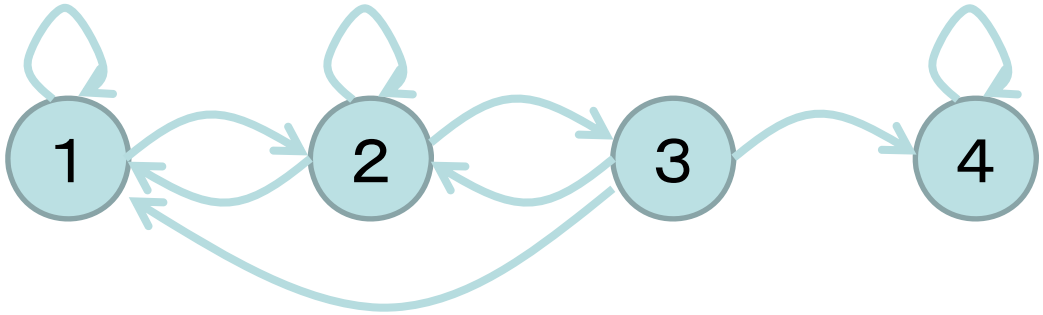
計算とは？
―状態遷移―

決定性計算

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}^{t(n)} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

確率化計算

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0.5 & 0.2 & 0.1 & 0 \\ 0.5 & 0.3 & 0.1 & 0 \\ 0 & 0.5 & 0 & 0 \\ 0 & 0 & 0.8 & 1 \end{pmatrix}^{t(n)} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$



量子計算

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0.64 & 0.48 & -0.48 & -0.36 \\ 0.48 & -0.64 & -0.36 & 0.48 \\ 0.48 & 0.36 & 0.64 & 0.48 \\ 0.36 & -0.48 & 0.48 & -0.64 \end{pmatrix}^{t(n)} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

純粋状態でのテンソル積と量子もつれ

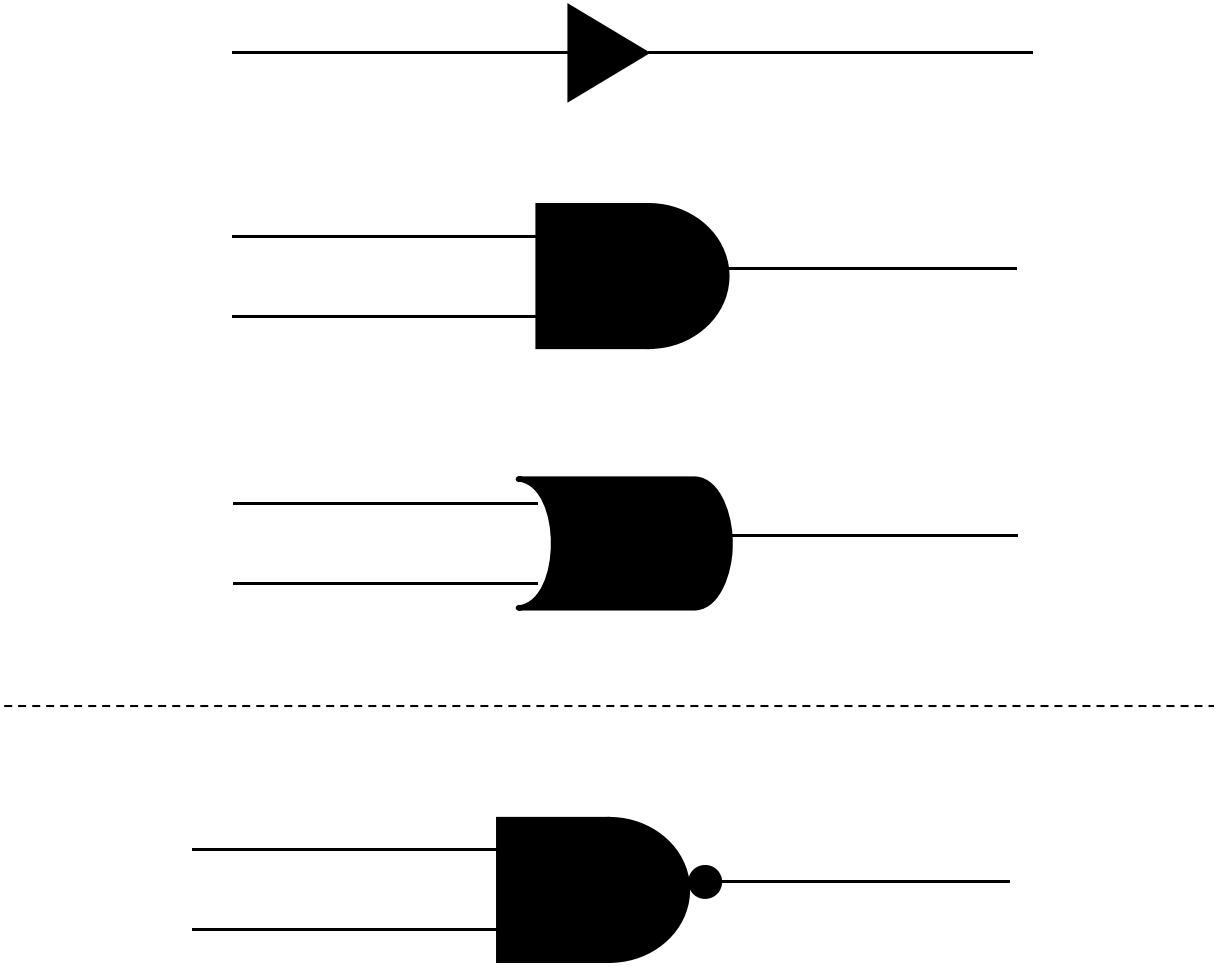
$\mathbf{C^2}$基底 $|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$, $|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$　　$|\phi\rangle=\begin{pmatrix}\alpha\\\beta\end{pmatrix}$, $|\alpha|^2+|\beta|^2=1$

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

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

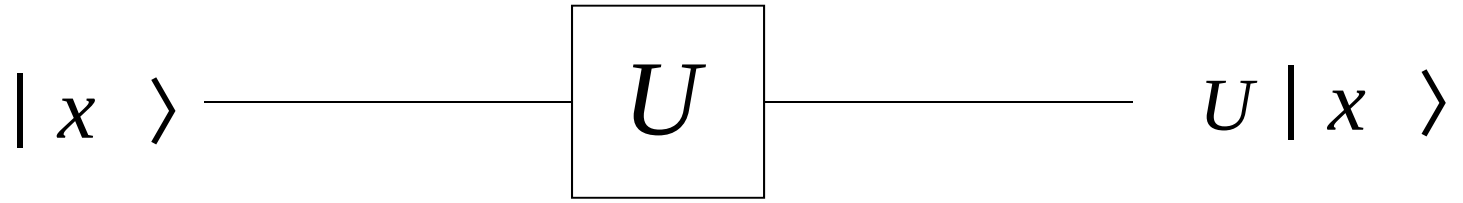
$\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$=???　分解不能, entangled

論理回路

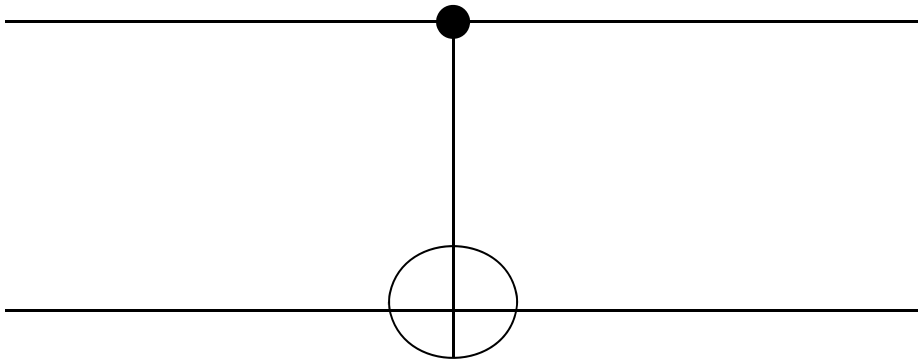


万能回路

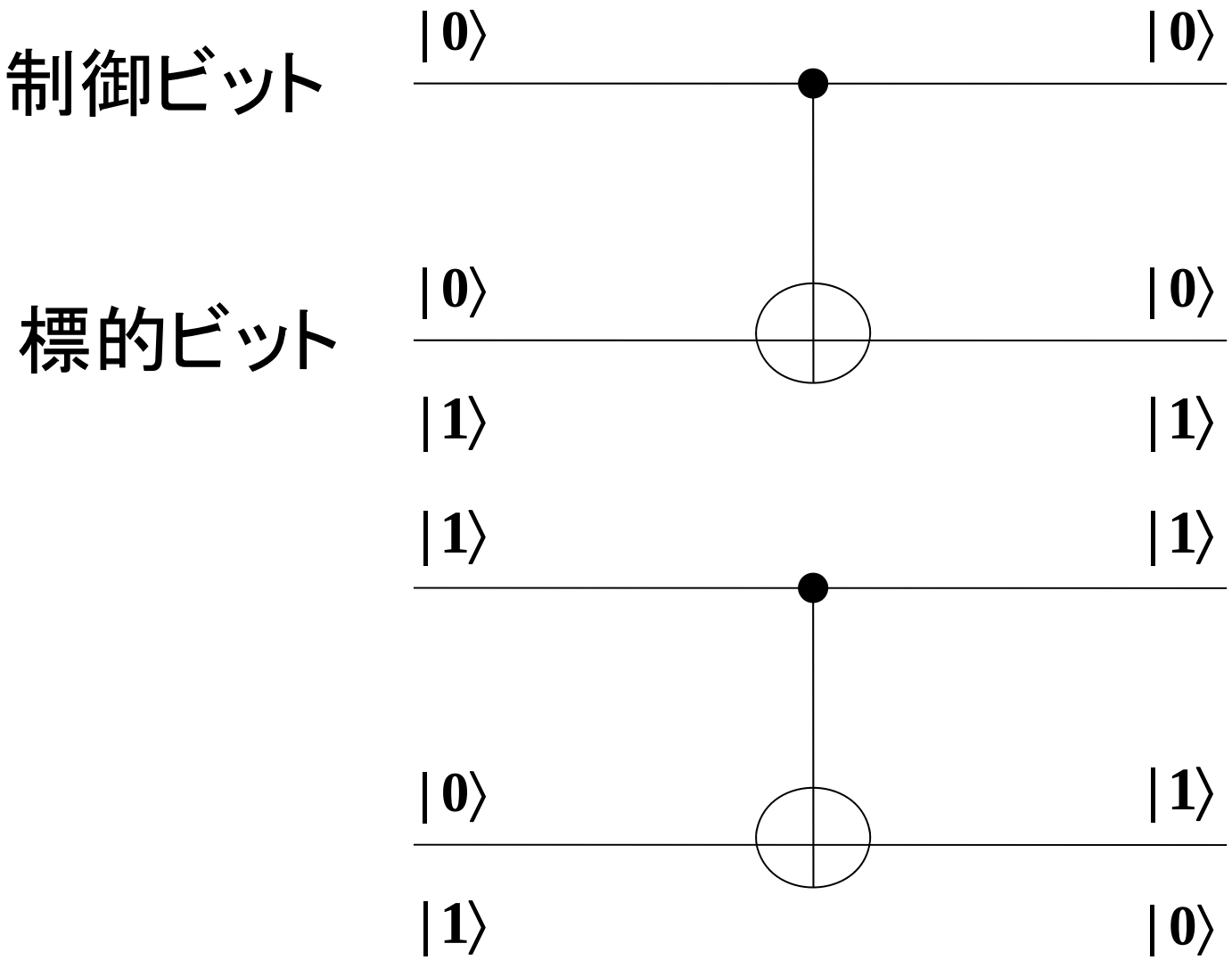
- Uゲート
  - 1量子ビットに対する任意のユニタリ変換



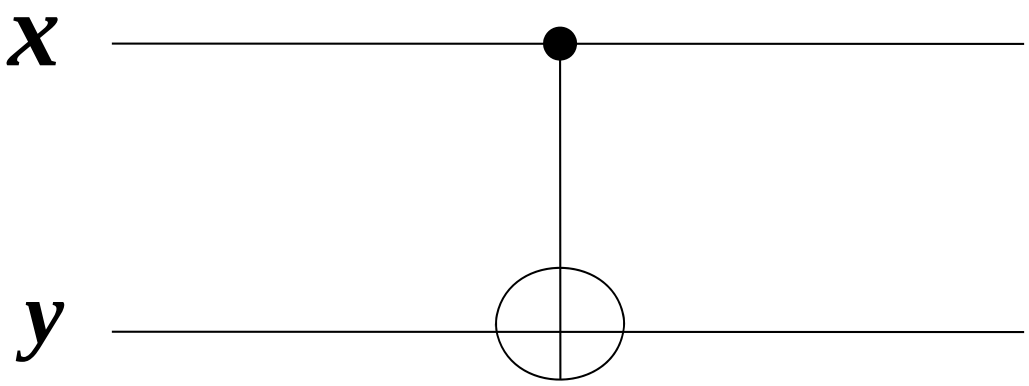
- 制御NOT ゲート （Controlled-NOT）



Controlled-NOT



Controlled-NOT



$(x + y \mod 2)$

x	y	x	$x \oplus y$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

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

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

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

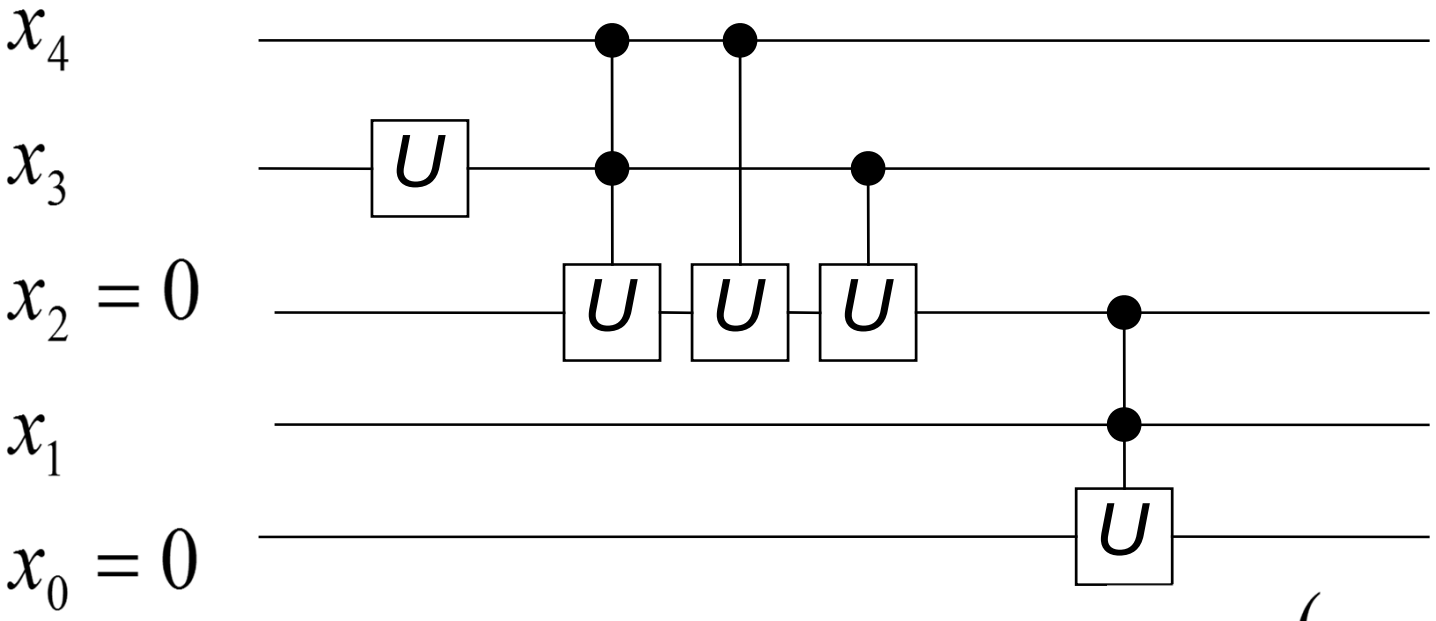
$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

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

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

量子回路

- ワイア : 1qubit
- 時間 : 左から右へ
  - アルゴリズムの記述が簡単

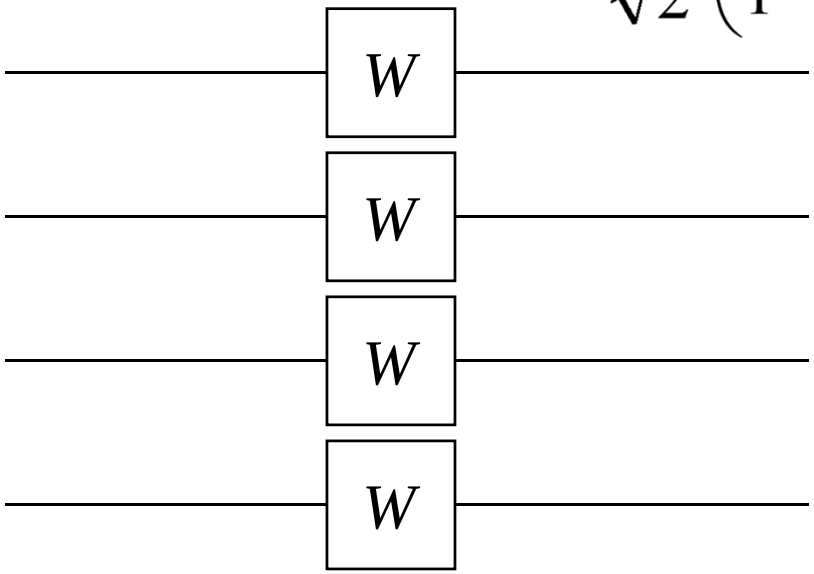


$$x_0 = \left(x_4 \vee \neg x_3\right) \wedge x_1$$

($U = I$)

Walsh-Hadamard 変換

- 全ビットに $W = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ をかける



$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

- 等重の重ね合わせ状態
- 干渉効果

$O(n2^n)$

$O(n)$

観測により真にランダムな乱数が得られる

$$H_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

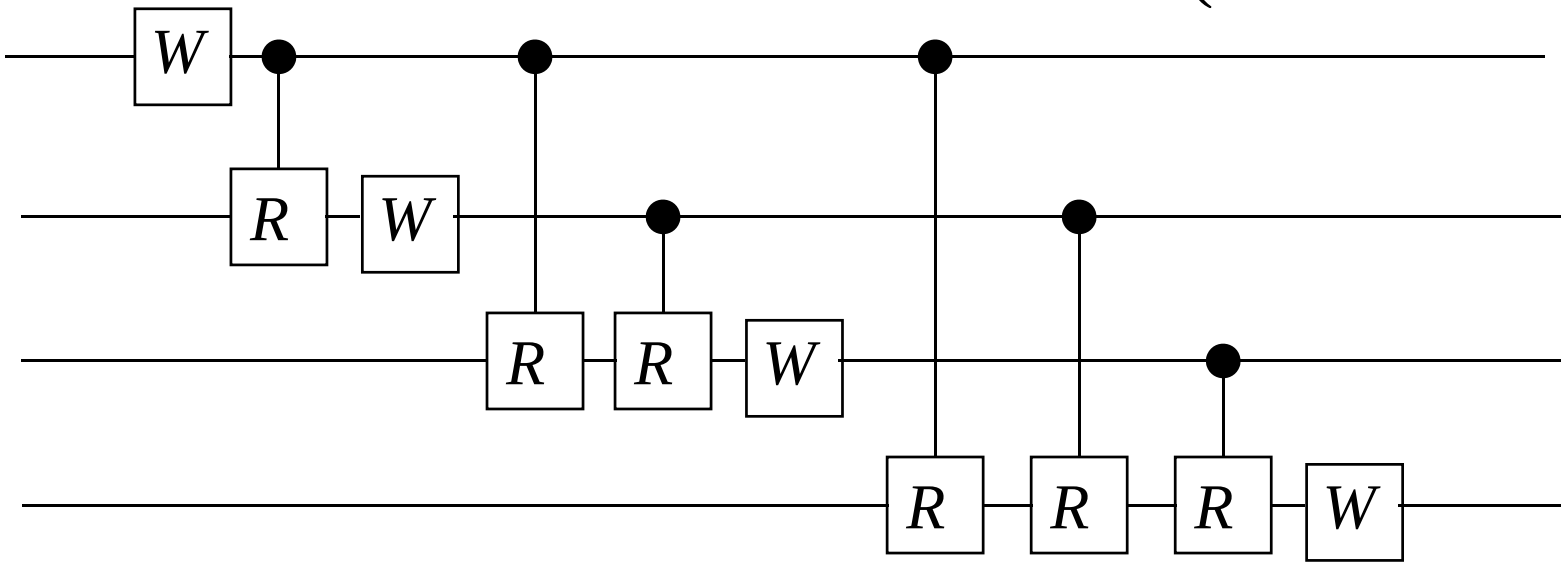
$$H_2 = H_1 \otimes H_1 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H_3 = \frac{1}{2\sqrt{2}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

離散フーリエ変換

- 周期を検出するための前処理

$$\mathbf{DFT}: |x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i xy/2^n} |y\rangle \qquad R = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{\pi i/2^{k-j}} \end{pmatrix}$$



$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\otimes\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & & 1 & \\ & 1 & & 1\\ 1 & & -1 & \\ & 1 & & -1\end{pmatrix}=A$$

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\otimes\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 & & \\ 1 & -1 & & \\ & & 1 & 1\\ & & 1 & -1\end{pmatrix}=B$$

$$\begin{pmatrix}1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{-\frac{\pi i}{2}}\end{pmatrix}=C,\qquad ACB=\frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & e^{-\frac{\pi i}{2}} & -e^{-\frac{\pi i}{2}}\\ 1 & 1 & -1 & -1\\ 1 & -1 & -e^{-\frac{\pi i}{2}} & e^{-\frac{\pi i}{2}}\end{pmatrix}$$

$$ACB = \frac{1}{2}\begin{array}{c} \begin{matrix} 00 & 10 & 01 & 11 \end{matrix} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & e^{-\frac{\pi i}{2}} & -e^{-\frac{\pi i}{2}} \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -e^{-\frac{\pi i}{2}} & e^{-\frac{\pi i}{2}} \end{pmatrix} \end{array}$$

$$\begin{pmatrix} y_{00} \\ y_{01} \\ y_{10} \\ y_{11} \end{pmatrix} = ACB \begin{pmatrix} x_{00} \\ x_{10} \\ x_{01} \\ x_{11} \end{pmatrix}$$

$$\left| y_j \right\rangle = \sum_{k=0}^{3} e^{-\frac{\pi i j k}{2}} \left| x_k \right\rangle$$

Shorのアルゴリズム

古典素因数分解アルゴリズム

- 2次ふるい法
- 数体ふるい法
- 楕円曲線法

$$x^2 \equiv y^2 \pmod{n}$$

Shor の素因数分解アルゴリズム

- 古典ふるい法と同様に、問題を位数発見に帰着
- $x^r \equiv 1 \pmod{n}$ となる最小のr を見つける

  (位数発見問題)

  (x : 1から$n-1$のnと互いに素なランダムな整数)

ここで、r が偶数だと同様にできる。

例

例 : $3 \times 5 = 15$

$\mathbf{Z}_{15}^{*} = \{1,2,4,7,8,11,13,14\}$, 位数1 : 1, 2 : 4,11,14, 4 : 2,7,8,13

$a = 14$のみ$a^{\frac{r}{2}} \equiv -1 \pmod{15}$

$a = 7$なら、$7^2 - 1 \equiv 3 \pmod{15}$, $7^2 + 1 \equiv 5 \pmod{15}$

$n = 15,\ x = 7, \quad N = 2^4 = 16$

$$\frac{1}{4}\sum_{k=0}^{15} |k\rangle|0\rangle$$

$$k \mapsto 7^k \pmod{15}$$

$$\frac{1}{4}(|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + \cdots + |15\rangle|13\rangle)$$

$$= \frac{1}{4}((|0\rangle + |4\rangle + |8\rangle + |12\rangle)|1\rangle + (|1\rangle + |5\rangle + |9\rangle + |13\rangle)|7\rangle$$

$$+ (|2\rangle + |6\rangle + |10\rangle + |14\rangle)|4\rangle + (|3\rangle + |7\rangle + |11\rangle + |15\rangle)|13\rangle)$$

逆Fourier変換

$$\frac{1}{4}((|0\rangle + |4\rangle + |8\rangle + |12\rangle)|1\rangle + (|0\rangle - i|4\rangle - |8\rangle + |12\rangle)|7\rangle$$

$$+ (|0\rangle - |4\rangle + |8\rangle + |12\rangle)|4\rangle + (|0\rangle - i|4\rangle - |8\rangle + i|12\rangle)|13\rangle)$$

0,4,8,12をそれぞれ確率$1/4$で観測

フーリエ変換

時間領域から
周波数領域へ

$$X(\omega) = \sqrt{\frac{1}{2\pi}} \int_{-\infty}^{+\infty} x(t) \mathrm{e}^{-i\omega t} \mathrm{d}t$$

周波数領域から
時間領域へ

$$x(t) = \sqrt{\frac{1}{2\pi}} \int_{-\infty}^{+\infty} X(\omega) \mathrm{e}^{i\omega t} \mathrm{d}\omega$$

離散フーリエ
変換

$$X(k) = \sqrt{\frac{1}{N}} \sum_{n=0}^{N} x(n) \mathrm{e}^{-\frac{2\pi \mathrm{i} nk}{N}}$$

$$x(n) = \sqrt{\frac{1}{N}} \sum_{k=0}^{N} X(k) \mathrm{e}^{\frac{2\pi \mathrm{i} nk}{N}}$$

周期関数を変換
→ 周期情報