1 Shor's algorithm

1.1 アルゴリズムの目標

$M \in \mathbb{Z}_{>0}$ に対して, 次の 2 つの条件を満たす函数 $f : \mathbb{N} \to \{0, M-1\}$ を考える.
【条件】
1. 周期 $^{\exists!}r$ (i.e) for $^{\forall}x \in \mathbb{N}$, $f(x+r) = f(x)$
2. $f(0), \cdots, f(r-1)$ are all distinct.

1.2 アルゴリズムの戦略

ここで述べる Shor のアルゴリズムは, IQFT を用いない確率的なアルゴリズムである. まず, 記号の準備をする.

$$\begin{array}{lrcl} for\ \ a \in \mathbb{N}, & f_a : \mathbb{N} & \to & \{0, \cdots, M-1\} \\ & x & \mapsto & a^x \mod M. \end{array} \tag{1}$$

Step1. M(n bit) の整数, $a \in \{1, M-1\}$ を gcd $(a, M) = 1$ を満たす整数とする. さらに Q を

$$M^2 \leq Q = 2^\ell \leq 2 \cdot M^2 \tag{2}$$

を満たす最小の 2 べきの数とする.
Step 2. 等重の並列状態にする. $\frac{1}{\sqrt{Q}} \sum_{x}^{Q-1} |x\rangle$
Step 3. Quantum part (後述) return $\sum_x \alpha_x |x\rangle|k\rangle$
Step 4. 第一レジスタを観測する.
Step 5. 周期 r を Step 4. で得た数値から推定する. もし Step4 での数値が "good number " なら, r を推測できる. そうでなければ, 再度 Step 3 に戻る.

2 Good Number

定義 1. $x \in \{0, \cdots, Q-1\}$ が " Good number "であるとは,

$$^{\exists}(t, r) : \text{互いに素}\ \ (s.t)\ \ t \cdot Q - x \cdot r = k\ \ where\ \ -r/2 \leq k \leq r/2 \tag{3}$$

例として, $Q = 256$
$t = 1.0, r = 4, x = 64, k = 0$
$t = 3.0, r = 4, x = 192, k = 0$

定理 2. x が Good number の時, 連分数展開によって, 周期 r が一意的に定まる.

証明. Good number の定義から,

$$\left| \frac{x}{Q} - \frac{t}{r} \right| \leq \frac{1}{2Q} \leq \frac{1}{M^2} \leq \frac{1}{r^2} \tag{4}$$

連分数展開について次の定理がある.

定理 3. $\frac{P}{Q}$ を $\|\frac{P}{Q}-x\|<\frac{1}{2Q^2}$ を満たす任意の有理数とする時、$\frac{P}{Q}$ は x の近似分数である。さらに、その近似分数は P,Q の最大公約数は 1 である.

□

補題 4. There are $\Omega\left(\frac{r}{\log\log r}\right)$ good numbers.

3 Quantum part of the Algorithm

ここでは, Step 3, 4 について述べる.
Quantum-Step 1. 次の量子重ね合わせ状態を構成する.

$$\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle\otimes|f_a(x)\rangle \tag{5}$$

Quantum-Step 2. 離散フーリエ変換

$$\begin{array}{rcl}\mathcal{F}_Q:\mathbb{C}^Q & \to & \mathbb{C}^Q \\ |x\rangle & \mapsto & \frac{1}{\sqrt{Q}}\sum_{k=0}^{Q-1}\exp\left(2\pi i\frac{x\cdot k}{Q}\right)|k\rangle\end{array}$$

を第一レジスタに作用させる. この時, 量子状態を

$$\sum_{(xy),x\in\{0,Q-1\}} b(xy)|x\rangle\otimes|y\rangle \tag{6}$$

とする.
Quatnum-Step 3. 第一レジスタを観測する.

3.1 Analysis

補題 5. Quantum-Step2 について, $b(xy)$ は, $f(x_0)=y, T=1+\lfloor\frac{Q-x_0}{r}\rfloor$ とした時,

$$b(xy)=\omega^{x_0+(T-1)r}\frac{1}{Q}\left(\frac{\sin(T\cdot\pi xr/Q)}{\sin(\pi xr/Q)}\right) \tag{7}$$

証明. □

(7) について, x が Good number (3), i.e. $tQ-xr=k$ の時,

$$\begin{aligned} b(xy) &= \omega^{x_0+(T-1)r}\frac{1}{Q}\left(\frac{\sin(T\cdot\pi xr/Q)}{\sin(\pi xr/Q)}\right) \\ &= \omega^{x_0+(T-1)r}\frac{1}{Q}\left(\frac{\sin(T\cdot\pi\frac{tQ-xr}{Q})}{\sin(\pi\frac{tQ-xr}{Q})}\right)\end{aligned}$$

T の定義から

$$T\le 1+\frac{Q}{r} \tag{8}$$

x が Good number であることから,

$$-\frac{r}{2Q} \leq \frac{tQ - xr}{Q} = \frac{k}{Q} \leq \frac{r}{2Q} \tag{9}$$

(8) ,(9) から

$$T \cdot \frac{tQ - xr}{Q} \leq \frac{1}{2} + \frac{r}{2Q} \tag{10}$$

(2) から,

$$\frac{Q}{r} > \frac{M^2}{r} > M \tag{11}$$

であることを思い出しておく. 先ほどの (10) から

$$\pi \cdot T \cdot \frac{tQ - xr}{Q} \leq \pi \left(\frac{1}{2} + \frac{r}{2Q} \right) \leq \pi \left(\frac{1}{2} + \frac{1}{2M} \right) \tag{12}$$

ここで,

$$\alpha := \frac{tQ - xr}{Q}. \tag{13}$$

と置いたとき, (12) は

$$T \cdot \alpha \leq \pi \left(\frac{1}{2} + \frac{1}{2M} \right) \tag{14}$$

となることがわかり、よって

$$\|b(xy)\|^2 = \left\| \frac{1}{Q} \left(\frac{\sin(T \cdot \alpha)}{\sin \alpha} \right) \right\|^2 \tag{15}$$

$$\geq \frac{T^2}{Q^2} \left(\frac{\sin(T \cdot \alpha)}{T\alpha} \right)^2 \tag{16}$$

$\frac{\sin(x)}{x}$ を, 微分した時の分子は, $\cos x \cdot (x - \tan x)$ となるため $0 \leq x \leq \frac{\pi}{2}$ で単調減少する.

4　考察

Good number は以下の通り. ($M = 15, a = 2$ の時) 参考: $r = 4$

Case 1 : $Q = 2$ の時

Case 2 : $Q = 4$ の時

$t = 1.0, x = 1, k = 0$

なので $\frac{Goodnumber \text{ の数}}{Q} = \frac{1}{4}$

一方で, Shor のアルゴリズムによると, $x = 1$ が出力される確率は (7) より $\frac{1}{4}$ とわかる.

Case 3 : $Q = 8$ の時

$t = 1.0, x = 2, k = 0;$

$t = 3.0, x = 6, k = 0;$

$\frac{Goodnumber \text{ の数}}{Q} = \frac{1}{4}$ である一方で、理論値では $\frac{3}{16}$

Case 4 : $Q = 16$ の時

$t = 1.0, x = 4, k = 0$

$t = 3.0, x = 12, k = 0$

$\frac{Goodnumber\text{ の数}}{Q} = \frac{1}{8}$ である一方で、理論値では $\frac{1}{8}$
Case 5 : $Q = 32$ の時
t$= 1.0, x = 8, k = 0$
$t = 3.0, x = 24, k = 0$

5 考えたいこと

サンプリングごとに Q を変えていって search する.

6 RSA 暗号と素因数分解問題について

p, q を素数として $M = p \cdot q$. この時,

$$(M/M\mathbb{Z})^* \simeq (M/p\mathbb{Z})^* \times (M/q\mathbb{Z})^* . \tag{17}$$

今, $e \in (M/M\mathbb{Z})^*$ に対して, ${}^{\exists}e' \in (M/M\mathbb{Z})^*$ s.t $e \cdot e' = 1 \mod (p-1) \cdot (q-1)$. ここで, e が公開情報, e' が秘密情報となる.
【暗号化】
メッセージ m に対して m^e で暗号化する.
復号は, $e \cdot e' =^{\exists} k \cdot (p-1) \cdot (q-1) + 1$ だから, $(m^e)^{e'} = m^{e \cdot e'} = m^{k \cdot (p-1) \cdot (q-1) + 1} = m$ となる.

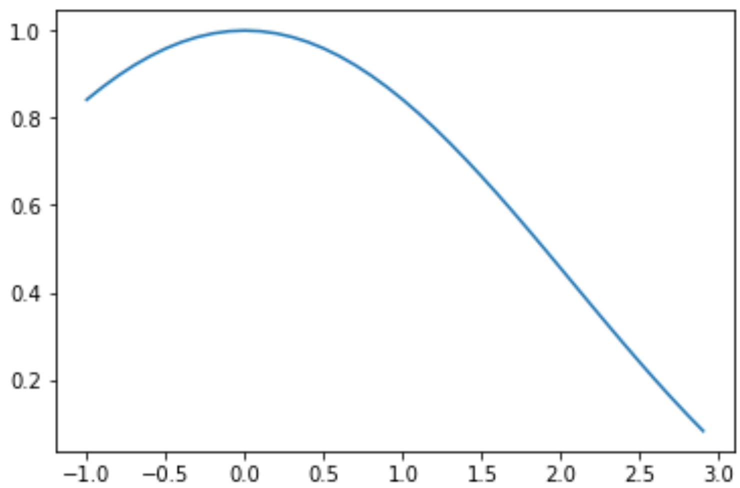

図 1 $5^{\frac{sin(x)}{x}}$