Shor のアルゴリズム解説

@0917datw

はじめに

本スライドは，下記の論文解説を行なうものである．
本論文では，量子コンピュータによって素因数分解問題や離散対数問題を解読できることを示している．

P. W. Shor:
"Algorithms for Quantum Computation: Discrete Logarithms and Factoring",
Proceedings of IEEE Symposium on Foundations of Computer Science (FOCS'94),
pp.124-134, 1994.

目次

1. Shor の素因数分解アルゴリズムの概要
2. 量子計算量理論入門
3. Shor の素因数分解アルゴリズムの詳細
4. Shor の素因数分解アルゴリズムの実装
5. Shor の離散対数アルゴリズムの詳細

1. Shor の素因数分解アルゴリズムの概要

Shor の素因数分解アルゴリズムの概要

Shor の素因数分解アルゴリズムの概要は次のようになる．
正整数 a, b に対して，(a, b) で a と b の最大公約数を表す．

Input： N
Output： N のある素因数

(i). $x \in \{1, \cdots, N-1\}$ をランダムに選ぶ
(ii). (x, N) が 1 でなければその値を出力して終了し，1 なら (iii) へ
(iii). $\mathrm{mod}\ N$ における x の位数 r を計算する
(iv). r が偶数かつ $x^{r/2} \neq N-1 \mod N$ なら $(x^{r/2}-1, N)$ を出力する，そうでなければ (i) へ戻る

Shor の素因数分解アルゴリズムの補足

- $x^r \equiv 1 \bmod N$ なる r は存在するのか？

$\rightarrow$ x と N が互いに素ゆえ，$r = \phi(N)$ での下記の Euler の定理から従う．つまり，$\{1 \leq r \leq N-1 | x^r \equiv 1 \bmod N\}$ なる集合は空でない．

- (iv) での $(x^{r/2}-1, N)$ は N の素因数になっているのか？

$\rightarrow$ まず，r が位数ゆえ，$x^{r/2}-1 \not\equiv 0 \bmod N$ に注意する．
$(x^{r/2}-1, N) = 1$ と仮定すると，$x^r - 1 = (x^{r/2}-1)(x^{r/2}+1)$
$\equiv 0 \bmod N$ ゆえ，$x^{r/2}+1 \equiv 0 \bmod N$ となるが，これは
$x^{r/2} \not\equiv N-1 \bmod N$ に矛盾．
よって，$(x^{r/2}-1, N) \geq 2$ ゆえ成り立つ．

Thm(Euler)

x と N が互いに素のとき，$x^{\phi(N)} \equiv 1 \bmod N$
ここで，$\phi(N)$ で N と互いに素で 1 以上 N 以下の自然数の個数を表す

Shor の素因数分解アルゴリズムの補足

- どの程度の確率で (iv) の「r が偶数かつ $x^{r/2} \not\equiv N-1 \mod N$」なる条件は満たされるのか？

$\rightarrow$ 下記の Thm[1] が確率の下界を与える.

Thm

$N = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ で奇素数の素因数分解とする.
$x \in (\mathbb{Z}/N\mathbb{Z})^{\times}$ をランダムに選び，r を $\mathrm{mod}\ N$ での x の位数とするとき，r が偶数かつ $x^{r/2} \not\equiv N-1 \mod N$ なる確率は $1 - \dfrac{1}{2^m}$ 以上である.

Shor の素因数分解アルゴリズムの具体例

$N = 35$ の場合での具体例
1) $x = 8$
$8^4 \equiv 1 \mod 35$ **であり，** 8 **の** $\mathrm{mod}\ 35$ **での位数は** 4.
よって，$(8^2 - 1, 35) = (63, 35) = 7$ **であり，上手く行っている.**
2) $x = 16$
$16^3 \equiv 1 \mod 35$ **であり，** 8 **の** $\mathrm{mod}\ 35$ **での位数は** 3 **で奇数.**
3) $x = 19$
$19^6 \equiv 1 \mod 35$ **であり，** 19 **の** $\mathrm{mod}\ 35$ **での位数は** 6.
しかし，$(19^3 - 1, 35) = (6858, 35) = 1$ **である.**

2. 量子計算量理論入門

量子計算の定義

以下では，$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ として，古典ビットの 0 と 1 に対応する量子ビット（以下単にビット，量子状態ともいう）をそれぞれ $|0\rangle, |1\rangle$ で表す．また，$\langle 0|, \langle 1|$ をそれぞれ $|0\rangle, |1\rangle$ の転置とする．

量子計算とは次のような操作である [2]．

1. 量子コンピュータの状態は，複素係数の振幅を持ち，

$$\sum_{z\in\{0,1\}^n} c_z|z\rangle$$

というベクトルで与えられる．
ここで，$c_z \in \mathbb{C}$ s.t. $\sum_{z\in\{0,1\}^n} |c_z|^2 = 1$ であり，$|z\rangle$ は，z を n ビット列として，各ビットの Tensor 積を表す．

量子計算の定義

2. 計算の開始時，量子計算機はある初期状態 $|\psi_1\rangle$ にある．
3. 状態ベクトルを変化させる際には，ユニタリ変換（転置共役が逆行列と等しい）によって得られる．
4. 最終状態が ψ_t で，

$$\psi_t = \sum_{z\in\{0,1\}^n} c_z|z\rangle$$

とするとき，これを測定すると，状態 $|z\rangle$ を確率 $|c_z|^2$ で得る．
測定値 z を得る確率は $|c_z|^2$ である，ともいう．

量子計算の具体例

古典ビットでの「01」は,

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

という量子状態で表せる.
また, 初期状態が $|0\rangle$ の際に,

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

として, $|0\rangle$ に H を 2 回作用させると, $|0\rangle$ が得られる. これは, 測定値 0 を得る確率は 1 で, 測定値 1 を得る確率は 0 なので, 確実に測定値 0 を得ることを意味する.

量子 Fourier 変換

2 べきで表せる正整数 q i.e. $\exists k$ s.t. $q = 2^k$ を取る．$z \in \{0,1\}^k$ で z を 2 進数とみたときに，10 進展開した整数を T_z として，$|T_z\rangle := |z\rangle$ とみなす．
例えば，2 量子ビットなら，$|0\rangle = |00\rangle, |1\rangle = |01\rangle, |2\rangle = |10\rangle$, $|3\rangle = |11\rangle$ である．

$0 \leq a \leq q-1$ としたとき，

$$\mathscr{F}|a\rangle := \frac{1}{q^{1/2}} \sum_{b=0}^{q-1} \exp\left(2\pi\sqrt{-1}\frac{ab}{q}\right)|b\rangle$$

なる状態を状態 $|a\rangle$ に対する量子 Fourier 変換という．これはユニタリ変換である．

量子 Fourier 変換はユニタリ変換

$a, a' \in \mathbb{Z}/q\mathbb{Z}$ を取ると，

$$\begin{aligned}
&\frac{1}{q}\sum_{b=0}^{q-1} \exp\left(2\pi\sqrt{-1}\frac{ab}{q}\right)\overline{\exp\left(2\pi\sqrt{-1}\frac{a'b}{q}\right)} \\
&= \frac{1}{q}\sum_{b=0}^{q-1} \exp\left(2\pi\sqrt{-1}\frac{(a-a')b}{q}\right) \\
&= \begin{cases} 1 & a = a' \\ 0 & \text{o.w.} \end{cases}
\end{aligned}$$

ゆえ，示された． □

3. Shor の素因数分解アルゴリズムの詳細

Shor の素因数分解アルゴリズムの概要再掲

Shor の素因数分解アルゴリズムの概要を再掲.
正整数 a, b に対して，(a, b) で a と b の最大公約数を表す.

Input : N
Output : N のある素因数

(i). $x \in \{1, \cdots, N-1\}$ をランダムに選ぶ
(ii). (x, N) が 1 でなければその値を出力して終了し，1 なら (iii) へ
(iii). $\mathrm{mod}\ N$ における x の位数 r を計算する
(iv). r が偶数かつ $x^{r/2} \not\equiv N-1 \mod N$ なら $(x^{r/2}-1, N)$ を出力する，そうでなければ (i) へ戻る

Shor の素因数分解アルゴリズムの詳細

$2N^2 \leq q < 4N^2$ であり，2 べきで表せる q を取る．このような q が一意的に存在することを示す．

$\because$) $q = \lceil 2\log_2 N \rceil + 1$ とする．q は正整数である．このとき，
$2^q \geq 2 \times 2^{2\log_2 N} = 2N^2$ であり，$2^q < 2^{2\log_2 N + 2} = 4N^2$ である．
$p < q$ なる正整数 p については，$2^p \leq 2^{q-1} = 2^{\lceil 2\log_2 N \rceil}$
$< 2^{2\log_2 N + 1} = 2N^2$ である．
一方，$p > q$ なる正整数 p については，$2^p \geq 2^{q+1} = 2^{\lceil 2\log_2 N \rceil + 2}$
$\geq 2^{2\log_2 N + 2} = 4N^2$ となる．
以上より，条件を満たす正整数 q は一意的に存在する．$\square$

Shor の素因数分解アルゴリズムの詳細

$a \in \mathbb{Z}/q\mathbb{Z}$ を取って,

$$\frac{1}{q^{\frac{1}{2}}} \sum_{a=0}^{q-1} |a\rangle$$

なる状態を考える.
また, $x^a \bmod N$ を計算するために,

$$\frac{1}{q^{\frac{1}{2}}} \sum_{a=0}^{q-1} |x^a \bmod N\rangle$$

なる状態を考える.
そして, これらの状態の合成として,

$$\frac{1}{q^{\frac{1}{2}}} \sum_{a=0}^{q-1} |a\rangle \otimes |x^a \bmod N\rangle$$

を以下では考える.

Shor の素因数分解アルゴリズムの詳細

ここで，状態 $|a\rangle$ に対して量子 Fourier 変換を作用させる．

$$\frac{1}{q}\sum_{c=0}^{q-1}\left(\sum_{a=0}^{q-1}\exp\left(2\pi\sqrt{-1}\frac{ac}{q}\right)\right)|c\rangle\otimes|x^a \bmod N\rangle$$

さて，ここで $r|N$ であることに注意する．

$\because$) $G := \{1 \bmod N, x \bmod N, \cdots, x^{N-1} \bmod N\}$ **は位数 N の部分群であり，** $\{1 \bmod N, x \bmod N, \cdots, x^{r-1} \bmod N\}$ **は $x^r \equiv 1 \bmod N$ から，G の部分群で位数 r である．よって，Lagrange の定理から主張を得る．** $\square$

Thm(Lagrange)

G を有限群，H をその部分群，$|G|, |H|$ でそれぞれ G, H の位数を表すとき，$|G| = |G/H||H|$ が成り立つ．

Shor の素因数分解アルゴリズムの詳細

このことから， $0 \le a \le q-1$ **で，** $0 \le k < r$ **を考えると，**
$x^a \equiv x^k \bmod N$ **なら** $a \equiv k \bmod N$ **となる．**
以下では，状態 $(|c\rangle, |x^k \bmod N\rangle)$ **を観測する確率を考える．その確率は，**

$$\left| \frac{1}{q} \sum_{a : x^a \equiv x^k \bmod N} \exp\left(2\pi\sqrt{-1}\frac{ac}{q}\right) \right|^2$$

で与えられる． $a \equiv k \bmod N$ **ゆえ，** $a = br + k$ **と置くと，上記の確率は，**

$$\left| \frac{1}{q} \sum_{b=0}^{\lfloor (q-k-1)/r \rfloor} \exp\left(2\pi\sqrt{-1}\frac{(br+k)c}{q}\right) \right|^2$$

となる．このとき， $\left|\exp\left(2\pi\sqrt{-1}\frac{kc}{q}\right)\right| = 1$ **に注意する．**

Shor の素因数分解アルゴリズムの詳細

$rc \equiv \{rc\}_q \bmod q$ で，$-\frac{q}{2} < \{rc\}_q \leq \frac{q}{2}$ なる $\{rc\}_q$ を考える．すると，前述の確率は，

$$\left| \frac{1}{q} \sum_{b=0}^{\lfloor (q-k-1)/r \rfloor} \exp\left(2\pi\sqrt{-1} b \frac{\{rc\}_q}{q} \right) \right|^2$$

と直せる．$|\{rc\}_q| \leq \frac{r}{2}$ で q よりも十分小さい場合には，$t = \frac{b}{q}$ と変数変換をすることで，

$$\left| \int_0^{\frac{1}{q}\lfloor (q-k-1)/r \rfloor} \exp\left(2\pi\sqrt{-1} \{rc\}_q t \right) \, dt \right|^2$$

なる積分へと近似できる．

Shor の素因数分解アルゴリズムの詳細

$$
\begin{aligned}
&\left| \int_0^{\frac{1}{q}\lfloor (q-k-1)/r \rfloor} \exp\left(2\pi\sqrt{-1}\{rc\}_q t\right)\ dt \right| \\
&= \left| \left[\frac{1}{2\pi\sqrt{-1}\{rc\}_q} \exp\left(2\pi\sqrt{-1}\{rc\}_q t\right) \right]_0^{\frac{1}{q}\lfloor (q-k-1)/r \rfloor} \right| \\
&\geq \frac{1}{\pi r} \left| \exp\left(2\pi\sqrt{-1}\{rc\}_q \frac{1}{q}\lfloor (q-k-1)/r \rfloor\right) - 1 \right| \\
&\geq \frac{1}{\pi r} \left(\left| \exp\left(2\pi\sqrt{-1}\{rc\}_q \frac{1}{q}\lfloor (q-k-1)/r \rfloor\right) \right| + |-1| \right) \\
&= \frac{2}{\pi r}
\end{aligned}
$$

であるから， $\frac{4}{\pi^2 r^2} \geq \frac{1}{3r^2}$ **ゆえ，状態** $(|c\rangle, |x^k \bmod N\rangle)$ **を観測する確率は，少なくとも** $\frac{1}{3r^2}$ **となる．**

Shor の素因数分解アルゴリズムの詳細

$rc \equiv \{rc\}_q \bmod q$ であったから，ある整数 d を用いて，$-\frac{r}{2} \leq rc - dq \leq \frac{r}{2}$ となり，このことから，$\left|\frac{c}{q} - \frac{d}{r}\right| \leq \frac{1}{2q}$ を得る．
今，c と q は既知で，$q \geq 2N^2 > 2r^2$ から，下記の定理 [3] を用いて，r を特定することができる．

Thm

$R_0 := q,\ R_1 := c$ とおき，$R_0 > R_1$ を入力とした拡張 Euclid の互除法により $R_2, R_3, \cdots$ を定める．同時に $R_i = (-1)^i(P_i R_0 - Q_i R_1)$ を満たす $P_i, Q_i \in \mathbb{Z}$ $(P_0 = 1,\ Q_0 = 0,\ P_1 = 0,\ Q_1 = 1)$ を定める．互除法によりはじめて $R_l = 0$ なる添字 l を取り，$(P_{l+1},\ Q_{l+1},\ R_{l+1}) = (P_l,\ Q_l,\ R_l)$ とする．
このとき，整数 $A > B > 0$ が $\left|\frac{R_1}{R_0} - \frac{B}{A}\right| < \frac{1}{2A^2}$ を満たすとき，ある $i \geq 2$ について $\frac{B}{A} = \frac{P_i}{Q_i}$ が成り立つ．

Shor の素因数分解アルゴリズムの詳細

r を特定できるような $(|c\rangle, |x^k \bmod N\rangle)$ が取りうる状態の数を求める.

$\left|\frac{c}{q} - \frac{d}{r}\right| \leq \frac{1}{2q}$ において, $\frac{d}{r}$ は既約ゆえ, d は $\phi(r)$ 個の値を取りうる.

r が x の位数ゆえ, x^k が取りうる値の数は r 個である.

ここで, 状態 $(|c\rangle, |x^k \bmod N\rangle)$ を観測する確率は, 少なくとも $\dfrac{1}{3r^2}$ であったから, r を得る確率は少なくとも $\dfrac{\phi(r)}{3r}$ となる. また, 下記の定理 [4] から, $O(\log \log r)$ の計算量で r を求めることができる.

Thm

$$\lim_{r \to \infty} \frac{\phi(r) \log\log r}{r} = e^{-\gamma}$$

ここで, γ は Euler 定数で, $\gamma = \lim_{n \to \infty}\left(\sum_{k=1}^{n} \frac{1}{k} - \log(n)\right)$ である.

4. Shor の素因数分解アルゴリズムの実装

実装の前準備

以下では，Python の Qiskit というモジュールを使用して実装する．
また，$(N,x) = (35,8)$ の場合のみに絞ってコードを紹介する．
初めに以下をインポートする．

```
from qiskit import QuantumCircuit, Aer, transpile, assemble
# from numpy.random import randint
from math import gcd
import math
import numpy as np
from fractions import Fraction
```

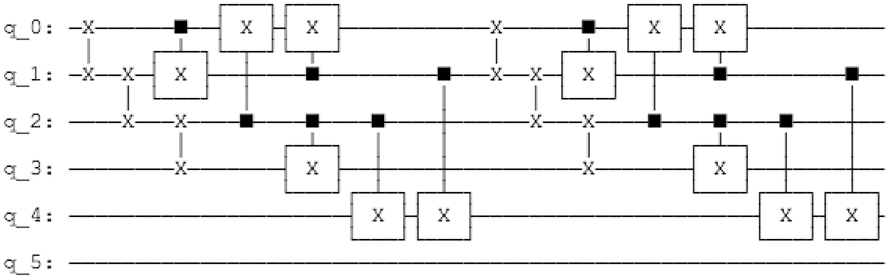
量子ゲートの実装

$U|y\rangle \equiv |8y \bmod 35\rangle$ として，$y = 1$ なる初期状態に，U を作用させるような量子ゲートを作る

```
def c_xmod35(x: int, N: int, power: int) -> list:
    """Controlled multiplication by a mod 35"""
    gate_number = int(math.log2(N))
    U = QuantumCircuit(gate_number)
    for iteration in range(power):
        U.swap(0, 1)
        U.swap(1, 2)
        U.swap(2, 3)
        U.cx(0, 1)
        U.cx(2, 0)
        U.cx(2, 3)
        U.cx(2, 4)
        U.cx(1, 0)
        U.cx(1, 4)
    U = U.to_gate()
    U.name = "%i^%i mod 35" % (x, power)
    c_U = U.control()
    return c_U
```

実装した量子ゲート

前スライドで実装した量子ゲートは次のように図示できる.



上記は 2 回しか繰り返していないが，実際は引数で与えられる power 回だけ繰り返す

量子 Fourier 変換の実装

固有状態を得るために，量子 Fourier 変換を作用させる．

```
def qft_dagger(n: int) -> list:
    qc = QuantumCircuit(n)
    for qubit in range(n//2):
        qc.swap(qubit, n-qubit-1)
    for j in range(n):
        for m in range(j):
            qc.cp(-np.pi/float(2**(j-m)), m, j)
        qc.h(j)
    qc.name = "†QFT"
    return qc
```

量子位相推定の実装

量子 Fourier 変換を作用して得られた値を測定し，位数を得る．

```
def qpe_xmod35(x: int, N: int) -> int:
    n_count = 3
    gate_number = int(math.log2(N))
    qc = QuantumCircuit(gate_number+n_count, n_count)
    for q in range(n_count):
        qc.h(q)
    qc.x(3+n_count)
    for q in range(n_count):
        qc.append(c_xmod35(x, N, 2**q),
                  [q] + [i+n_count for i in range(gate_number)])
    qc.append(qft_dagger(n_count), range(n_count))
    qc.measure(range(n_count), range(n_count))
    qasm_sim = Aer.get_backend('qasm_simulator')
    t_qc = transpile(qc, qasm_sim)
    obj = assemble(t_qc, shots=1)
    result = qasm_sim.run(assemble(t_qc), memory=True).result()
    readings = result.get_memory()
    print("Register Reading: " + readings[0])
    phase = int(readings[0],2)/(2**n_count)
    print("Corresponding Phase: %f" % phase)
    return phase
```

実装のまとめと出力結果の確認

以下を実行することで，35 の素因数として 5 と 7 を得る．

```
N = 35
factor_found = False
attempt = 0
while not factor_found:
    x = 8 # 本当は x = randint(2, N - 1)
    if gcd(x, N) == 1:
        attempt += 1
        print("\nAttempt %i:" % attempt)
        phase = qpe_xmod35(x, N) # Phase = s/r
        frac = Fraction(phase).limit_denominator(N)
        r = frac.denominator
        if phase != 0 :
            guesses = [gcd(x**(r//2)-1, N), gcd(x**(r//2)+1, N)]
            print("Guessed Factors: %i and %i" % (guesses[0],
                guesses[1]))
            for guess in guesses:
                if guess not in [1,N] and (N % guess) == 0:
                    print("*** Non-trivial factor found: %i ***" %
                          guess)
                    factor_found = True
```

5. Shor の離散対数アルゴリズムの詳細

1. Shor の素因数分解アルゴリズムの概要
2. 量子計算理論入門
3. Shor の素因数分解アルゴリズムの詳細
4. Shor の素因数分解アルゴリズムの実装
5. Shor の離散対数アルゴリズムの詳細

Shor の離散対数アルゴリズムの詳細

p を素数，g を $\mathbb{Z}/p\mathbb{Z}$ の生成元，x を $\mathbb{Z}/p\mathbb{Z}$ からランダムに選ぶ．
また，$p \leq q < 2p$ で 2 べきなる q を取る．
このとき，$g^r \equiv x \bmod p$ なる r を見つけることが目標．
a, b を $\mathbb{Z}/p\mathbb{Z}$ からランダムに取り，次の状態を観測する．

$$\frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}|a\rangle \otimes |b\rangle$$

そして，この a, b を fix して，$g^a x^{-b} \bmod p$ を観測すると，

$$\frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}|a\rangle \otimes |b\rangle \otimes |g^a x^{-b} \bmod p\rangle$$

となる．

Shor の離散対数アルゴリズムの詳細

このとき，量子 Fourier 変換を作用させると，

$$\frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}\left(\frac{1}{q^{1/2}}\sum_{c=0}^{q-1}\exp(2\pi\sqrt{-1}\frac{ac}{q})|c\rangle\right)\otimes\left(\frac{1}{q^{1/2}}\sum_{d=0}^{q-1}\exp(2\pi\sqrt{-1}\frac{bd}{q})|d\rangle\right)\otimes|g^a x^{-b} \bmod p\rangle$$

$$=\frac{1}{(p-1)q}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}\sum_{c=0}^{p-2}\sum_{d=0}^{p-2}\left(\exp(2\pi\sqrt{-1}\frac{ac+bd}{q})\right)|c\rangle\otimes|d\rangle\otimes|g^a x^{-b} \bmod p\rangle$$

となる．このとき，状態 $|c\rangle\otimes|d\rangle\otimes|y\rangle$ s.t. $y\equiv g^k \bmod p,\ k\in\mathbb{Z}$ を観測する確率は，

$$\left|\frac{1}{(p-1)q}\sum_{\substack{a,b\\ a-rb\equiv k}}\exp(2\pi\sqrt{-1}\frac{ac+bd}{q})\right|^2$$

である．

Shor の離散対数アルゴリズムの詳細

$$a - rb \equiv k \mod p-1 \Rightarrow a = br + k - (p-1)\left\lfloor \frac{br+k}{p-1} \right\rfloor$$

であり,

$$\{z\}_q : z \mod q \text{ s.t. } -\frac{q}{2} < \{z\}_q \leq \frac{q}{2}$$

$$U = bT, \quad T = rc + d - \frac{r}{p-1}\{c(p-1)\}_q$$

$$V = \left(\frac{br}{p-1} - \left\lfloor \frac{br+k}{p-1} \right\rfloor \right) \{c(p-1)\}_q$$

と置くと，前述の確率は,

$$\left| \frac{1}{(p-1)q} \sum_{b=0}^{p-2} \exp\left(\frac{2\pi\sqrt{-1}}{q} U\right) \exp\left(\frac{2\pi\sqrt{-1}}{q} V\right) \right|^2$$

と表せる.

Shor の離散対数アルゴリズムの詳細

このとき，以下の 2 **つを仮定する**:

- $|\{T\}_q| = |T - jq| \leq \dfrac{1}{2}$
- $\{c(p-1)\}_q \leq \dfrac{q}{20}$

ここで， j **は** T/q **に最も近い整数で，** 2 **つ目の条件から，** $|V| \leq \frac{q}{20}$ **を得る．** $0 \leq b \leq p-2$ **ゆえ，** $0 \leq \frac{2\pi\sqrt{-1}}{q} U \leq \frac{2\pi\sqrt{-1}}{q} W$ **となる．ただし，** $W = (p-2)T$ **である．**

このとき， b **を動かしたときの** $\exp(\frac{2\pi\sqrt{-1}}{q} U)$ **の合成は，**

$\exp(\pi\sqrt{-1}W)$ **方向を向かい，** $\forall b$ **に対して，** $\exp\left(\dfrac{2\pi\sqrt{-1}}{q} U\right)$

$= \exp\left(\frac{2\pi\sqrt{-1}}{p-2} Wb\right)$ **の** $\exp(\pi i W)$ **方向への射影の大きさは**

$\cos\left(2\pi\left|\dfrac{W}{2} - \dfrac{Wb}{p-2}\right|\right)$ **である．**

Shor の離散対数アルゴリズムの詳細

また， $|V| \le \frac{q}{20}$ **であったから，** $|\exp(\frac{2\pi\sqrt{-1}}{q}V)| \le \exp(\frac{\pi\sqrt{-1}}{10})$ **である．先ほど考えた射影と合成すると，** $\forall b$ **に対して，** $\exp(\pi i W)$ **方向への射影の大きさは** $\cos\left(2\pi\left|\frac{W}{2}-\frac{Wb}{p-2}\right|+\frac{\pi}{10}\right)$ **である．**

つまり，状態 $|c\rangle \otimes |d\rangle \otimes |y\rangle$ s.t. $y \equiv g^k \bmod p,\ k \in \mathbb{Z}$ **を観測する確率は，**

$$\left|\frac{1}{(p-1)q}\sum_{b=0}^{p-2}\cos\left(2\pi\left|\frac{W}{2}-\frac{Wb}{p-2}\right|+\frac{\pi}{10}\right)\right|^2$$

であり，これを整理すると，

$$\left(\frac{1}{q}\frac{2}{\pi}\int_{\frac{\pi}{10}}^{\frac{7\pi}{20}}\cos t\ dt\right)^2$$

となる．

Shor の離散対数アルゴリズムの詳細

$$
\begin{aligned}
&\left(\frac{1}{q}\frac{2}{\pi}\int_{\frac{\pi}{10}}^{\frac{7\pi}{20}} \cos t \; dt\right)^2 \\
&\geq \left(\frac{1}{q}\frac{2}{\pi}[\sin t]_{\frac{\pi}{10}}^{\frac{7\pi}{20}}\right)^2 \\
&\geq \left(\frac{1}{q}\frac{2}{\pi}\left(\sin\left(\frac{7\pi}{20}\right) - \sin\left(\frac{\pi}{10}\right)\right)\right)^2 \\
&\geq \left(\frac{1}{q}\frac{2}{3.15}0.58\right)^2 \\
&\geq \frac{135}{1000q^2}
\end{aligned}
$$

Shor の離散対数アルゴリズムの詳細

ここで，仮定した 2 条件を満たす (c,d) のペアがどのくらいあるのかを考察する．
$|\{T\}_q| = |T - jq| \le \frac{1}{2}$ であり，$T = rc + d - \frac{r}{p-1}\{c(p-1)\}_q$ であったから，$\forall c$ に対して，このような d が一意的に定まる．
また，$\{c(p-1)\}_q \le \frac{q}{20}$ では，$\{z\}_q : z \bmod q \text{ s.t. } -\dfrac{q}{2} < \{z\}_q \le \dfrac{q}{2}$
ゆえ，$\frac{q}{10}$ 個の (c,d) のペアが条件を満たす．
更に，$0 \le b \le p-1$ ゆえ，b は p 個の値を取りうるから，合計で $\frac{pq}{10}$ 個の状態がありうる．
それぞれの状態に対して，$\frac{135}{1000q^2}$ の確率で r を発見できるから，合計で，$\frac{135}{1000q^2} \times \frac{pq}{10} > \frac{p}{80q}$ であり，$q < 2p$ ゆえ，$\frac{p}{80q} > \frac{1}{160}$ を得る．

Shor の離散対数アルゴリズムの詳細

条件を満たす (c, d) から，r を発見できることを示す．

条件から $-\frac{1}{2} \leq \frac{T}{q} - j \leq \frac{1}{2}$ である．つまり，

$$-\frac{1}{2q} \leq \frac{d}{q} + \frac{r}{q}\left(c - \frac{\{c(p-1)\}_q}{p-1}\right) \leq \frac{1}{2q}$$

である．ここで，r と $p-1$ が互いに素であれば，

$$\frac{r}{q}\left(c - \frac{\{c(p-1)\}_q}{p-1}\right) = \frac{r}{p-1}c', \quad c' = \frac{c(p-1) - \{c(p-1)\}_q}{q}$$

としたとき，$c' \in \mathbb{Z}$ である，特に，$c' = \left\lfloor \frac{c(p-1)}{q} \right\rfloor$ or $\left\lceil \frac{c(p-1)}{q} \right\rceil$ となる．

Shor の離散対数アルゴリズムの詳細

以上より，

$$\left(-\frac{1}{2q}-\frac{d}{q}\right)\frac{1}{c'}\leq\frac{r}{p-1}\leq\left(\frac{1}{2q}-\frac{d}{q}\right)\frac{1}{c'}$$

であり，$\frac{r}{p-1}$ が既約分数であることから，r を特定できる．また，特定できる確率は少なくとも $\frac{1}{160}$ 以上であるから，（多項式回）繰り返すことで r を特定できる．

参考文献

[1] M. A. Nielsen and I.L. Chuang:
Quantum Computation and Quantum Information, Cambridge University Press, 2000

[2] **森前 智行,『量子計算理論』, 森北出版,** 2017 **年**

[3] **縫田 光司,『耐量子計算機暗号』, 森北出版,** 2020 **年**

[4] G. H. Hardy and E. M. Wright:
An Introduction to the Theory of Numbers, *Fifth Edition*, Oxford University Press, New York, 1979