隠れ部分群問題から見る素因数分解，離散対数問題

國廣昇

筑波大学

2022 年 8 月 3 日

九州大学 IMI 研究集会
耐量子計算機暗号と量子情報の数理

Agenda

1. 隠れ部分群問題
2. Quantum Fourier Transformation
3. 初期のアルゴリズム（DJ, BV, Simon）
    - Deutsch–Jozsa, Bernstein–Vazirani アルゴリズム
    - Bernstein–Vazirani 問題
    - Simon のアルゴリズム
4. 素因数分解，離散対数アルゴリズム
    - 位相推定アルゴリズム
    - 素因数分解アルゴリズム
    - 離散対数問題を解くアルゴリズム
5. まとめ

隠れ部分群問題

隠れ部分群問題

有限生成群 G と有限集合 X に対して，f は，

- G から X への関数，
- G の部分群 K の剰余類上で定数であり，各剰余類に対して互いに異なる，
- オラクルとして与えられている

とき，K（に対する生成集合）を求めよ．

登場人物

X は実質的に，$f(G) = \{f(x) \mid x \in G\}(\subseteq X)$ と制限しても問題ないので，これ以降あまり気にしないことにする．

- 関数 f
- 有限生成群 G
- G の部分群 K

知られている結果

- G が有限可換群であれば，多項式時間で求解可能（Simon の問題，離散対数問題など）．
- G が有限生成可換群でも，多項式時間で求解可能（素因数分解など）．
- G が非可換群（例えば，対称群や二面体群）のとき，多項式時間アルゴリズムは知られていない．
    - グラフ同型性判定問題は，G が対称群の場合に相当
    - G が二面体群であれば，準指数関数時間で求解可能．ある種の格子問題に関連がある．

有限生成可換群

有限生成群

有限部分集合 S を生成元とする群 G を有限生成群という

有限生成可換群の基本定理

群 G が有限生成可換群であるならば，$e_1 > 1, e_i | e_{i+1}$ となるような自然数 $e_1, e_2, \ldots, e_s$ と非負整数 r が存在し，

$$G \cong \mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_s\mathbb{Z} \times \mathbb{Z}^r$$

となる．

有限生成可換群は，適当な n を用いて $\mathbb{Z}/n\mathbb{Z}$ と $\mathbb{Z}$ の直積で表現できる．

隠れ部分群問題に対する量子アルゴリズム

- f に対するユニタリ変換 $U_f |g\rangle |h\rangle = |g\rangle |h \oplus f(g)\rangle$ を実行する量子オラクルが与えられているとする．
- 量子重ね合わせ

$$|0\rangle |0\rangle \longrightarrow \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |f(x)\rangle$$

を作成．第１レジスタを逆量子フーリエ変換し，測定する．

実装上で気にすること

- G の元の表現方法はどうするか？
- 特に，G は有限集合とは限らない．あくまでも，有限生成群．
  - G が可換群の場合，元は整数値で表現することにする（有限生成可換群の基本定理より）．
  - G を（十分大きい）有限の値で打ち切ることにする．特に，$0, 1, 2, \ldots, 2^m - 1$ で表現する（実装上の都合）．
  - ただし，有限で打ち切っても問題ないことを確認する必要あり．

位数発見問題の隠れ部分群問題を通した解釈

- $G = \mathbb{Z}$ とする．
- $f(x) = a^x \bmod N$ とする．
- $X = f(\mathbb{Z}) = \{a^j \bmod N \mid j \in \mathbb{Z}\}$ とする．
- r を a の N を法とした位数とする．
- $K = r\mathbb{Z} = \{, \ldots, 0, r, 2r, 3r, \ldots\}$ とする．K は r により生成される．
- 全ての $k \in K$ に対して，$a^k \equiv 1 \pmod{N}$
- $0 \leq t < r$ に対して，集合 K_t を

$$K_t := t + K = \{t + k | k \in K\} = \{\ldots, t - r, t, t + r, t + 2r, \ldots\}$$

  とする．全ての $k \in K_t$ に対して，$f(k) = a^t \bmod N = f(t)$．
- $t \neq s$ のとき，$f(K_t) \neq f(K_s)$．

$N = 15$ の例

$G = \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ とする．
$N = 15, a = 7$ とすると，$r = 4$ である（$a^4 \bmod N = 1, a^2, a^3 \neq 1$）．

- $K (= K_0) = \{\ldots, 0, 4, 8, \ldots, \}$ に対して，$f(K_0) = 1$（$a^0 \bmod N = 1$）
- $K_1 = \{\ldots, 1, 5, 9, \ldots, \}$ に対して，$f(K_1) = 7$（$a^1 \bmod N = 7$）
- $K_2 = \{\ldots, 2, 6, 10, \ldots, \}$ に対して，$f(K_2) = 4$（$a^2 \bmod N = 4$）
- $K_3 = \{\ldots, 3, 7, 11, \ldots, \}$ に対して，$f(K_3) = 13$（$a^3 \bmod N = 13$）

離散対数問題

離散対数問題

p を素数として，$a, b \in \mathbb{F}_p$ とする．$b \equiv a^s \pmod{p}$ となる $s \in \mathbb{Z}$ を求めよ．(議論を簡単にするため，a の位数は素数 q とし，q は既知とする.)

一般化された離散対数問題

$(G, \cdot)$ を可換群とし，G の位数を素数 q とする．$a, b \in G$ としたときに，$b = a^s$ となる $s \in \mathbb{Z}$ を求めよ．

離散対数問題の隠れ部分群問題を通した解釈

- $G = \mathbb{Z}_q \times \mathbb{Z}_q$ とする．
- $f(x_1, x_2) = b^{x_1} a^{x_2}$ とする．
- $X = \{a^j \mid j \in \mathbb{Z}_q\}$ とする．
- $K = \{(l, -ls) \mid l \in \mathbb{Z}\}$ とする．K は $(1, -s)$ により生成される．
- 全ての $(k_1, k_2) \in K$ に対して，$b^{k_1} a^{k_2} = (a^s)^l a^{-ls} = a^0 = 1$
- $0 \leq t < q - 1$ に対して，集合 K_t を

$$K_t := \{(k_1, k_2) | sk_1 + k_2 \bmod q = t\}$$

  とする．全ての $(k_1, k_2) \in K_t$ に対して，$f(k_1, k_2) = a^t$．
- $t \neq s$ のとき，$f(K_t) \neq f(K_s)$．

例：$q = 3$ の場合

$b = a^2$ とする．$s = 2$ が解．

$G = \mathbb{Z}_3 \times \mathbb{Z}_3$ とし，$f(x_1, x_2) = b^{x_1} a^{x_2}$ とする．

- $K(= K_0) = \{(0,0), (1,1), (2,2)\}$ の時は，a^0 に移る．
- $K_1 = \{(0,1), (1,2), (2,0)\}$ の時は，a^1 に移る．
- $K_2 = \{(0,2), (1,0), (2,1)\}$ の時は，a^2 に移る．

K は，$(1,1)$ により生成される．$-s = 1$ より，$s = 2$．

$G = \mathbb{Z} \times \mathbb{Z}$ としてみる

- $K(= K_0) = \{(x_1, x_2) \mid x_2 = x_1\}$ の時は，a^0 に移る．
- $K_1 = \{(x_1, x_2) \mid x_2 = x_1 + 1\}$ の時は，a^1 に移る．
- $K_2 = \{(x_1, x_2) \mid x_2 = x_1 + 2\}$ の時は，a^2 に移る．

K は，$(1,1)$ により生成される．$-s = 1$ より，$s = 2$．

周期関数の周期を求める

- $G = \mathbb{Z}$ とする．
- f は周期関数．つまり，ある正整数 r が存在して，すべての x に対して $f(x+r) = f(x)$ が成り立つ．最小の r を求めたい．
- $X = \{f(x) \mid x \in G\}$ とする．当然 $|X| = r$．
- $K = r\mathbb{Z} = \{, \ldots, 0, r, 2r, 3r, \ldots\}$ とする．K は r により生成される．
- 全ての $k \in K$ に対して，$f(k) = f(0)$
- $0 \le t < r$ に対して，集合 K_t を

$$K_t := t + K = \{t + k | k \in K\} = \{\ldots, t - r, t, t + r, t + 2r, \ldots\}$$

  とする．全ての $k \in K_t$ に対して，$f(k) = f(t)$．
- $t \neq s$ のとき，$f(K_t) \neq f(K_s)$．

全射群準同型写像 f の場合

- G を有限生成群，H を有限群として，f を，G から H への全射群準同型写像とする．
- $\ker(f) = \{g \in G \mid f(g) = e_H\}$ とする．
- $\ker(f)$ は，G の正規部分群となる．
- $K = \ker(f)$ としてよい．
- このとき，K の生成元を求めることができる．

$G = \mathbb{Z}, H = \{a^x \mid x \in \mathbb{Z}\} \subseteq \mathbb{Z}_N$，$f(x) = a^x \bmod N$ とする．
このとき，f は群準同型写像である．
$\ker(f) = \{x \in \mathbb{Z} \mid a^x \equiv 1 \pmod N\} = r\mathbb{Z}$ であり，K の生成元は r．

- $G = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ とし，H を有限群とする．
- $f(x_1, \ldots, x_n)$ が，G から H への全射群準同型写像とする．
- $\ker(f)$ が，$(s_1, \ldots, s_n)$ により生成されるとする．$(s_1, \ldots, s_n)$ を求めることができる．

$G = \mathbb{Z} \times \mathbb{Z}, H = \{g^x \mid x \in \mathbb{Z}\} \subseteq \mathbb{Z}_p$ とし，$f(x, y) = b^x a^y \bmod p$ とする．このとき，f は群準同型写像である．
$f(x, y) = 1$ となる x, y は，$sx + y \bmod q = 0$ を満たす．
$\ker(f) = \{l(1, -s) \mid l \in \mathbb{Z}_q\}$ であり，K の生成元は $(1, -s)$．

Quantum Fourier Transformation

量子フーリエ変換 (QFT)

正規直交基底 $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ に対して，以下で定義される．

$$|j\rangle \xrightarrow{\mathsf{QFT}} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp(2\pi \mathrm{i} jk/N) |k\rangle$$

重ね合わせ状態に対する作用は，

$$\sum_{j=0}^{N-1} x_j |j\rangle \xrightarrow{\mathsf{QFT}} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} x_j \exp(2\pi \mathrm{i} jk/N) |k\rangle$$

この変換は，ユニタリ変換

QFT の積表現

実装を考えると，$N = 2^n$ に限定することが多い．
これ以降は，$N = 2^n$ とし，基底 $|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle$ を基底とする．
状態 $|j\rangle$ を j の 2 進数表現 $j = j_1 j_2 \cdots j_n$ を用いて表現（順番に注意）．
（$j/2^n$ を扱うため，$j/2^n = 0.j_1 j_2 \cdots j_n$ の方が便利）

量子フーリエ変換の積表現

$$|j_1 \cdots j_n\rangle \to \frac{(|0\rangle + \exp(2\pi i 0.j_n)|1\rangle)(|0\rangle + \exp(2\pi i 0.j_{n-1}j_n)|1\rangle) \cdots (|0\rangle + \exp(2\pi i 0.j_1 \cdots j_n)|1\rangle)}{2^{n/2}}$$

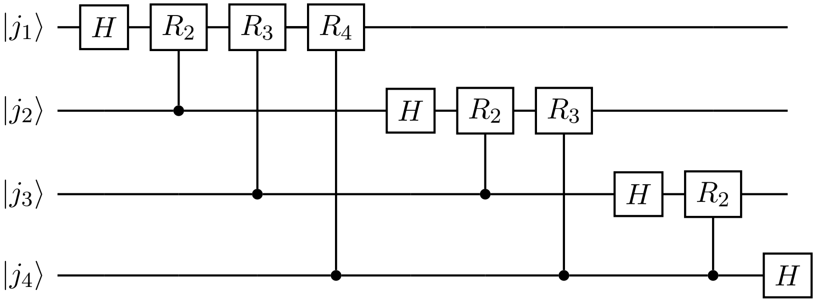
ゲート総数 $n + (n-1) + \cdots + 1 = n(n+1)/2$ 個での実装を紹介．

回路構成（$n = 4$ の場合の例）

回転ゲート R_k を

$$R_k := \begin{pmatrix} 1 & 0 \\ 0 & \exp(2\pi \mathrm{i}/2^k) \end{pmatrix}$$

とする．ここで，$R_2 = S, R_3 = T$



最終状態は逆の順番になっている（SWAP を行い順番を戻す必要あり）

$$\frac{(|0\rangle + \exp(2\pi \mathrm{i} 0.j_1 j_2 j_3 j_4)\,|1\rangle)\cdots(|0\rangle + \exp(2\pi \mathrm{i} 0.j_3 j_4)\,|1\rangle)(|0\rangle + \exp(2\pi \mathrm{i} 0.j_4)\,|1\rangle)}{2^{n/2}}$$

Agenda

1. 隠れ部分群問題
2. Quantum Fourier Transformation
3. 初期のアルゴリズム（DJ, BV, Simon）
   - Deutsch–Jozsa, Bernstein–Vazirani アルゴリズム
   - Bernstein–Vazirani 問題
   - Simon のアルゴリズム
4. 素因数分解，離散対数アルゴリズム
   - 位相推定アルゴリズム
   - 素因数分解アルゴリズム
   - 離散対数問題を解くアルゴリズム
5. まとめ

Phase Kickback

$f : \{0,1\}^n \to \{0,1\}$ とし，

$$U_f : |x\rangle |y\rangle \to |x\rangle |y \oplus f(x)\rangle$$

とする．

$$\frac{1}{\sqrt{2}} |x\rangle (|0\rangle - |1\rangle) \xrightarrow{U_f} \frac{1}{\sqrt{2}} |x\rangle (|f(x)\rangle - |1 \oplus f(x)\rangle)$$

を考える．

- $f(x) = 0$ のとき，$\frac{1}{\sqrt{2}} |x\rangle (|0\rangle - |1\rangle)$
- $f(x) = 1$ のとき，$\frac{1}{\sqrt{2}} |x\rangle (|1\rangle - |0\rangle) = -\frac{1}{\sqrt{2}} |x\rangle (|0\rangle - |1\rangle)$

まとめると，

$$\frac{1}{\sqrt{2}} |x\rangle (|0\rangle - |1\rangle) \xrightarrow{U_f} \frac{1}{\sqrt{2}} (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle)$$

$f(x)$ の値を位相部分に埋め込んでいることに相当．

$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ 部は，前後で変化しないので，無視することにする．結局，

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle$$

とみなすことにする．

Deutsch–Jozsa アルゴリズム

問題

$f(x) : \{0,1\}^n \to \{0,1\}$ は，
(i) 常に 0 もしくは 1 を返す関数 (constant) か，
(ii) 半分の x については 0，残りの半分は 1 を返す関数 (balanced)
のどちらかであるとする．f に対するオラクルが与えられたときに，どちらであるかを判定する問題．

$$|0\rangle^{\otimes n} \to \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \to \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle$$

Hadamard 変換（$\mathbb{Z}_2^n$ 上での QFT）を施すと，

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \to \frac{1}{2^n} \sum_{y=0}^{2^n-1} (\sum_{x=0}^{2^n-1} (-1)^{f(x)} + (-1)^{\boldsymbol{x}\cdot\boldsymbol{y}})$$

測定をする

$0 \cdots 0$ で出てきたら，$f(x)$ は constant，それ以外なら，balanced．

確認

- $\mathbf{0}, \mathbf{1}$ を長さ 2^n で，すべての要素が，それぞれ $1(= (-1)^0)$, $-1(= (-1)^1)$ のベクトルとする．
- $\boldsymbol{y}$ を長さ 2^n で 2^{n-1} 個が 1，2^{n-1} 個が -1 のベクトルとする．
- このとき，$\mathbf{0} \cdot \boldsymbol{y} = \mathbf{1} \cdot \boldsymbol{y} = 0$ であるので，$\mathbf{0}$ と $\mathbf{1}$ は，$\boldsymbol{y}$ はそれぞれ直交する．
- ユニタリ変換は，内積を保存するので，balanced の場合は，$0 \cdots 0$ 以外を出力する．

$n=1$ のとき：Deutsch アルゴリズム

問題は次の形になる．

- $f(0)=f(1)$ であるか，$f(0)\neq f(1)$ であるかを当てる問題．
- $(f(0),f(1))=(0,0),(1,1),(0,1),(1,0)$

最終状態は，

- $\frac{1}{2}\{(1+(-1)^{f(0)\oplus f(1)})\,|0\rangle+\{(1-(-1)^{f(0)\oplus f(1)})\,|1\rangle$
- $f(0)=f(1)$ のときは $|0\rangle$，
- $f(0)\neq f(1)$ のときは $|1\rangle$

になる．

K は？

- constant 関数の場合は，$K=\{0,1\}$，
- balanced 関数の場合は，$K=\{0\}$．

Bernstein–Vazirani アルゴリズム

問題

$\boldsymbol{s} \in \{0,1\}^n$ を未知とし，
$f : \{0,1\}^n \to \{0,1\}$ とし，$f(x) = \boldsymbol{x} \cdot \boldsymbol{s} \bmod 2$ とする．
f がオラクルとして与えられているときに，s を求める問題．

比較

古典的には，n 回のオラクル呼び出しで十分．n 回は絶対に必要．
量子的には，1 回のオラクル呼び出しで十分．

簡単な例 $n = 3, \boldsymbol{s} = (1, 0, 1)$ のとき

x	000	001	010	011	100	101	110	111
$f(x)$	0	1	0	1	1	0	1	0

このオラクルが与えられたときに，s を求める問題．

K は？

$$K = \{\boldsymbol{z} \in \mathbb{Z}_2^n \mid \boldsymbol{s} \cdot \boldsymbol{z} \bmod 2 = 0\}$$

$$\begin{aligned} |0\rangle^n &\to \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \\ &\xrightarrow{H^{\otimes n}} \frac{1}{2^n} \sum_{x,y \in \{0,1\}^n} (-1)^{f(x) + \boldsymbol{x} \cdot \boldsymbol{y}} |y\rangle = |\boldsymbol{s}\rangle \end{aligned}$$

最後の等式の確認

$$f(x) + \boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{x} \cdot \boldsymbol{s} + \boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{x} \cdot (\boldsymbol{y} + \boldsymbol{s})$$

となる．$\boldsymbol{y} \oplus \boldsymbol{s} = \boldsymbol{0}$（つまり，$\boldsymbol{y} = \boldsymbol{s}$）のとき，

$$(-1)^{f(x) + \boldsymbol{x} \cdot \boldsymbol{y}} = 1$$

になる．それ以外の時は，0 になる．

Simon のアルゴリズム

問題

以下の条件をみたす関数 $f : \{0,1\}^n \to \{0,1\}^{n-1}$ を考える
ある $\boldsymbol{r} \in \{0,1\}^n$ が存在して，全ての $\boldsymbol{x} \in \{0,1\}^n$ に対して，
$f(\boldsymbol{x} \oplus \boldsymbol{r}) = f(\boldsymbol{x})$ が成り立つ．
この時，$\boldsymbol{r} \in \{0,1\}^n$ を求めよ．簡単のため，$\boldsymbol{r} \neq \boldsymbol{0}$ とする．

f の例

x	000	001	010	011	100	101	110	111
$f(x)$	00	01	10	11	01	00	11	10

なお，解は $\boldsymbol{r} = 101$．

$K = \{\boldsymbol{0}, \boldsymbol{r}\}(= l\boldsymbol{r})$ for $l = 0, 1$ となる．$\boldsymbol{r}$ が生成元．

Simon のアルゴリズム詳細

Step1: **初期状態を用意**

$$|0\rangle^{\otimes n} |0\rangle^{\otimes n-1}$$

Step2：**先頭の n-qubit に対して，アダマール変換を作用させる．**

$$|0\rangle^{\otimes n} |0\rangle^{\otimes n-1} \to \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle |0\rangle^{\otimes n-1}$$

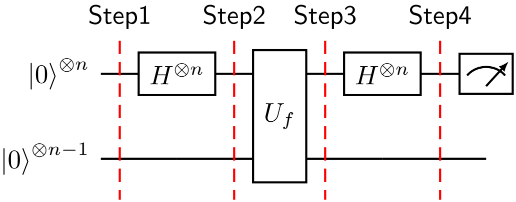
Step3：$U_f : |x\rangle |y\rangle \to |x\rangle |y \oplus f(x)\rangle$ **として，U_f を作用させる**

$$\frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle |0\rangle^{\otimes n-1} \to \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle |f(x)\rangle$$

Step4: **最初の n-qubit にアダマール変換を作用させる**

$$\frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle |f(x)\rangle \to \frac{1}{2^n} \sum_{x\in\{0,1\}^n} \sum_{u\in\{0,1\}^n} (-1)^{x\cdot u} |u\rangle |f(x)\rangle$$

Step5: **第 1 レジスタ（最初の n-qubit）を測定**



集合 R を

$$R = \{\boldsymbol{u} \in \{0,1\}^n \mid \boldsymbol{r} \cdot \boldsymbol{u} = 0\}$$

とする．測定をすると，R の元 $\boldsymbol{u}$ が等確率で得られる．なお，$|R| = 2^{n-1}$

アルゴリズムの残りの部分

- 1 回実行すると，$\boldsymbol{r}$ と直交するベクトルが 1 本得られる．
- これを繰り返し，互いに線形独立で $\boldsymbol{r}$ と直交するベクトルを $n-1$ 本得る．
- （簡単な線形代数の計算により）$\boldsymbol{r}$ を得る．

Agenda

1. 隠れ部分群問題
2. Quantum Fourier Transformation
3. 初期のアルゴリズム（DJ, BV, Simon）
   - Deutsch–Jozsa, Bernstein–Vazirani アルゴリズム
   - Bernstein–Vazirani 問題
   - Simon のアルゴリズム
4. 素因数分解，離散対数アルゴリズム
   - 位相推定アルゴリズム
   - 素因数分解アルゴリズム
   - 離散対数問題を解くアルゴリズム
5. まとめ

周期関数の周期を求めるアルゴリズム

$G=\mathbb{Z}$ とする．すべての $x\in G$ に対して，ある r が存在して $f(x+r)=f(x)$ が成り立つとする．この r を求めたい．

$G=\mathbb{Z}$ であるが，$0\le x\le 2^m-1$ で打ち切ることにする．

$$|0\rangle|0\rangle \to \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|f(x)\rangle$$

$|\hat{f}(l)\rangle=\frac{1}{\sqrt{r}}\sum_{x=0}^{r-1}\exp(-2\pi\mathrm{i}lx/r)|f(x)\rangle$ とすると，
$|f(x)\rangle=\frac{1}{\sqrt{r}}\sum_{x=0}^{r-1}\exp(2\pi\mathrm{i}lx/r)|\hat{f}(l)\rangle$ であるので，

$$\approx\frac{1}{\sqrt{r2^m}}\sum_{l=0}^{r-1}\sum_{x=0}^{2^m-1}\exp(2\pi\mathrm{i}lx/r)|x\rangle|\hat{f}(l)\rangle$$

$$\xrightarrow{\text{IQFT}}\frac{1}{\sqrt{r2^m}}\sum_{l=0}^{r-1}\left|\frac{l2^m}{r}\right\rangle|\hat{f}(l)\rangle \xrightarrow{\text{measure}} \frac{l2^m}{r} \xrightarrow{\text{連分数展開}} r$$

位相推定 (Phase Estimation) 問題

設定

- U をユニタリ変換とする
  - ユニタリ変換の固有値は，その絶対値は 1 であることに注意
- 固有ベクトルを $|\psi\rangle$ とすると，ある実数 $0 \leq \phi < 1$ に対して，

$$U|\psi\rangle = \exp(2\pi \mathrm{i}\phi)|\psi\rangle$$

位相推定問題

U とその固有ベクトルの一つ $|\psi\rangle$ が与えられている時に，対応する固有値の位相 ϕ（の近似値）を求めよ．

解くアルゴリズムのレシピは，Simon のアルゴリズムと同じ．

位相推定アルゴリズム

Step1: 初期状態 $|0\rangle^{\otimes m}|\psi\rangle$ を用意
Step2：第 1 レジスタ（先頭 m-qubit）に対してアダマール変換を施す

$$|0\rangle^{\otimes m}|\psi\rangle \to \frac{1}{2^{m/2}}\sum_{x=0}^{2^m-1}|x\rangle|\psi\rangle$$

Step3：$|x\rangle|\psi\rangle \to |x\rangle U^x|\psi\rangle$ を作用させる．

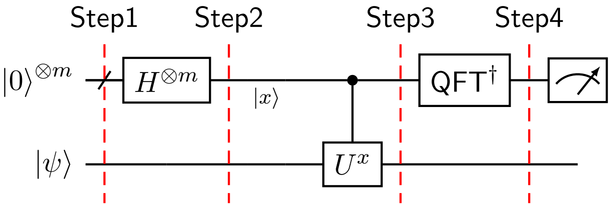
$$\frac{1}{2^{m/2}}\sum_{x=0}^{2^m-1}|x\rangle|\psi\rangle \to \frac{1}{2^{m/2}}\sum_{x=0}^{2^m-1}|x\rangle U^x|\psi\rangle\left(=\frac{1}{2^{m/2}}\sum_{x=0}^{2^m-1}\exp(2\pi\mathrm{i}\phi x)|x\rangle|\psi\rangle\right)$$

Step4: 最初の m-qubit に逆 QFT を作用させる

$$\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}\exp(2\pi\mathrm{i}\phi x)|x\rangle|\psi\rangle \to \frac{1}{2^m}\sum_{j=0}^{2^m-1}\sum_{k=0}^{2^n-1}\exp\left(-\frac{2\pi k\mathrm{i}}{2^m}(j-2^m\phi)\right)|j\rangle|\psi\rangle$$

Step5: 第 1 レジスタを測定

回路図（位相推定アルゴリズム）



測定すると...

$2^m\phi$ が整数のとき

Step4 終了後は，

$$|2^m\phi\rangle\,|\psi\rangle$$

となる．測定を行うと，常に $2^m\phi$ が測定される．

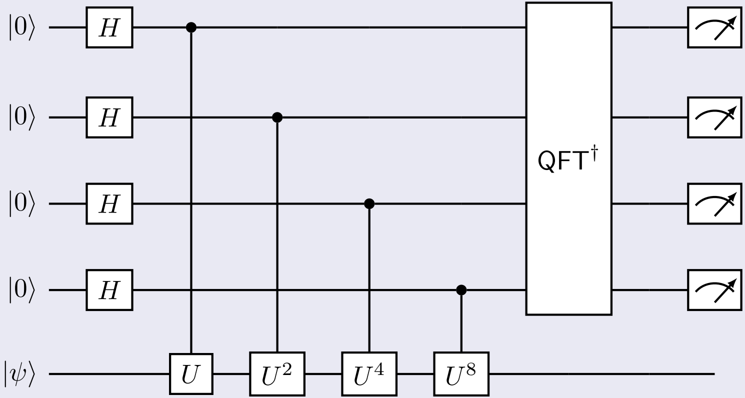
一般の ϕ の場合

測定を行うと，

$$\lfloor 2^m\phi + \frac{1}{2}\rfloor$$

をある一定の確率で得られる．
ϕ の近似値を m ビットの精度で得られたことになる．

位相推定回路 $(m=4)$ の場合



目次

1. 隠れ部分群問題
2. Quantum Fourier Transformation
3. 初期のアルゴリズム（DJ, BV, Simon）
    - Deutsch–Jozsa, Bernstein–Vazirani アルゴリズム
    - Bernstein–Vazirani 問題
    - Simon のアルゴリズム
4. 素因数分解，離散対数アルゴリズム
    - 位相推定アルゴリズム
    - 素因数分解アルゴリズム
    - 離散対数問題を解くアルゴリズム
5. まとめ

素因数分解アルゴリズム

Shor の（古典部分での）アルゴリズムの戦略

ターゲットとする合成数 N，N と互いに素な自然数 a に対して，

$$a^r \bmod N = 1$$

となる自然数 r を求める．

r を求めることと素因数分解の関係

- r を求めることができれば，古典的な計算により（一定の確率で）N の因数を見つけることが多項式時間で可能．
- 逆に，素因数分解ができれば，r を求めることが可能．
- これより，【素因数分解をすること】と【r を求めること】の難しさは等しい．

量子パートは，位相推定アルゴリズムを利用

位相推定問題への翻訳

ユニタリ変換 $U|y\rangle = |ay \bmod N\rangle$ を考える．

天下り的に...

U の固有値は，$j = 0, 1, 2, \ldots, r-1$ に対して，

$$\exp\left(2\pi\mathrm{i}\,\frac{j}{r}\right)$$

で与えられる．対応する固有ベクトルは，

$$|w_j\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left(-\frac{2\pi kj\mathrm{i}}{r}\right)|a^k \bmod N\rangle$$

位相推定アルゴリズムを用いて，j/r を m ビットの精度で求める．

アルゴリズムの残り

問題点

その 1： 固有ベクトルを知らない（r が含まれているので）

その 2： U^{2^k} はどうやって計算したらいいのか？(素朴な実装では 2^k 回 U を適用しないといけない)

その 3： j/r の近似値から r をどうやって求めるのか？

問題点その 1 の解決

固有ベクトルは知らなくてよい．

$$\frac{1}{\sqrt{r}}\sum_{j=0}^{r-1}|w_j\rangle = |1\rangle$$

となる．$|1\rangle$ は固有ベクトルが全て足し合わされたもの．固有ベクトルの代わりに，$|1\rangle$ を使うことにする．

問題点その 2 の解決

$U^{2^k}|x\rangle = |a^{2^k}x \bmod N\rangle$ で十分．
$A_k := a^{2^k} \bmod N$ を古典的に計算し，

$$|x\rangle \to |A_k x \bmod N\rangle$$

をダイレクトに行う回路 (Modular multiplication circuit) を構成．

問題点その 3 の解決

得られた j/r の近似値を連分数展開することにより，j と r を求める．
$m = 2\lfloor \log N \rfloor + 1$ とすれば十分．
（直観的には，j も r も $\log N$ ビットなので，復元に必要な情報は得られたことになる）

二進近似からの有理数復元

問題

r は 4 ビットとし，s/r の 9 ビット近似値 $\phi = 0.010001011$ が得られたとする．ここから，s と r を求めたい．

ϕ の値は，$139/512$

- $\frac{512}{139} = 3 + \frac{95}{139}$
- $\frac{139}{95} = 1 + \frac{44}{95}$
- $\frac{95}{44} = 2 + \frac{7}{44}$
- $\frac{44}{7} = 6 + \frac{2}{7}$
- $\frac{7}{2} = 3 + \frac{1}{2}$
- $\frac{2}{1} = 2$

これより，$\frac{139}{512} = [3, 1, 2, 6, 3, 2]$ となる．途中で打ち切った値は，

$$[3] = \frac{1}{3} \to [3, 1] = \frac{1}{4} \to [3, 1, 2] = \frac{3}{11} \Rightarrow (s, r) = (3, 11)$$

r の値から素因数分解をする

r が求められたとする．ただし，r は偶数であるとする．
$a^r \bmod N = 1 \Rightarrow (a^{r/2})^2 \bmod N = 1$
これより，$a^{r/2} \bmod p = \pm 1, a^{r/2} \bmod q = \pm 1$

$$\begin{cases} a^{r/2} \bmod p = +1, & a^{r/2} \bmod q = -1 \\ a^{r/2} \bmod p = -1, & a^{r/2} \bmod q = +1 \end{cases}$$

のとき，素因数分解可能．前者の場合は，$\gcd(a^{r/2} - 1, N) = p$．

素因数分解回路

Step1：初期状態を用意．ただし，$m = \lfloor 2\log N \rfloor + 1$

$$|0\rangle^{\otimes m} |1\rangle$$

Step2：第 1 レジスタ（先頭 m-qubit）に対してアダマール変換を施す．

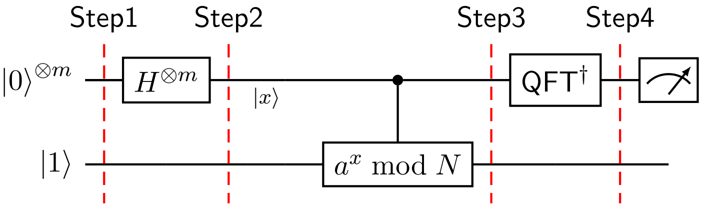
$$|0\rangle^{\otimes m} |1\rangle \to \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle |1\rangle$$

Step3：べき乗剰余を適用する．

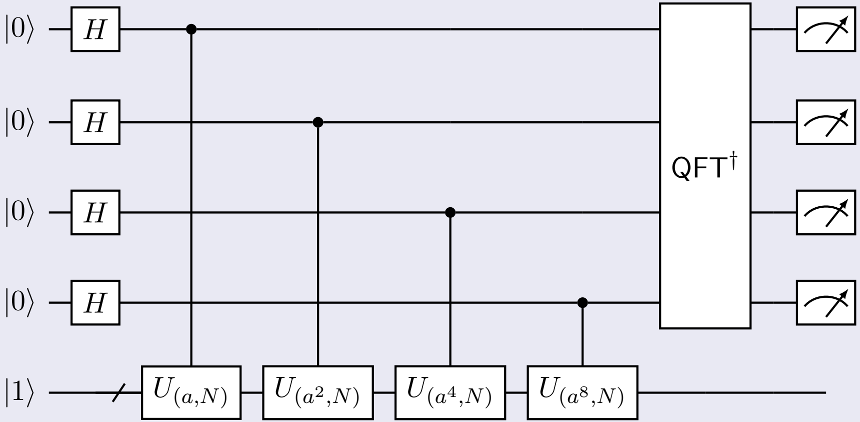
$$\frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle |1\rangle \to \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle |a^x \bmod N\rangle$$

Step4: 最初の m-qubit に逆 QFT を作用させる
Step5: 第 1 レジスタを測定

回路図（素因数分解回路）


Step1
Step2
Step3
Step4
$|0\rangle^{\otimes m}$
$|1\rangle$
$H^{\otimes m}$
$|x\rangle$
$a^x \bmod N$
$\mathrm{QFT}^\dagger$

$(m = 4)$ の場合



$U_{(b,N)} : |y\rangle \to |by \bmod N\rangle$ の実装をすれば十分

離散対数問題を解く量子アルゴリズム

Step1：初期状態を用意．ただし，$t = \lfloor \log q \rfloor + 1$

$$|0\rangle^{\otimes t} |0\rangle^{\otimes t} |1\rangle$$

Step2：第 1 レジスタ，第 2 レジスタに対してアダマール変換を施す．

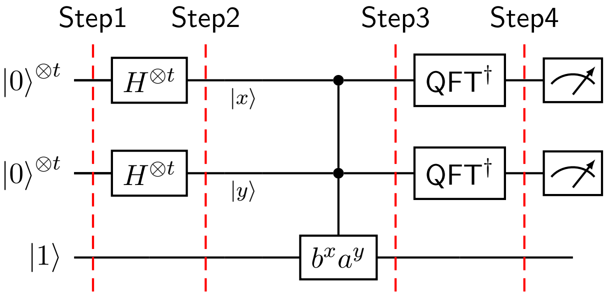
$$\to \frac{1}{2^t} \sum_{x=0}^{2^t-1} \sum_{y=0}^{2^t-1} |x\rangle |y\rangle |1\rangle$$

Step3：べき乗計算を適用する．

$$\to \frac{1}{2^t} \sum_{x=0}^{2^t-1} \sum_{y=0}^{2^t-1} |x\rangle |y\rangle |b^x a^y\rangle$$

Step4: 第 1 レジスタ，第 2 レジスタに対して逆 QFT を作用させる
Step5: 第 1 レジスタ，第 2 レジスタを測定

回路図（離散対数問題を解く回路）



- Step3 でのべき乗演算が一番大変
- Step5 での測定により，sl/q の近似値と l/q の近似を得ることができる．ここから，連分数展開を用いることにより，s（と l）を求める．

非可換の G に対する量子フーリエ変換

既知の事実

- （非可換でも）群の要素の行列表現を経由して，フーリエ変換は定義可能
- 対称群 S_n 上で効率的にフーリエ変換をする量子アルゴリズムは存在する．
- S_n 上の隠れ部分群問題を解くアルゴリズムは知られていない

量子計算と暗号に関する解説

CRYPTREC 外部評価報告書

https://www.cryptrec.go.jp/ex_reports.html

2019 年度
量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価
（細山田 光倫さん@ NTT）
Simon のアルゴリズムを用いた共通鍵暗号の攻撃，Grover のアルゴリズムを用いたハッシュ関数の攻撃

2020 年度
Shor のアルゴリズム実装動向調査（高安 敦先生@東大）

電子情報通信学会会誌

量子計算機に対する暗号の安全性解析（國廣），2022 年６月号（筑波大レポジトリよりダウンロード可）

まとめ

1. 隠れ部分群問題
2. Quantum Fourier Transformation
3. 初期のアルゴリズム（DJ, BV, Simon）
   - Deutsch–Jozsa, Bernstein–Vazirani アルゴリズム
   - Bernstein–Vazirani 問題
   - Simon のアルゴリズム
4. 素因数分解，離散対数アルゴリズム
   - 位相推定アルゴリズム
   - 素因数分解アルゴリズム
   - 離散対数問題を解くアルゴリズム
5. まとめ