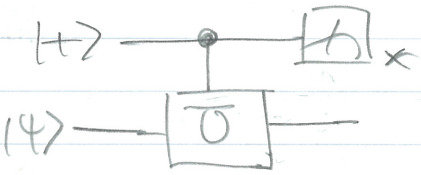
⑥量子アルゴリズム

∨ Hadamard テスト



$$P_+ = \frac{1}{2}(1 + \mathrm{Re}\langle\psi|U|\psi\rangle)$$

$$P_- = \frac{1}{2}(1 - \mathrm{Re}\langle\psi|U|\psi\rangle)$$

レポート
計算せよ。

- Uが固有値±1のエルミート演算子（パウリ演算子など）のときは、固有状態測定となる (∨)

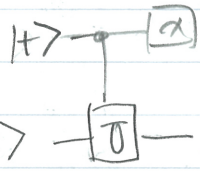
- Hadmad test で N回繰り返すとき N_+回 +1が得られたとするとき (∨)

$$P\left(\left|\frac{N_+}{N} - P_+\right| \geq \delta\right) \leq 2e^{-2\delta^2 N}$$

Chernoff + Hoeffding bound

- $|\psi\rangle$が右の固有状態のときは、Uの固有値の測定
- $|\psi\rangle$が完全混合状態のときは $\mathrm{Tr}[U]$ (∨)

Uの固有状態 $|\lambda\rangle$ が与えられているとする。



$U|\lambda\rangle = e^{i\lambda}|\lambda\rangle$ とする

$|0\rangle|\lambda\rangle \Rightarrow |0\rangle|\lambda\rangle$

$|1\rangle|\lambda\rangle \rightarrow e^{i\lambda}|1\rangle|\lambda\rangle$ 位相がひろう

λをもっと精度よく（指数精度）

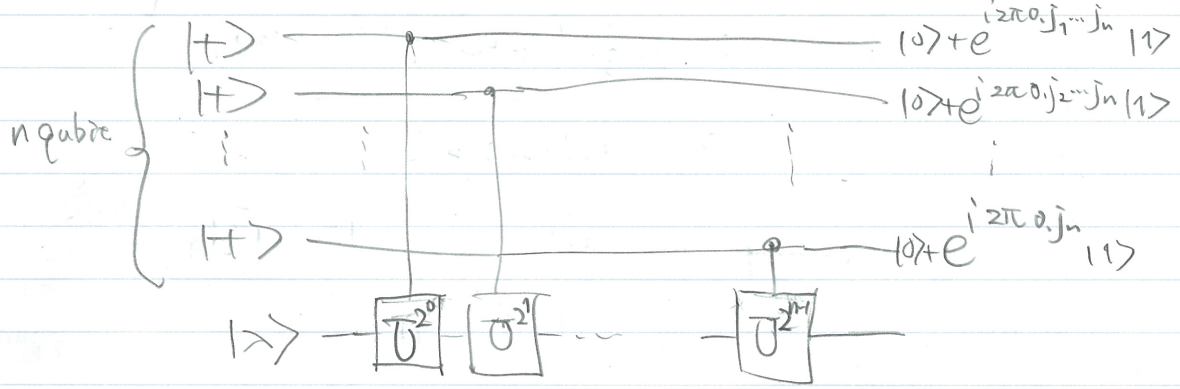
決められない？

→ Kitaev の位相推定アルゴリズム

∨ Kitaev の位相推定アルゴリズム

U の固有状態を $|\lambda\rangle$, その固有値を $e^{i2\pi\lambda}$ とする.
ただし, $\lambda = 0.j_1 j_2 \cdots j_n$ とする.

$$\left(\lambda = \sum_{k=1}^{n} \left(\frac{1}{2}\right)^k j_k \right)$$



∨ 量子フーリエ変換.

$$F|y\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i xy/N} |x\rangle \qquad y, x = 0, 1, \cdots, N-1$$

2進数表示 $(2^n = N)$ $\quad y \Rightarrow y_1 y_2 \cdots y_n$, $\quad x = x_1 x_2 \cdots x_n$

$$F|y\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} e^{2\pi i xy/2^n} |x\rangle$$

回路

$$= \frac{1}{2^{n/2}} \sum_{x_1=0}^{1} \cdots \sum_{x_n=0}^{1} e^{2\pi i \left[\sum_{k=1}^{n} \left(\frac{1}{2}\right)^k x_k\right] y} |x_1 \cdots x_n\rangle$$

$$= \frac{1}{2^{n/2}} \bigotimes_{k=1}^{n} \sum_{x_k=0}^{1} e^{2\pi i \left(\frac{1}{2}\right)^k x_k y} |x_k\rangle$$

$$= \frac{1}{2^{n/2}} \bigotimes_{k=1}^{n} \left(|0\rangle + e^{2\pi i \left(\frac{1}{2}\right)^k y} |1\rangle \right)$$

$y = y_1 y_2 \cdots \underbrace{y_n}$

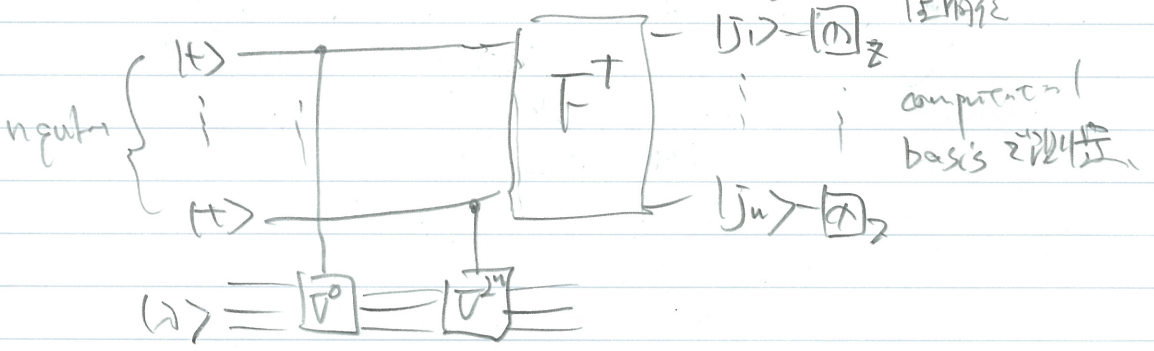
ここで $e^{2\pi i (\frac{1}{2})^k y} = e^{2\pi i\, 0.\, y_{n-k+1} \cdots y_n}$

よって

$$F|y_1 y_2 \cdots y_n\rangle = \frac{1}{2^{n/2}} \bigotimes_{k=1}^{n} \left(|0\rangle + e^{2\pi i\, 0.\, y_{n-k+1} \cdots y_n} |1\rangle \right)$$

逆変換は $\frac{1}{2^{n/2}} \bigotimes_{k=1}^{n} \left(|0\rangle + e^{2\pi i\, 0.\, y_{n-k+1} \cdots y_n} |1\rangle \right) \xrightarrow{F^\dagger} |y_1 \cdots y_n\rangle$

Kitaevの位相推定アルゴリズムに戻る.



位相化を指数精度で推定できる

注) U^{2^n} が多項式的に容易でないと多項式時間量子アルゴリズムにはならない!!

✓ 冪剰余と素因数分解アルゴリズム

(modular exponential)

x と N を互いに素とする. $|y\rangle \xrightarrow{U_x} |x \cdot y \bmod N\rangle$

$$U_x = \sum_y |x \cdot y \bmod N\rangle\langle y|$$

$$U_x^2 = \sum_y |x^2 \cdot y \bmod N\rangle\langle y|$$

$$U_x^{2^k} = \sum_y |x^{2^k} \cdot y \bmod N\rangle\langle y|$$

↳ 効率よく計算できる.

位数 r を $x^r \equiv 1 \pmod N$ を満す最小の整数とする

ある状態 $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^k \bmod N\rangle$

$(0 \leq s \leq r-1)$

は、 $U_x |u_s\rangle = \exp\left[\frac{2\pi i s}{r}\right] |u_s\rangle$ を満す。

Shorの位相推定アルゴリズムより $\frac{s}{r}$ を満めることができる。

- $|u_s\rangle$ の準備は $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle |1\rangle$ より $|1\rangle$ を射影し、
  固有空間への射影により得られる。
  (位相推定アルゴリズム)

- 満めた位相 $\varphi \approx \frac{s}{r}$ から連分数展開により、
  r を求める
- 連分数展開 (例)

$$\frac{31}{13} = 2.3846153\cdots$$

$$= 2 + 0.3846153\cdots$$

$$= 2 + \frac{1}{\frac{1}{0.3846153\cdots}} = 2 + \frac{1}{2.600\cdots}$$

$$= 2 + \frac{1}{2 + \frac{1}{1.66\cdots}}$$

$$= 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1.50\cdots}}}$$

$$= 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}$$

$$= \frac{31}{13}$$

✓ 素因数分解.

→ 互いに素な x と N に対して $x^r = 1 \pmod N$ が求まった.

N を合成数とすると, r は高い確率で(えられない) 偶数となり,

$$(x^{r/2}-1)(x^{r/2}+1) = 0 \pmod N$$

N と $x^{r/2}-1$ もしくは $x^{r/2}+1$ との最大公約数は N の因数となる → 素因数分解!! (ユークリッドの互除法)