量子コンピュータの基礎と物理との接点

(集中講義 @お茶水女子大学)

Part 1. 量子情報 & 量子計算の基礎.

Part 2. 量子誤り訂正 (スタビライザー形式)

Part 3. 物理との接点 (スピングラス模型, トポロジカル秩序)

Part 1. 量子情報 & 量子計算の基礎.

◎ 量子力学 (有限次元) の復習.

○状態. $\{|1\rangle, |2\rangle, \cdots, |d-1\rangle\}$ 正規直交基底

$$|\psi\rangle = \sum_{i=1}^{d} c_i |i\rangle \quad , \quad \sum_i |c_i|^2 = 1$$

c_i ← complex

$$|\psi\rangle = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_d \end{pmatrix}$$ 複素列ベクトル.

ケット

$$(|\psi\rangle)^\dagger = \langle\psi| = (c_1^* \ c_2^* \cdots c_d^*)$$ 行ベクトル.

ブラ.

$$(|\phi\rangle)^\dagger (|\psi\rangle) = \langle\phi|\psi\rangle$$

内積.

○時間発展、

転置＋複素共役、

$$|\psi'\rangle = U|\psi\rangle$$

$\underbrace{}_{}$ ユニタリ演算子、 $U^{\dagger} U = I$

$$U = \begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1d} \\ \vdots & \ddots & & \\ u_{d1} & \cdots & & u_{dd} \end{pmatrix}$$

○測定　$\{P_i\}$ 射影演算子、 $\left(\begin{array}{l} \sum_i P_i = I \\ P_i P_j = \delta_{ij} P_i \end{array} \right)$

iを得る確率　$p_i = \| P_i |\psi\rangle \|^2$　(例) $P_i = |i\rangle\langle i|$

$$= (\langle\psi|P_i)(P_i|\psi\rangle) \qquad |i\rangle\langle i| = \begin{pmatrix} 0 & & & \\ & 0 & & \\ & & 1 & \\ & & & \ddots \; 0 \end{pmatrix}$$

$$= \langle\psi|P_i|\psi\rangle$$

$$= Tr[P_i |\psi\rangle\langle\psi|]$$

(トレース　$Tr[A] = \sum_i \langle i|A|i\rangle$
$Tr[ABC] = Tr[CAB]$)

状態ベクトルから作った
演算子 → 密度行列

(例1) $\dfrac{|0\rangle+|1\rangle}{\sqrt{2}} \equiv |+\rangle$, $\left(|-\rangle = \dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$

$P_0 = |0\rangle\langle 0|$, $P_1 = |1\rangle\langle 1|$

$$p_0 = \left(\frac{\langle 0|+\langle 1|}{\sqrt{2}}\right) |0\rangle\langle 0| \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)$$

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

$$= \frac{1}{2}\Big(\langle 0|0\rangle\langle 0|0\rangle + \cancel{\langle 0|0\rangle\langle 0|1\rangle} + \cancel{\langle 1|0\rangle\langle 0|0\rangle + \langle 1|0\rangle\langle 0|1\rangle}\Big)$$

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

$p_1 = \dfrac{1}{2}$

○混合状態、

確率 q_j で、$|\psi_j\rangle$ が与えられる。

$$P_i = \sum_j q_j \mathrm{Tr}[P_i |\psi_j\rangle\langle\psi_j|]$$

$$= \mathrm{Tr}\Big[P_i \underbrace{\sum_j q_j |\psi_j\rangle\langle\psi_j|}_{\rho}\Big]$$

密度演算子、ρ　(古典的な統計性もとり込んだ状態の表記、

○密度演算子、

・$\rho = \rho^\dagger$　(エルミート)

・$\rho \geq 0$　(半正定値行列)

positive. $\forall |\psi\rangle,\ \langle\psi|\rho|\psi\rangle \geq 0$
(固有値が非負)

・$\mathrm{Tr}[\rho] = 1$、$\left(\because \sum_i P_i = \sum_i \mathrm{Tr}[P_i \rho] = \mathrm{Tr}[\rho]\right)$

(例)

$$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \rho$$

$P_0 = |0\rangle\langle 0|$, $P_1 = |1\rangle\langle 1|$

$p_1 = \frac{1}{2}$, $p_2 = \frac{1}{2}$.

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ との違い。

$P_+ = |+\rangle\langle +|$, $P_- = |-\rangle\langle -|$

$|+\rangle \to p_+ = 1, \quad p_- = 0$,

$\rho \to p_+ = \frac{1}{2}, \quad p_- = \frac{1}{2}$.

重ねあわせと混合の違い。

○複合系

A　B　　AB系の基底

$\{|i\rangle_A\}$　$\{|j\rangle_B\}$ $\longrightarrow$ $|ij\rangle_{AB} = |i\rangle_A \otimes |j\rangle_B$

テンソル積。

$|\psi\rangle_{AB} = c_{ij}|ij\rangle_{AB}$.

$|\psi_A\rangle = \sum_i a_i |i\rangle_A$

$|\phi_B\rangle = \sum_j b_j |j\rangle_B$

$$|\psi\rangle_A \otimes |\phi\rangle_B = \sum_{ij} (a_i |i\rangle_A)(b_j |j\rangle_A)$$

$$= \sum_{ij} a_i b_j |ij\rangle_{AB}$$

$$(U_A \otimes V_B)|\psi\rangle_A |\phi\rangle_B = (A|\psi_A\rangle)(B|\phi\rangle_B)$$

$$\underset{d\text{次元}}{\begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix}} \otimes \underset{d'\text{次元}}{\begin{pmatrix} b_1 \\ \vdots \\ b_{d'} \end{pmatrix}} = \underset{d\times d'\text{次元.}}{\begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ \vdots \\ a_1 b_{d'} \\ \vdots \\ a_d b_1 \\ \vdots \\ a_d b_d \end{pmatrix}}$$

クロネッカー積

$$A \otimes B = \begin{pmatrix} a_{11} & \cdots & a_{1d} \\ \vdots & \ddots & \vdots \\ a_{d1} & \cdots & a_{dd} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & \cdots & b_{1d'} \\ \vdots & \ddots & \vdots \\ b_{d'1} & \cdots & b_{d'd'} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11} \begin{pmatrix} b_{11} & b_{12} \cdots & b_{1d'} \\ \vdots & \ddots & \\ b_{d'1} & & b_{d'd'} \end{pmatrix} & \cdots & a_{1d} \begin{pmatrix} \cdots \\ \vdots & \ddots \end{pmatrix} \\ \vdots & \ddots & \\ a_{d1} \begin{pmatrix} \cdots \\ \vdots & \ddots \end{pmatrix} & & a_{dd} \begin{pmatrix} \cdots \\ \vdots & \ddots \end{pmatrix} \end{pmatrix}$$

(例)

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

特に $|\psi\rangle_A \otimes |\varphi\rangle_B$ と書ける状態

→ セパラブル状態

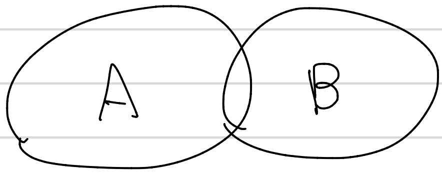
書けない状態 → エンタングル状態

(例) $$\frac{|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B}{\sqrt{2}}$$

$$= \frac{|+\rangle_A |+\rangle_B + |-\rangle_A |-\rangle_B}{\sqrt{2}}$$

基底に依存せずエンタングルしている.

○縮約密度演算子 (reduced density matrix)



ρ_{AB}

Bに関する情報を一切利用できないとき、

A上での確率分布は?

A上での時間発展は?

$$p_i = \mathrm{Tr}\left[P_i^{(A)}\otimes I^{(B)}\left(U^{(A)}\otimes I^{(B)}\right)\rho_{AB}\left(U^{(A)}\otimes I^{(B)}\right)^{\dagger}\right]$$

$$= \sum_{ij} \langle i|_A\otimes\langle j|_B \quad |i\rangle_A\otimes|j\rangle_B$$

$$= \mathrm{Tr}\left[P_i^{(A)}\, U^{(A)}\, \rho_A\, U^{(A)\dagger}\right]$$

$$\rho_A = \mathrm{Tr}_B\left[\rho_{AB}\right]$$

部分トレース $= I_A\otimes\langle j|_B\, \rho\, |j\rangle_B\otimes I_A$

reduced density operator

(例1) $\dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$

↳ ・ AとBがエンタングル
= Bを失うと情報を失う。

$\rho_A = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$

$S(\rho_A) = -\rho_A \log \rho_A$

$= 1$ エンタングルメント
エントロピー

フォンノイマン
エントロピー

◎量子ビット.

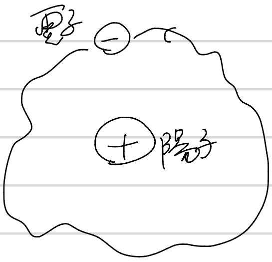
$$\begin{pmatrix}1\\0\end{pmatrix} \qquad \begin{pmatrix}0\\1\end{pmatrix}$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$ 量子ビット.

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \qquad |\alpha|^2 + |\beta|^2 = 1.$$

(量子情報の最小単位)

水素原子 シュレーディンガー方程式



$$H = -\frac{\hbar^2}{2\mu}p^2 + V(r)$$

$$H\psi(r,\theta,\phi) = E\psi(r,\theta,\phi)$$

1s, 2s, 2p 軌道…

$$\psi = \alpha\psi_s + \beta\psi_p$$

もし、2状態以外はほとんど出てこない.

スピン1/2 → $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

→ $|\uparrow\rangle = |0\rangle$ $\quad |\downarrow\rangle = |1\rangle$

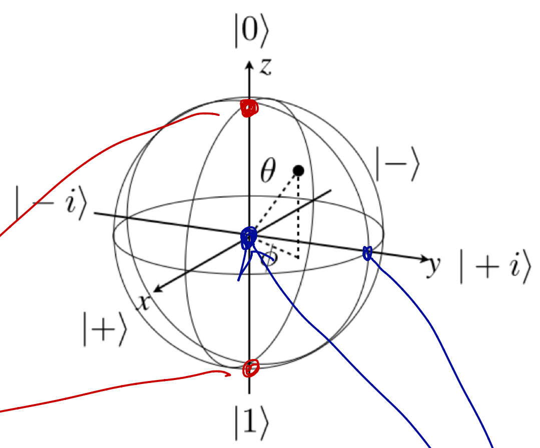
光子の偏光 $|H\rangle, |V\rangle$

直交する2つの量子状態なら何でもOK

○ブロッホ球

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |\alpha|^2 + |\beta|^2 = 1.$$

$$\alpha = \cos\frac{\theta}{2}, \quad \beta = e^{i\phi}\sin\frac{\theta}{2}$$



$$(r_x, r_y, r_z) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta),$$

古典ビットは2点しかとりえない。

球面上どの点もとりうる。

混合状態

$$(r_x, r_y, r_z) = \underline{(\mathrm{Tr}[X\rho], \mathrm{Tr}[Y\rho], \mathrm{Tr}[Z\rho])}$$

パウリ演算子は次のページ

混合 $\frac{I}{2} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$

重ね合せ、$|+\rangle$

○パウリ演算子、

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$: bit flip.

$\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$

(古典情報にもある)

$Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$

phase flip

(重ね合わせのある量子特有)

$XZ = -ZX$

$Y = -iXZ$, $X^2 = Y^2 = Z^2 = I$

○ Hadamard 演算子、Phase 演算子、

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

- $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |+\rangle$

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

- $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \equiv |-\rangle$

- $X|+\rangle = |+\rangle, \quad X|-\rangle = -|-\rangle$

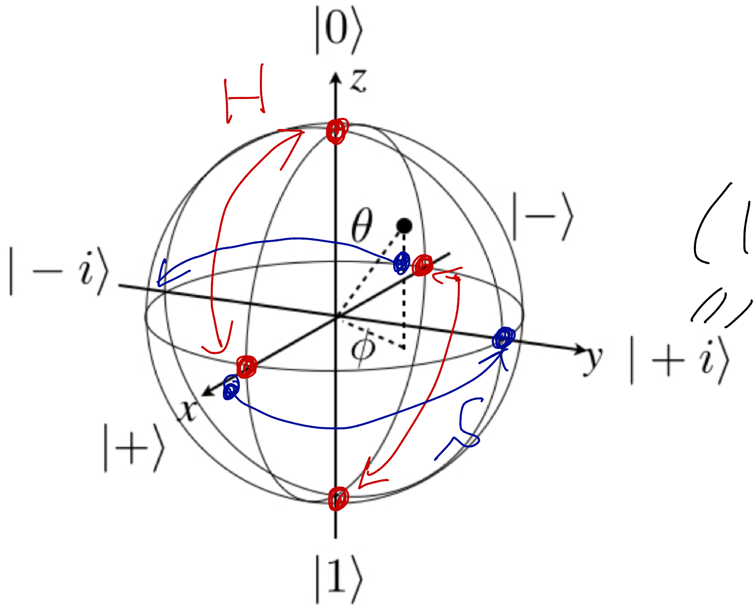
→ Zの固有状態をXへ…

・ $S|0\rangle = |0\rangle, \quad S|1\rangle = i|1\rangle$

$S|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$

$\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$

$\equiv$



$(|0\rangle + i|1\rangle)/\sqrt{2}$

//

○ 1量子ビット演算, SU(2)

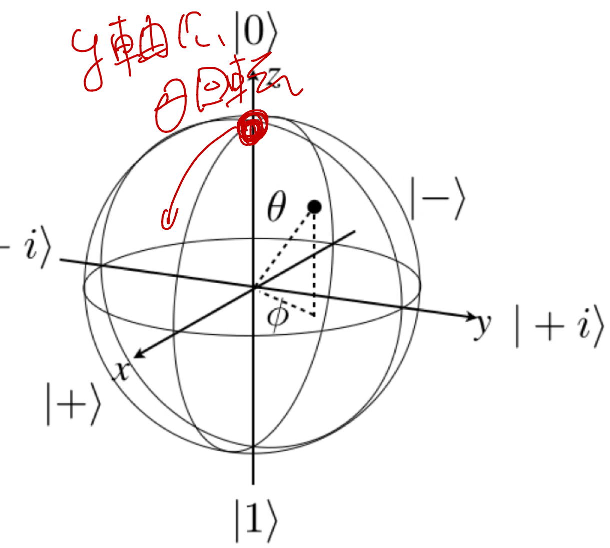
2×2 複素ユニタリ行列, $\det(U)=1$

(例) $$e^{-i\frac{\theta}{2}Y} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y$$

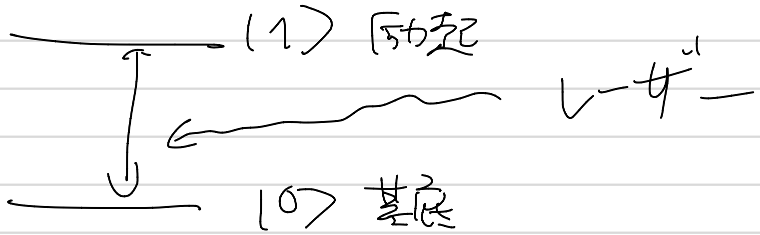
(テーラー展開 & $Y^2 = I$)

$$e^{-i\frac{\theta}{2}Y}\left(-\right)^\dagger = I$$

$$\begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix}$$



$$e^{-i\frac{\theta}{2}Y}|0\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$$



一般に任意のSU(2)は

$$U = e^{i\alpha X} e^{i\beta Z} e^{i\gamma X}$$

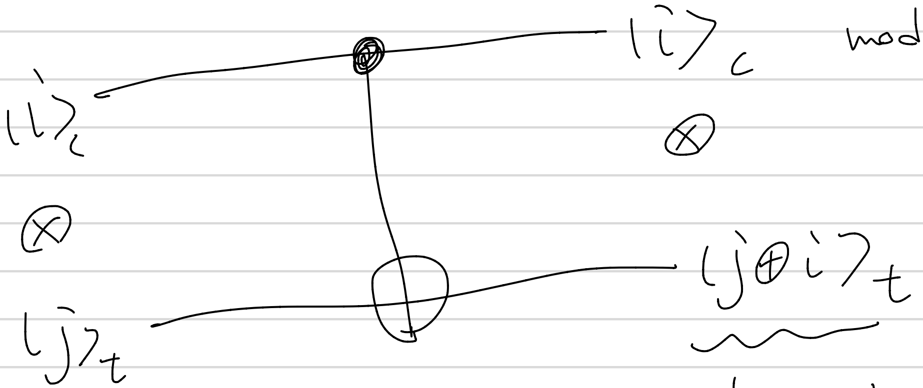
(オイラー分解).

○ CNOT演算.

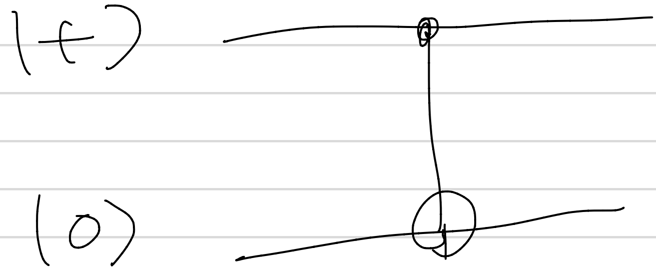
$$\Lambda(X) = |0\rangle\langle 0|_c \otimes I_t + |1\rangle\langle 1|_c \otimes X_t = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

$$\Lambda(X)|i\rangle_c\otimes|j\rangle_t = |i\rangle_c \otimes |j\oplus i\rangle_t$$

mod 2の和.



古典計算では
XOR
排他的論理和.



$$\Lambda(X)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_c\otimes|0\rangle_t = \Lambda(X)\frac{1}{\sqrt{2}}|0\rangle|0\rangle + \Lambda(X)\frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

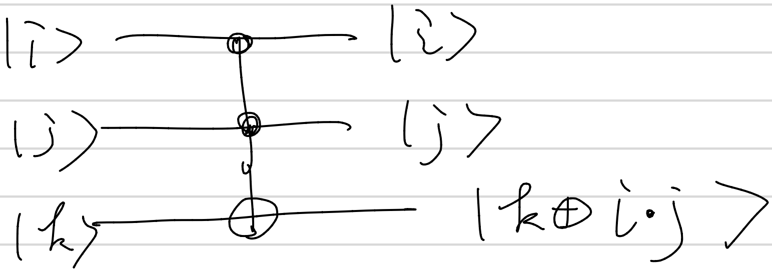
$$= \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$$

エンタングル状態が発生.

① 古典可逆計算

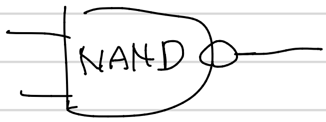
○ Toffoli 演算. (3量子ビット演算)

$$\Lambda^2(X) = |00\rangle\langle 00| \otimes I + |01\rangle\langle 01| \otimes I + |10\rangle\langle 10| \otimes I + |11\rangle\langle 11| \otimes X$$



k=1 にすると 古典では NAND
に対応.

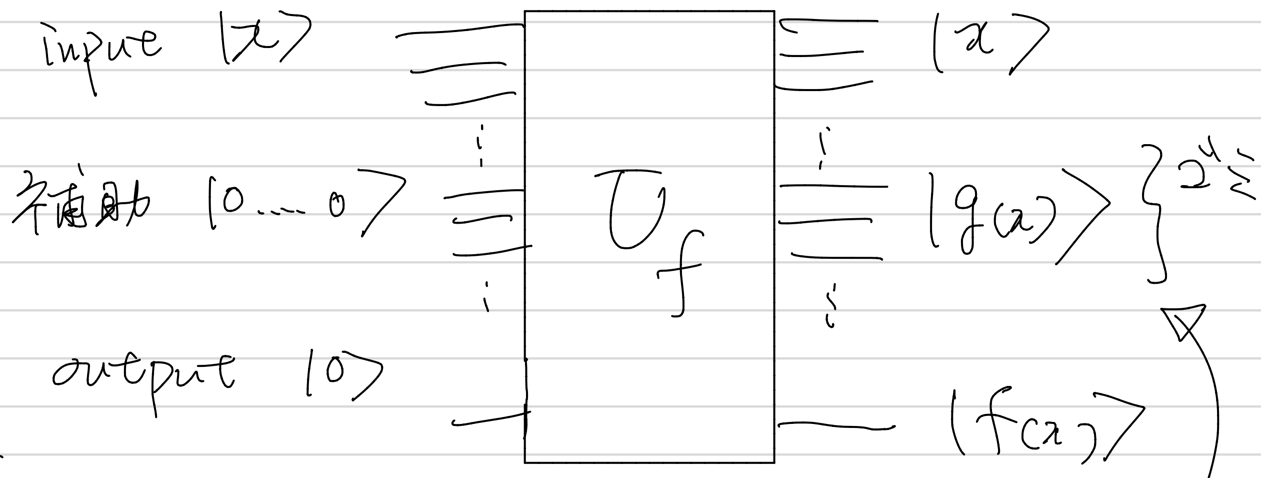
NANDだけで任意の
古典計算を作れる.



0	0	→ 1
0	1	→ 1
1	0	→ 1
1	1	→ 0

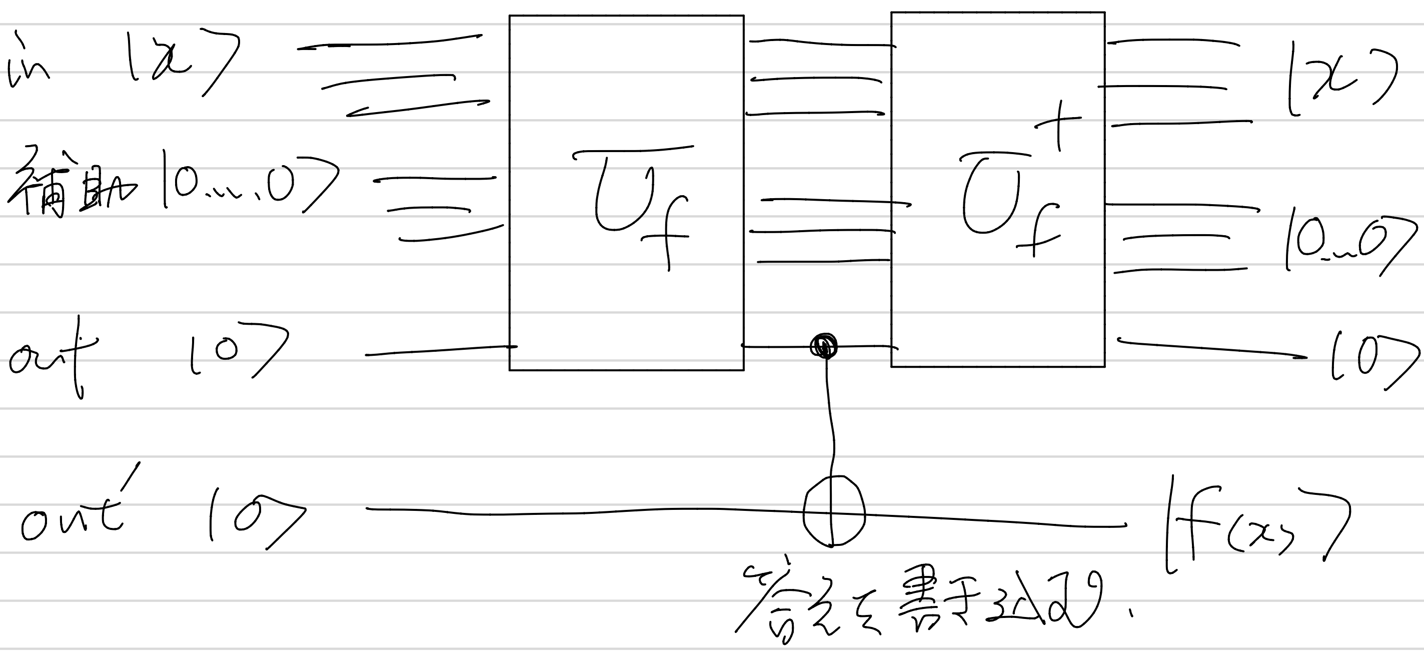
○ 可逆古典計算

input x ⟶ output $f(x)$



uncomputation

消すのに
エネルギーが必要。



ゴミを残さずに可逆計算できる!!

◎ ユニバーサル量子計算.

。CNOT と SU(2) を組みあわせて,

任意の N量子ビットユニタリ $SU(2^n)$ が作れる.

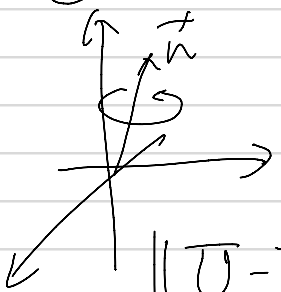
。SU(2) は H と $e^{-i\frac{\pi}{8}Z}$ で作れる.

（Solovay-Kitaev の定理）

density implies fast approximation!

$e^{-i\frac{\pi}{8}Z} H e^{-i\frac{\pi}{8}Z} H \to \vec{n} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$ 軸に;

$\cos(\frac{\theta}{2}) = \cos^2\frac{\pi}{8}$ を満す θ 回転



π の 無理倍.

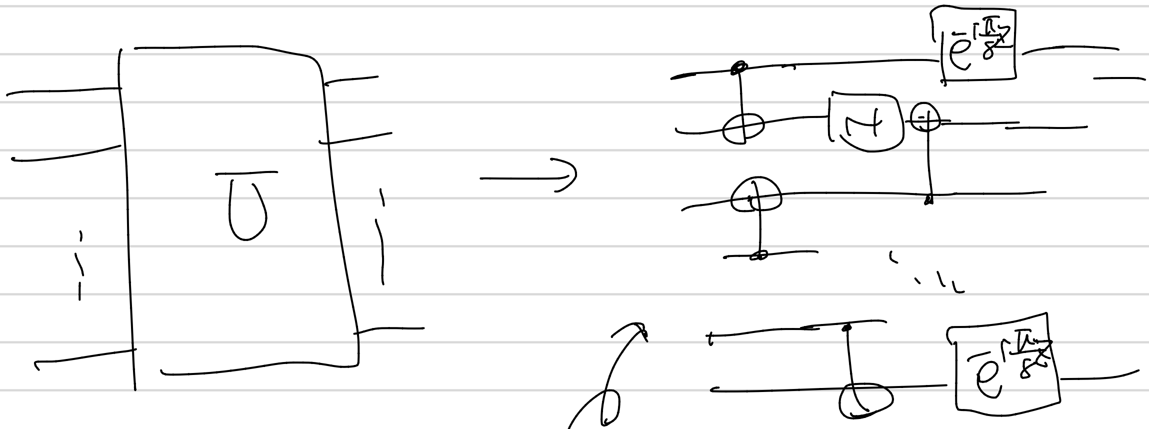
= すべてをうめつくす

$\|U - U^{app}\| \le \epsilon$, overhead は

目標　近似

poly $\log(1/\epsilon)$!!

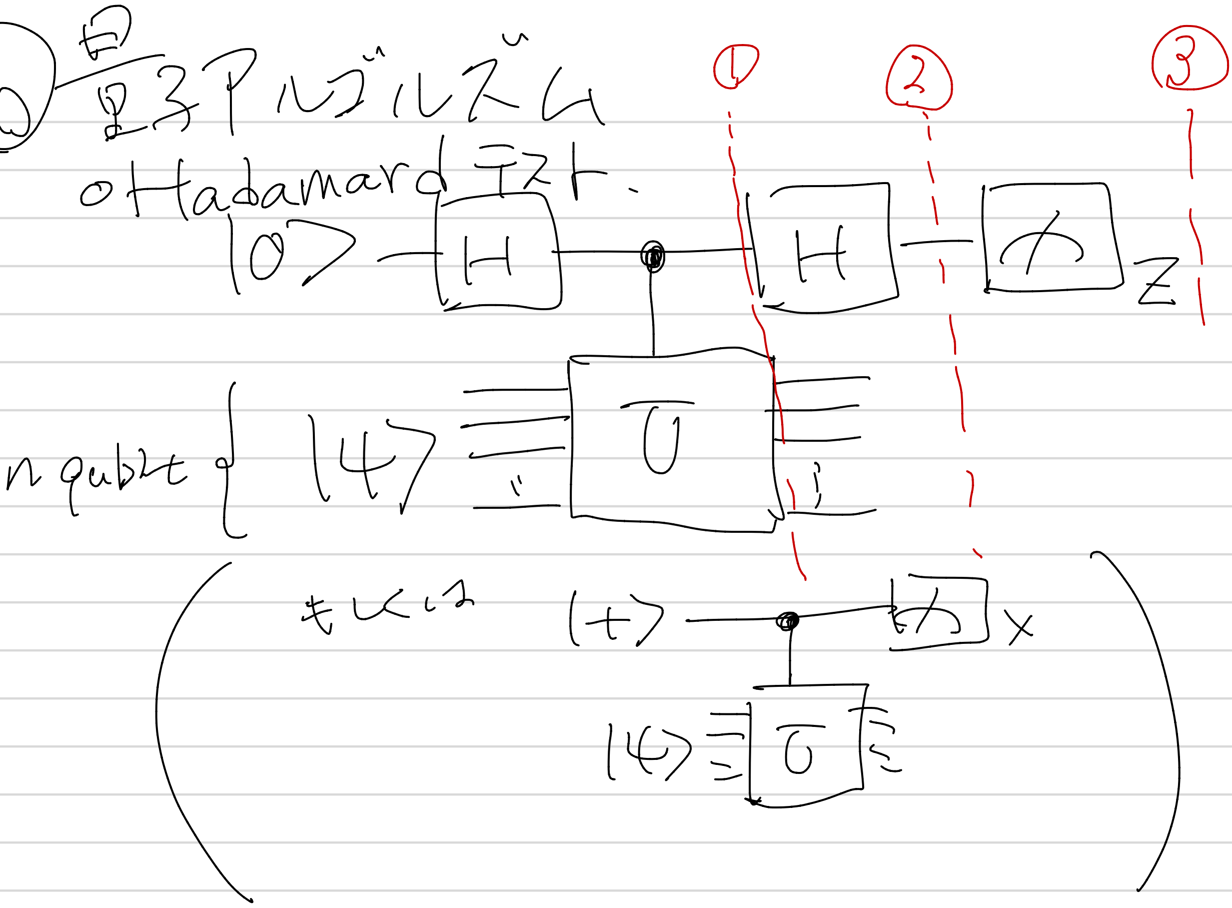
$\{CNOT, H, e^{-i\frac{\pi}{8}Z}\}$ universal gate set.



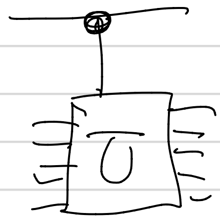
量子力学で記述される我々の世界.

① 量子アルゴリズム

・Hadamardテスト.



$\Lambda(U)$: controlled-U



$$= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

$2^n \times 2^n$ ユニタリ行列.

これまでの知識を使って、出力の確率を計算してみよう.

①まで

$$\left(|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes U\right)\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes|\psi\rangle$$

$$= \frac{1}{\sqrt{2}}|0\rangle|\psi\rangle + \frac{1}{\sqrt{2}}|1\rangle U|\psi\rangle$$

②まで

$$\frac{1}{2}(|0\rangle+|1\rangle)|\psi\rangle + \frac{1}{2}(|0\rangle-|1\rangle)U|\psi\rangle$$

$$= \frac{1}{2}|0\rangle(I+U)|\psi\rangle + \frac{1}{2}|1\rangle(I-U)|\psi\rangle$$

③

$$p_0 = \Big\| \underset{\substack{\shortparallel \\ |0\rangle\langle 0|\otimes I}}{P_0}\left(\frac{1}{2}|0\rangle(I+U)|\psi\rangle + \cdots\right)\Big\|^2$$

$\| |\phi\rangle \|^2 = \langle\phi|\phi\rangle$

$$= \left\|\frac{1}{2}|0\rangle(I+U)|\psi\rangle\right\|^2$$

$$= \frac{1}{4}\langle\psi|(I+U^\dagger)(I+U)|\psi\rangle$$

$(\langle\psi|U^\dagger|\psi\rangle)^*$
$= (\langle\psi|U^\dagger|\psi\rangle)^\dagger$
$= \langle\psi|U|\psi\rangle$

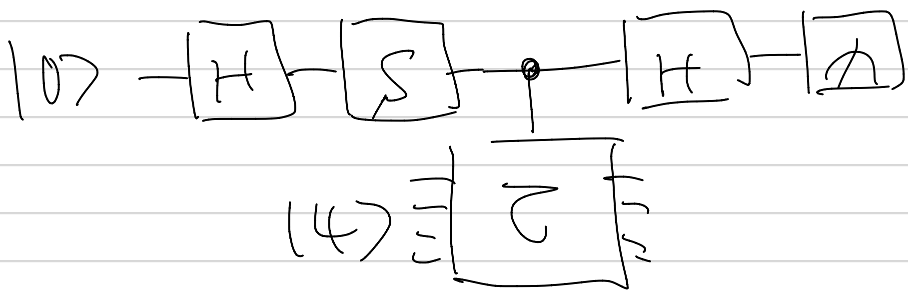
$$= \frac{1}{4}\Big(\langle\psi|\psi\rangle + \langle\psi|U^\dagger|\psi\rangle + \langle\psi|U|\psi\rangle + \langle\psi|\psi\rangle\Big)$$

$$= \frac{1 + \mathrm{Re}\left[\langle\psi|U|\psi\rangle\right]}{2}$$

同様に　$p_1 = \dfrac{1 - \mathrm{Re}[\langle\psi|U|\psi\rangle]}{2}$

→ 何回もくり返すことで、$\mathrm{Re}\langle\psi|U|\psi\rangle$ を計算できる。

$\mathrm{Im}\langle\psi|U|\psi\rangle$ は、



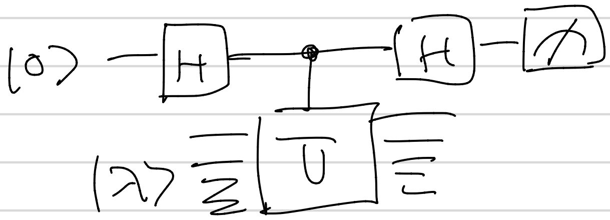
→ 行列要素 $\langle\psi|U|\psi\rangle$ が得られる。

一般に古典では指数時間かかる。

誤差 ε に対して $\mathrm{poly}(1/\varepsilon)$ のリソースで。

○ 固有値の計算、

$U|\lambda\rangle = e^{i2\pi\lambda}|\lambda\rangle$ とする。



$\langle\lambda|U|\lambda\rangle = e^{i2\pi\lambda}$

Hadamard testで固有値 $e^{i2\pi\lambda}$ がわかる。

($e^{-iHt}|E\rangle = e^{-iEt}|E\rangle$ でエネルギー固有状態、エネルギーがわかる。)

$e^{i2\pi\lambda}$ の推定だと λ を高い精度(低い桁まで)で求められない → もっと賢いアルゴリズムが必要。

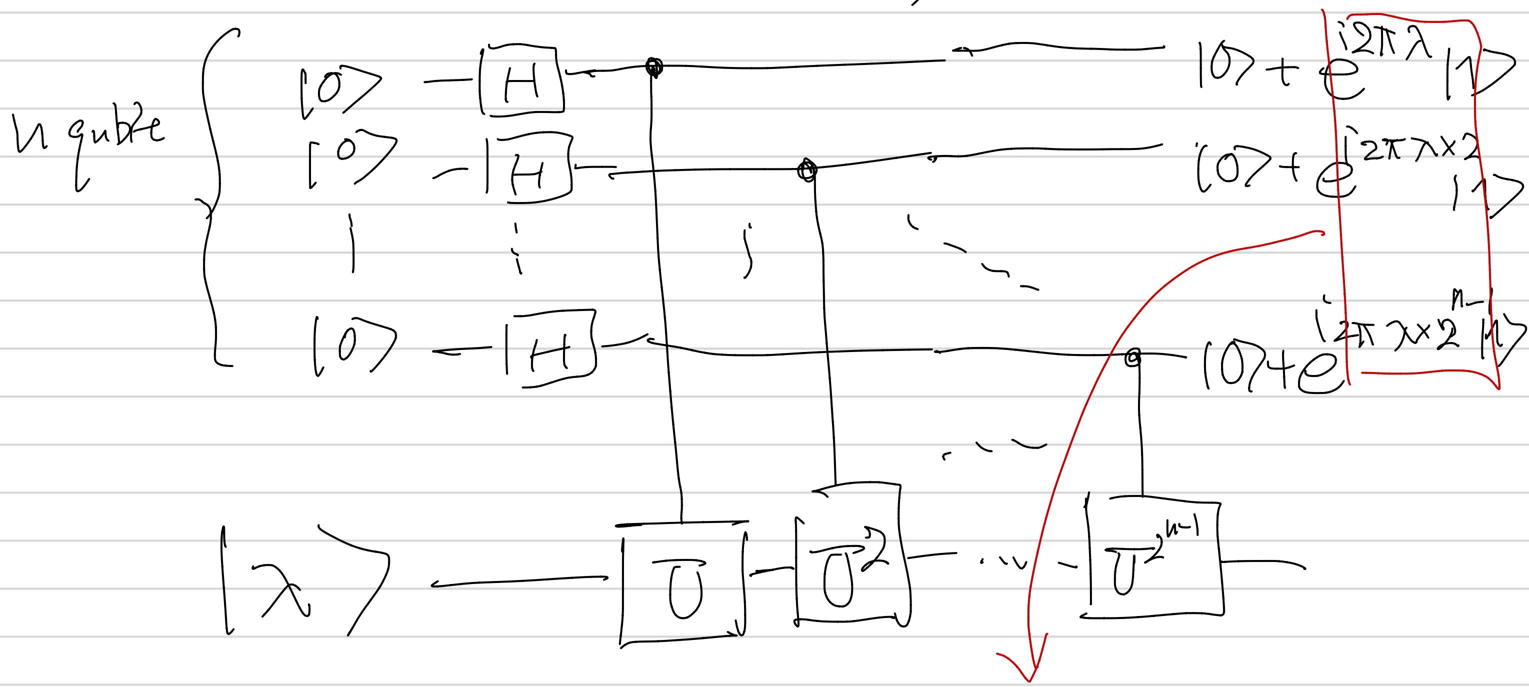
・Kitaevの位相推定。

→ λを　n桁まで求める。

$$\lambda = 0.j_1 j_2 \cdots j_n \quad \left(\lambda = \sum_{k=1}^{n} \left(\frac{1}{2}\right)^k j_k\right)$$

2進数の少数。　$j_k \in \{0, 1\}$

(例1　$0.1 = \frac{1}{2}$, $0.01 = \frac{1}{4}$, $0.101 = \frac{1}{2} + \frac{1}{8}$)



$$\lambda \times 2^k = \underbrace{j_1 j_2 \cdots j_k}_{\text{整数}} . j_{k+1} \cdots j_n$$

$2\pi\lambda 2^k$では

2πの整数倍として寄与

・量子フーリエ変換

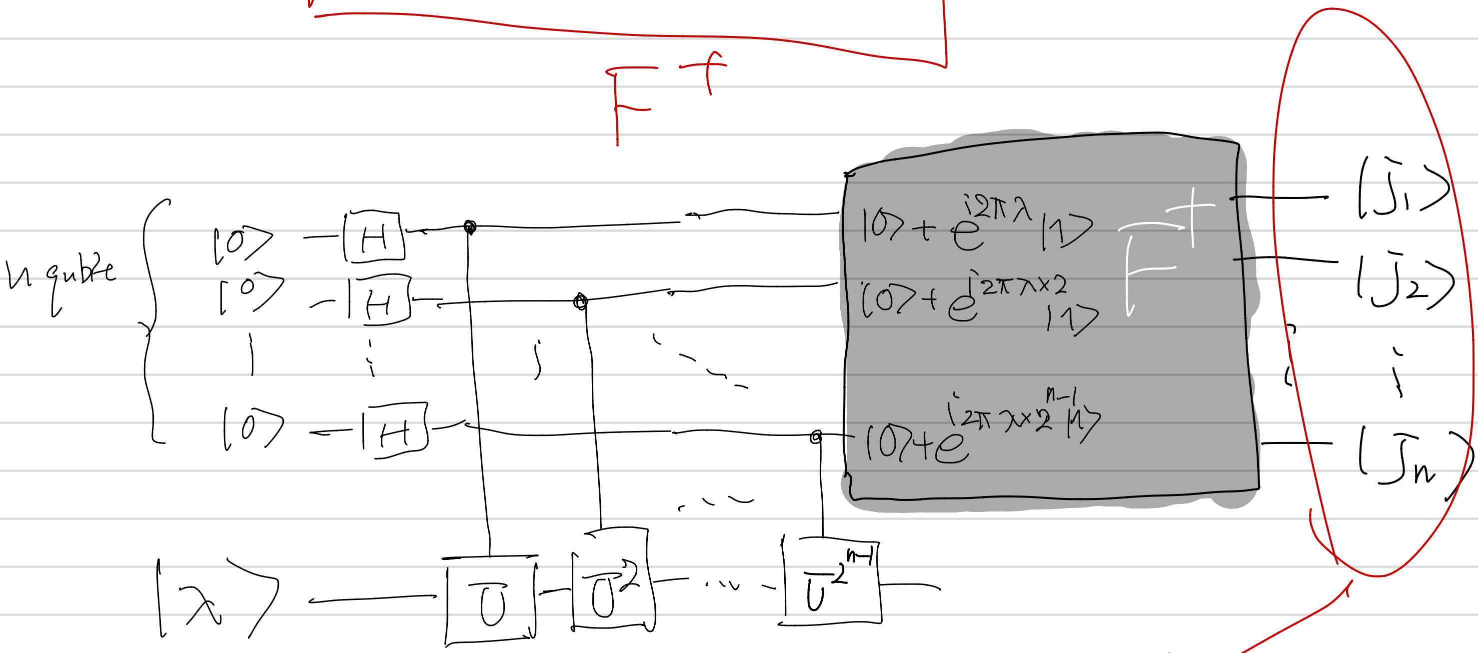
$x, y = 0, 1, \dots, N-1$ とする。

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

↓ 2進数で書き直すと。 (次のページで計算)

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

$F^\dagger$



n桁まで位相が求まった。

（補：量子フーリエ変換の2進数化）

$$N \equiv 2^n$$

$$F|y\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i \frac{x \cdot y}{N}} |x\rangle$$

$$x = \sum_{k=1}^{n} 2^k \tilde{x}_k, \quad y = \sum_{l=1}^{n} 2^l \tilde{y}_l$$

$$= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i \sum_{k,l} \frac{2^k \cdot 2^l \cdot \tilde{x}_k \tilde{y}_l}{2^n}} |\tilde{x}_1 \tilde{x}_2 \cdots \tilde{x}_n\rangle$$

$$= \frac{1}{\sqrt{N}} \underbrace{\sum_{\{\tilde{x}_i\}}} e^{2\pi i \sum_{k,l} 2^k \boxed{\frac{2^l}{2^n} \tilde{y}_l} \tilde{x}_k} |\tilde{x}_1 \tilde{x}_2 \cdots \tilde{x}_n\rangle$$

2進少数の定ぎ

↳すべての $\tilde{x}_1 \cdots \tilde{x}_n$ のビット列での和.

$$= \frac{1}{\sqrt{N}} \bigotimes_k \underbrace{\left(|0\rangle + e^{2\pi i \cdot 2^k 0.\tilde{y}_1 \tilde{y}_2 \cdots \tilde{y}_n} |1\rangle\right)}$$

すべてのビット列の和

（要素への和）

Σテンソル積にした.

2進少数の桁がくり上がる

○素因数分解（Shor）

→ ある特殊な U の固有値を求める

N を素因数分解したいとする。
互いに素な x を選ぶ

$$U_x : |y\rangle \longrightarrow |x \cdot y \bmod N\rangle$$

$y \in \{0, \cdots, N-1\}$

実は、

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

s：固有値のラベル。 $\exp\left[\frac{2\pi i s}{r}\right]$：固有値。

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

r：位数 $x^r \equiv 1 \pmod N$

Kitaev の位相推定より $\frac{s}{r}$ が求まる。

$$x^r \equiv 1 \pmod N$$

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

これらとNの最大公倍数が因数.

(例) $N=143$, $x=7$

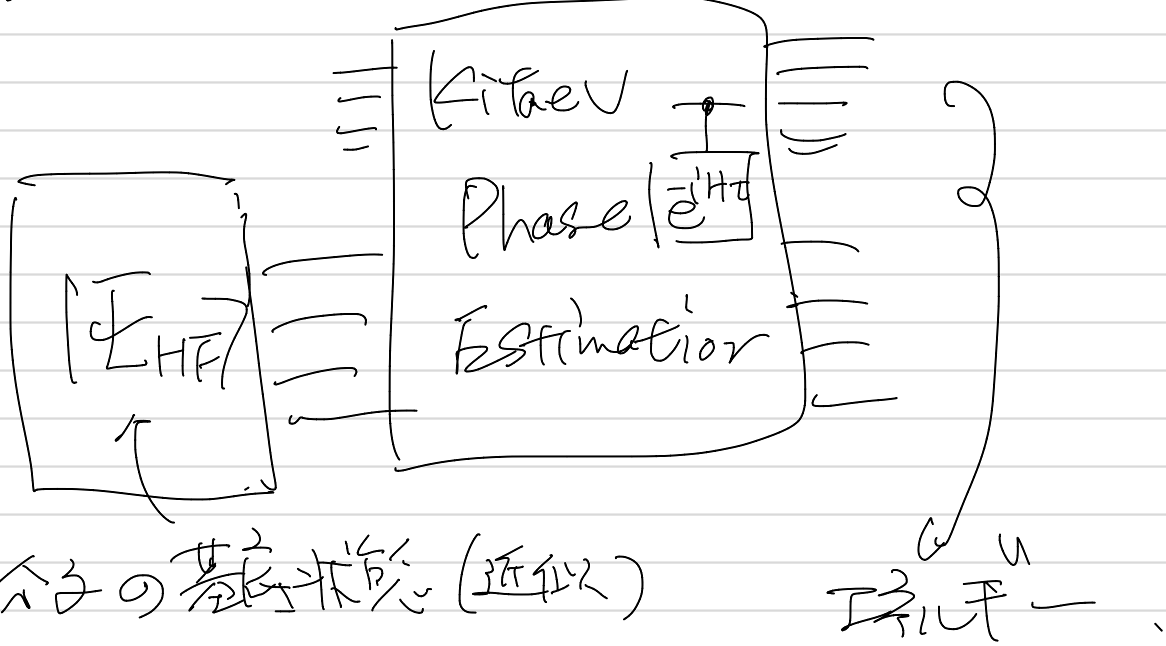
$7^1 \equiv 7$
$7^2 \equiv 49$
$7^3 \equiv 57$
$7^4 \equiv 113$
$7^5 \equiv 76$
$7^6 \equiv 103$
$7^7 \equiv 6$
$7^8 \equiv 42$
$7^9 \equiv 8$
$7^{10} \equiv 56$
$7^{11} \equiv 106$
$7^{12} \equiv 27$
$7^{13} \equiv 46$
$7^{14} \equiv 36$
$7^{15} \equiv 109$
$7^{16} \equiv 48$
$7^{17} \equiv 50$
$7^{18} \equiv 64$
$7^{19} \equiv 19$
$7^{20} \equiv 133$
$7^{21} \equiv 73$
$7^{22} \equiv 82$
$7^{23} \equiv 2$
$7^{24} \equiv 14$
$7^{25} \equiv 98$
$7^{26} \equiv 114$
$7^{27} \equiv 83$
$7^{28} \equiv 9$
$7^{29} \equiv 63$
$7^{30} \equiv 12$
$7^{31} \equiv 84$
$7^{32} \equiv 16$
$7^{33} \equiv 112$
$7^{34} \equiv 69$
$7^{35} \equiv 54$
$7^{36} \equiv 92$
$7^{37} \equiv 72$
$7^{38} \equiv 75$
$7^{39} \equiv 96$
$7^{40} \equiv 100$
$7^{41} \equiv 128$
$7^{42} \equiv 38$
$7^{43} \equiv 123$
$7^{44} \equiv 3$
$7^{45} \equiv 21$
$7^{46} \equiv 4$
$7^{47} \equiv 28$
$7^{48} \equiv 53$
$7^{49} \equiv 85$
$7^{50} \equiv 23$
$7^{51} \equiv 18$
$7^{52} \equiv 126$
$7^{53} \equiv 24$
$7^{54} \equiv 25$
$7^{55} \equiv 32$
$7^{56} \equiv 81$
$7^{57} \equiv 138$
$7^{58} \equiv 108$
$7^{59} \equiv 41$
$7^{60} \equiv 1$

$7^{30}-1 = 11$

$7^{30}+1 = 13$

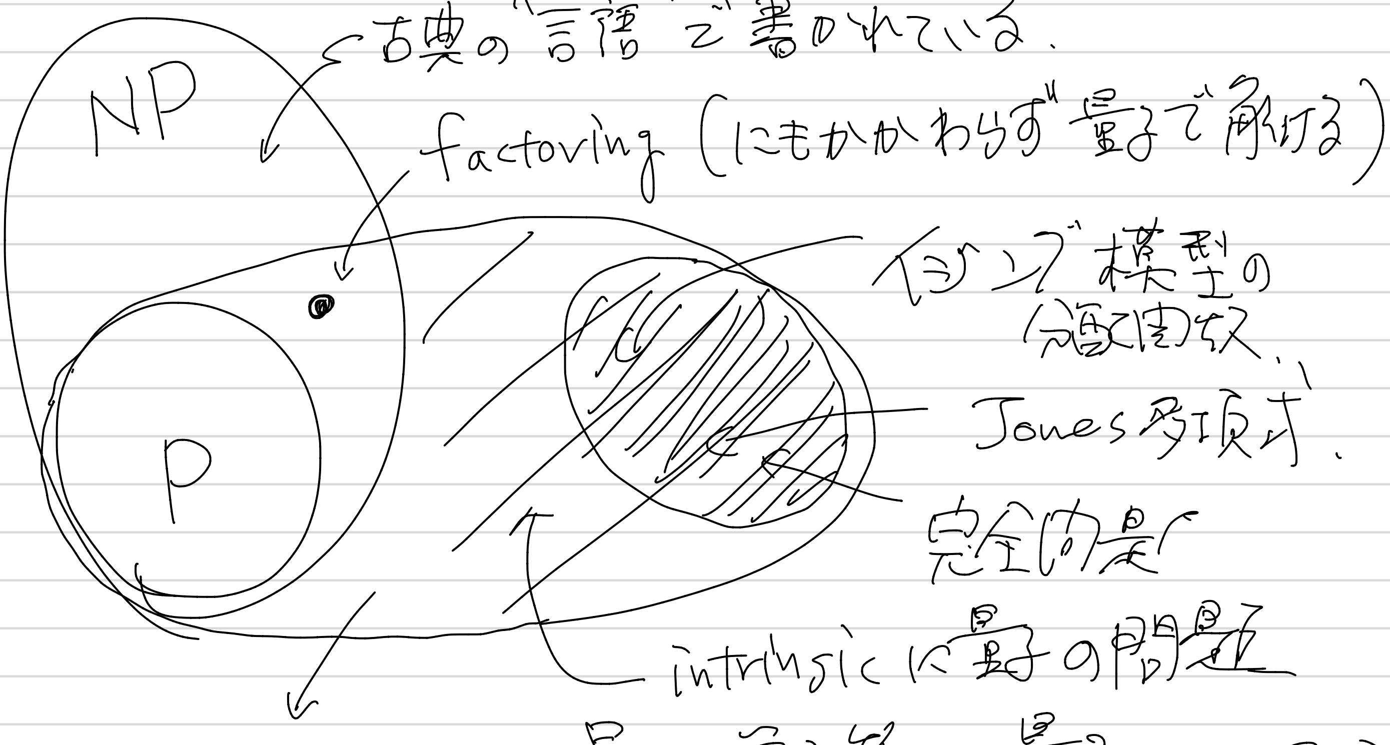
$11 \times 13 = 143$

○量子化学計算、



Aspuru-Guzik Science 2005

問題が、intrinsic に量子で記述



量子化学計算，量子シミュレーション.