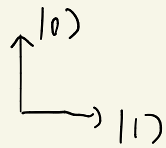
量子計算大学院こうぎ

森前 智行 （京大基研）

状態ベクトル



$$|0\rangle \equiv \begin{pmatrix}1\\0\end{pmatrix}$$

$$|1\rangle \equiv \begin{pmatrix}0\\1\end{pmatrix}$$

$|\ \rangle$ ケット

$\langle\ |$ ブラ

$\langle\ \ \rangle$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha, \beta \in \mathbb{C}$$

$$|\alpha|^2 + |\beta|^2 = 1$$

$$\langle\psi|\psi\rangle = (\alpha^* \underset{(1,0)}{\underset{\uparrow}{\langle 0|}}\ \ \beta^*\langle 1|)(\alpha|0\rangle + \beta|1\rangle)$$

$$= \alpha^*\alpha \underbrace{\langle 0|0\rangle}_{1} + \alpha^*\beta \underset{0}{\underset{\uparrow}{\langle 0|1\rangle}} + \beta^*\alpha \underset{0}{\underset{\uparrow}{\langle 1|0\rangle}} + \beta^*\beta \underset{1}{\underset{\uparrow}{\langle 1|1\rangle}}$$

$$= |\alpha|^2 + |\beta|^2$$

$$\langle 0|1\rangle = (1, 0)\begin{pmatrix}0\\1\end{pmatrix} = 0$$

そくてい $\{P_i\}_{i=1}^{m}$ $\quad P_i^2 = P_i \quad \sum_{i=1}^{m} P_i = I$

$$\mathrm{Prob}(i) = \langle \psi | P_i | \psi \rangle = \langle \psi | P_i \cdot P_i | \psi \rangle$$

$$\frac{P_i | \psi \rangle}{\sqrt{\langle \psi | P_i | \psi \rangle}}$$

POVM そくてい $\{\Pi_i\}_{i=1}^{m}$ $\quad \Pi_i \geq 0 \quad \sum_{i=1}^{m} \Pi_i = I$

$$\mathrm{Prob}(i) = \langle \psi | \Pi_i | \psi \rangle$$

混合状態

$$\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i| \qquad \lambda_i \geq 0 \qquad \sum_i \lambda_i = 1$$

$$\mathrm{Tr}(P_i \rho) \qquad\qquad \mathrm{Tr}\, A = \sum_i \langle i | A | i \rangle$$

$$\mathrm{Tr}(\Pi_i \rho)$$

maximally mixed state $\quad \dfrac{I}{2} = \dfrac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2}$

ユニタリ

$$U^\dagger U = I$$

$$U|\psi\rangle = |\psi'\rangle \qquad U = e^{iHt}$$

$$U\rho U^\dagger = \rho'$$

エルミート共役

$A^\dagger$ てんち

復素共役

Pauli operator (gate)

$$I \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\sigma_x \quad X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_y \quad Y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_z \quad Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$X^2 = Y^2 = Z^2 = I$$

$$X^\dagger = X, \quad Y^\dagger = Y, \quad Z^\dagger = Z$$

$$XY = iZ \qquad XY = -YX$$

$$XZ = Y \qquad XZ = -ZX$$

$$YZ = X \qquad YZ = -ZY$$

$$Z|0\rangle = |0\rangle$$

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

$$X|0\rangle = |1\rangle$$

$$X|1\rangle = |0\rangle$$

$$Y|0\rangle = i|1\rangle$$

$$Y|1\rangle = -i|0\rangle$$

$$|+\rangle \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|-\rangle \equiv \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$X|+\rangle = |+\rangle \qquad Z|+\rangle = |-\rangle$$

$$X|-\rangle = -|-\rangle \qquad Z|-\rangle = |+\rangle$$

Clifford operator (gate)

$$H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ Hadamard アダマール $H^\dagger = H$

$$S \equiv \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = Z^{\frac{1}{2}} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix}$$

(P)

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$H|0\rangle = |+\rangle$ $H|+\rangle = |0\rangle$

$H|1\rangle = |-\rangle$ $H|-\rangle = |1\rangle$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

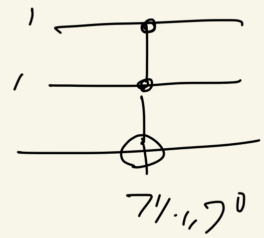
$$= |+\rangle$$

$HXH = Z$ $SXS^\dagger = Y$

$HZH = X$ $SYS^\dagger = -X$

$HYH = -Y$ $SZS^\dagger = Z$

H + トフォリ



non-Clifford

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

$$T X T^{\dagger} = \frac{X+Y}{\sqrt{2}} = e^{-i\frac{\pi}{4}} S X$$

Clifford のみ ← 古典シミュレート可 (Gottesman-Knill)

+

any non-Clifford

||

universal (任意の n-qubit ユニタリが可)

Solvay-Kitaev

$|\psi\rangle \otimes |\phi\rangle$

↑

テンソル積

$$(U_1 \otimes U_2)(|\psi\rangle \otimes |\phi\rangle)$$

$$= U_1|\psi\rangle \otimes U_2|\phi\rangle$$

$$(U_1 \otimes I)(|\psi\rangle \otimes |\phi\rangle)$$

$$= U_1|\psi\rangle \otimes |\phi\rangle$$

$|\psi_1\rangle \otimes |\phi_1\rangle$

と

$|\psi_2\rangle \otimes |\phi_2\rangle$

の内積

$$(\langle\psi_1| \otimes \langle\phi_1|)(|\psi_2\rangle \otimes |\phi_2\rangle)$$

$$= \langle\psi_1|\psi_2\rangle \langle\phi_1|\phi_2\rangle$$

$|0\rangle^{\otimes n}$ $\qquad \bigotimes_{i=1}^{n} |\psi_i\rangle$

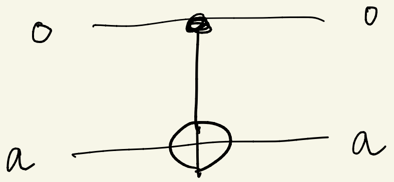
Entanglement

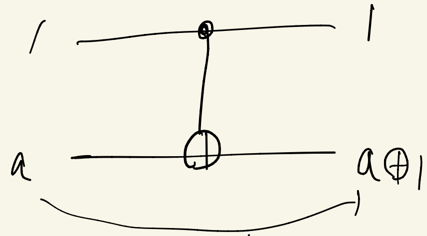
2-qubit $\quad 2^2$-dim

product state

$$\underline{\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)} \neq |\psi\rangle \otimes |\phi\rangle$$

CNOT

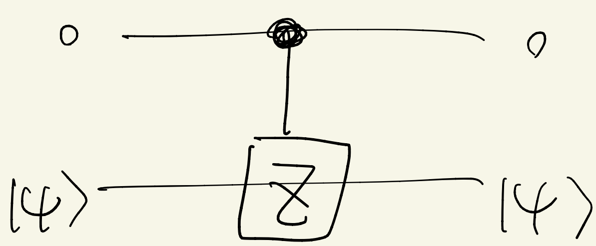


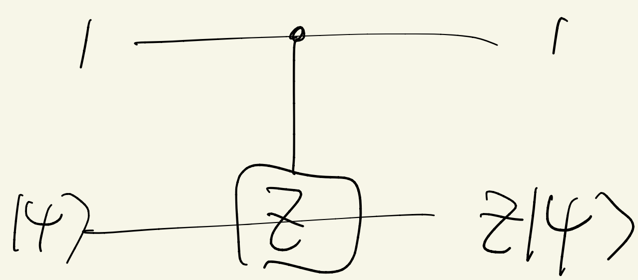


$$\mathrm{CNOT}\,|0\rangle\otimes|0\rangle = |0\rangle\otimes|0\rangle$$
$$|0\rangle\otimes|1\rangle = |0\rangle\otimes|1\rangle$$
$$|1\rangle\otimes|0\rangle = |1\rangle\otimes|1\rangle$$
$$|1\rangle\otimes|1\rangle = |1\rangle\otimes|0\rangle$$

つまり $\mathrm{CNOT} = |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes X$

CZ

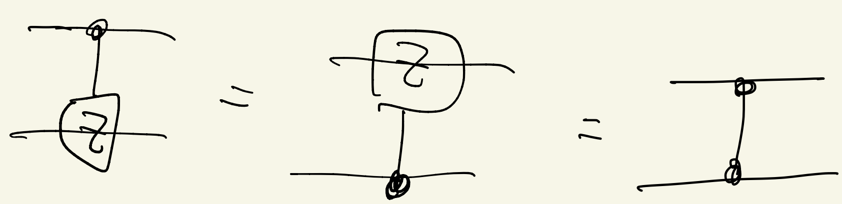




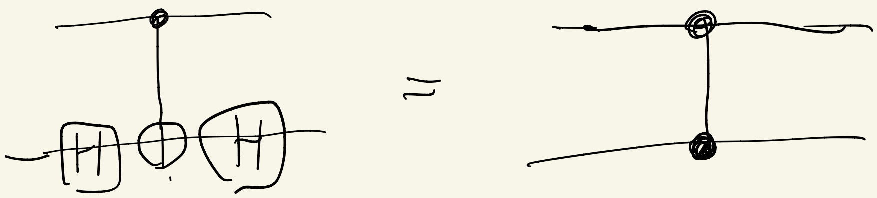
$$CZ\,|00\rangle = |00\rangle$$
$$CZ\,|01\rangle = |01\rangle$$
$$CZ\,|10\rangle = |10\rangle$$
$$CZ\,|11\rangle = -|11\rangle$$

$$CZ = |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes Z$$

$$CZ = I - 2|11\rangle\langle 11|$$



CZ



CNOT, CZ .. clifford. $CZ^{\dagger} = CZ$

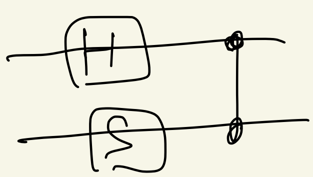
$$CZ(Z \otimes Z)CZ = Z \otimes Z$$

$$CZ(X \otimes I)CZ = (X \otimes Z)$$

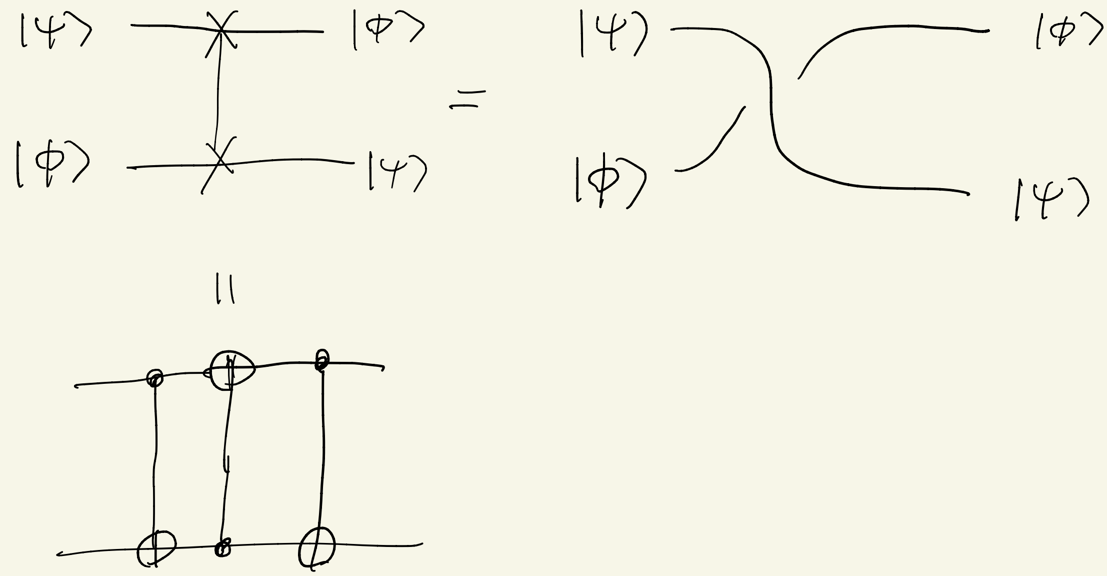
H, S, CZ.

T

+

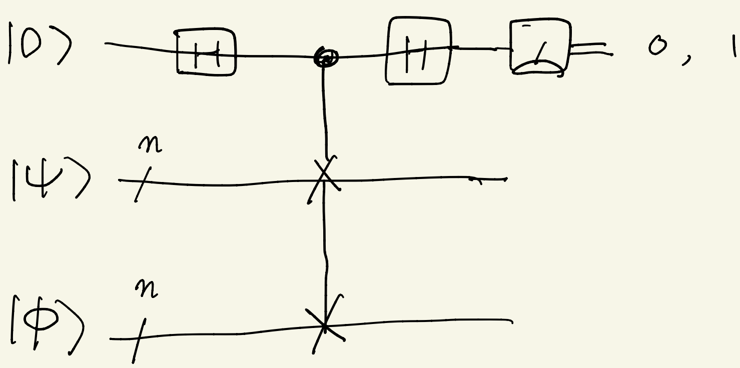


SWAP



SWAP test

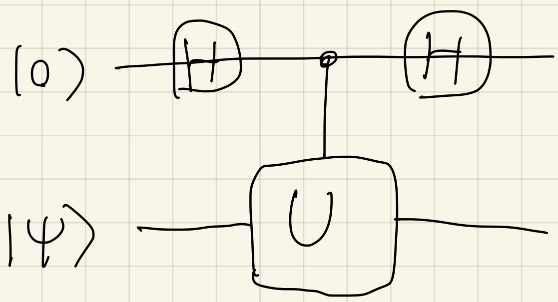
$\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$



$$P_0 = \frac{1 + |\langle\psi|\phi\rangle|^2}{2}$$

$$\langle\psi|\phi\rangle = \begin{cases} 0 & \text{直交} \\ 1 & \text{同じ} \end{cases}$$

Hadamard test



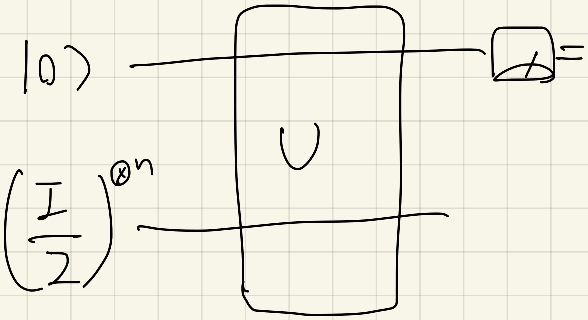
$$\frac{1}{\sqrt{2}}\left(|0\rangle \otimes |\psi\rangle + |1\rangle|\psi\rangle\right) \longrightarrow \frac{1}{\sqrt{2}}\left(|0\rangle|\psi\rangle + |1\rangle U|\psi\rangle\right)$$

$$\longrightarrow \frac{1}{\sqrt{2}}\left[\langle +|0\rangle|\psi\rangle + \langle +|1\rangle U|\psi\rangle\right]$$

$$P_0 = \frac{2 + \langle\psi|U|\psi\rangle + \langle\psi|U^\dagger|\psi\rangle}{4}$$

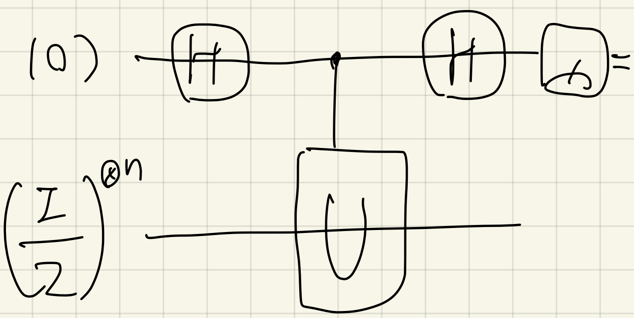
$$= \frac{1 + \langle\psi|U|\psi\rangle}{2}$$

one-clean-qubit model (Knill-Laflamme PRL 1998)



量子スプレマシー

(TM et al. PRL 2014)



$$\left(\frac{I}{2}\right)^{\otimes n} = \frac{1}{2^n}\sum_z |z\rangle\langle z|$$

$$P_0 = \frac{1 + \langle\psi|U|\psi\rangle}{2}$$

$$= \frac{1 + \frac{\mathrm{Tr}(U)}{2^n}}{2}$$

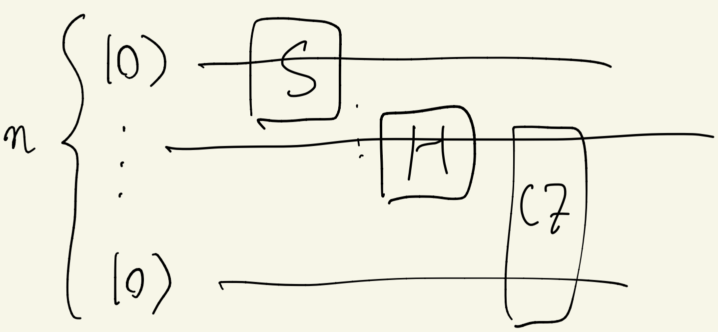
Pauli　X, Y, Z, I.

Clifford　H, S, CZ

non-Clifford　T

Gottesman-Knill 定理

Clifford gate のみの量子回路は
古典で poly(n)-time でシミュレート可

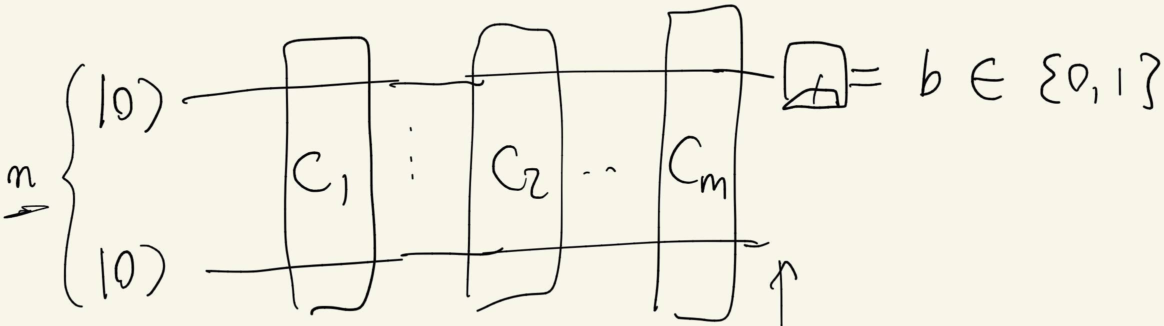


Clifford のみで
$|0\cdots0\rangle + |1\cdots1\rangle$
もつくれる！

$\Rightarrow$ 量子性が大

$\not\Downarrow$

量子高速性



$$C_m \cdots C_2 C_1 |0^n\rangle$$

$$P_0 = \langle 0^n | C_1^\dagger \cdots C_m^\dagger \left(\underbrace{|0\rangle\langle 0|}_{= \frac{I+Z}{2}} \otimes I^{\otimes n-1} \right) C_m \cdots C_1 |0^n\rangle$$

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

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

$$P_0 = \langle 0^n | C_1^\dagger \cdots C_m^\dagger \left(\frac{I+Z}{2} \otimes I^{\otimes n-1} \right) C_m \cdots C_1 |0^n\rangle$$

$$= \frac{1}{2} \langle 0^n | C_1^\dagger \cdots C_m^\dagger \left(I \otimes I^{\otimes n-1} \right) C_m \cdots C_1 |0^n\rangle$$

$$+ \frac{1}{2} \langle 0^n | C_1^\dagger \cdots C_m^\dagger \left(Z \otimes I^{\otimes n-1} \right) C_m \cdots C_1 | 0^n \rangle$$

$$= \frac{1}{2} \underbrace{\langle 0^n | 0^n \rangle}_{1}$$

$$+ \frac{1}{2} \langle 0^n | C_1^\dagger \cdots C_{m-1}^\dagger \underbrace{C_m^\dagger \left(Z \otimes I^{n-1} \right) C_m}_{\downarrow} C_{m-1} \cdots C_1 | 0^n \rangle$$

$$\underbrace{C_{m-1} \; \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n \; C_{m-1}}_{\downarrow}$$

$$\sigma_1' \otimes \cdots \otimes \sigma_m' + \sigma \otimes \cdots \otimes \sigma$$

$$\vdots$$

$$= \frac{1}{2} + \left.\begin{aligned} & \frac{1}{2} \langle 0^n | \sigma_1 \otimes \cdots \otimes \sigma_n | 0^n \rangle \\ & + \frac{1}{2} \langle 0^n | \sigma \otimes \cdots \otimes \sigma | 0^n \rangle \\ & + \\ & \vdots \\ & + \frac{1}{2} \langle 0^n | \sigma \otimes \cdots \otimes \sigma | 0^n \rangle \end{aligned}\right\} \text{poly}$$

T-gate が log 個でも可

$$T^\dagger X T = \frac{X+Y}{\sqrt{2}}$$

$$T^\dagger Y T = \frac{X-Y}{\sqrt{2}}$$

$$T^\dagger Z T = Z$$

古典でシミュレートできる量子回路

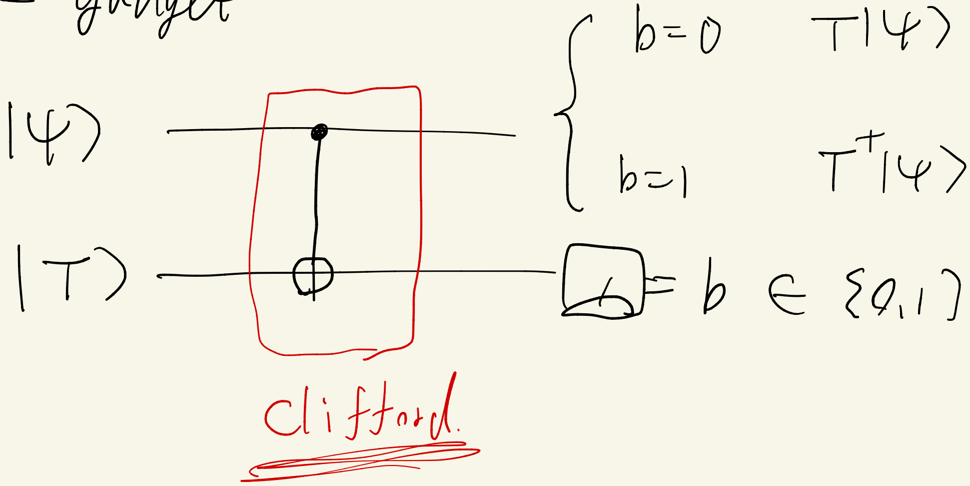
Gottesman-Knill　　クリフォード回路.

match gate → free Fermion.

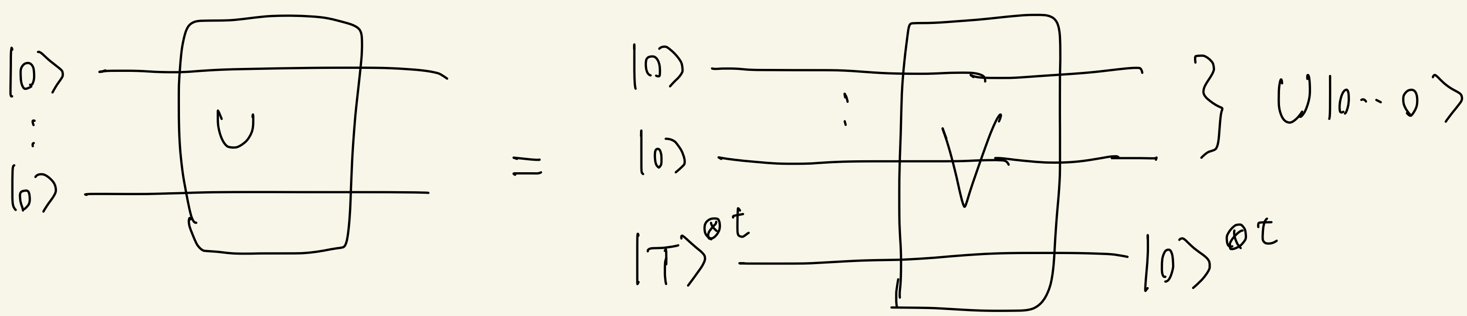
magic state

$$|T\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{\pi}{4}}|1\rangle\right)$$

T - gadget

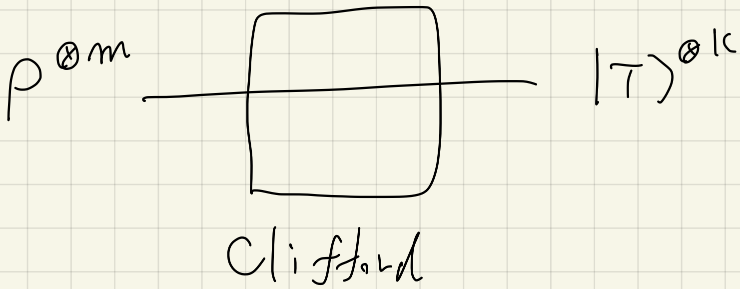


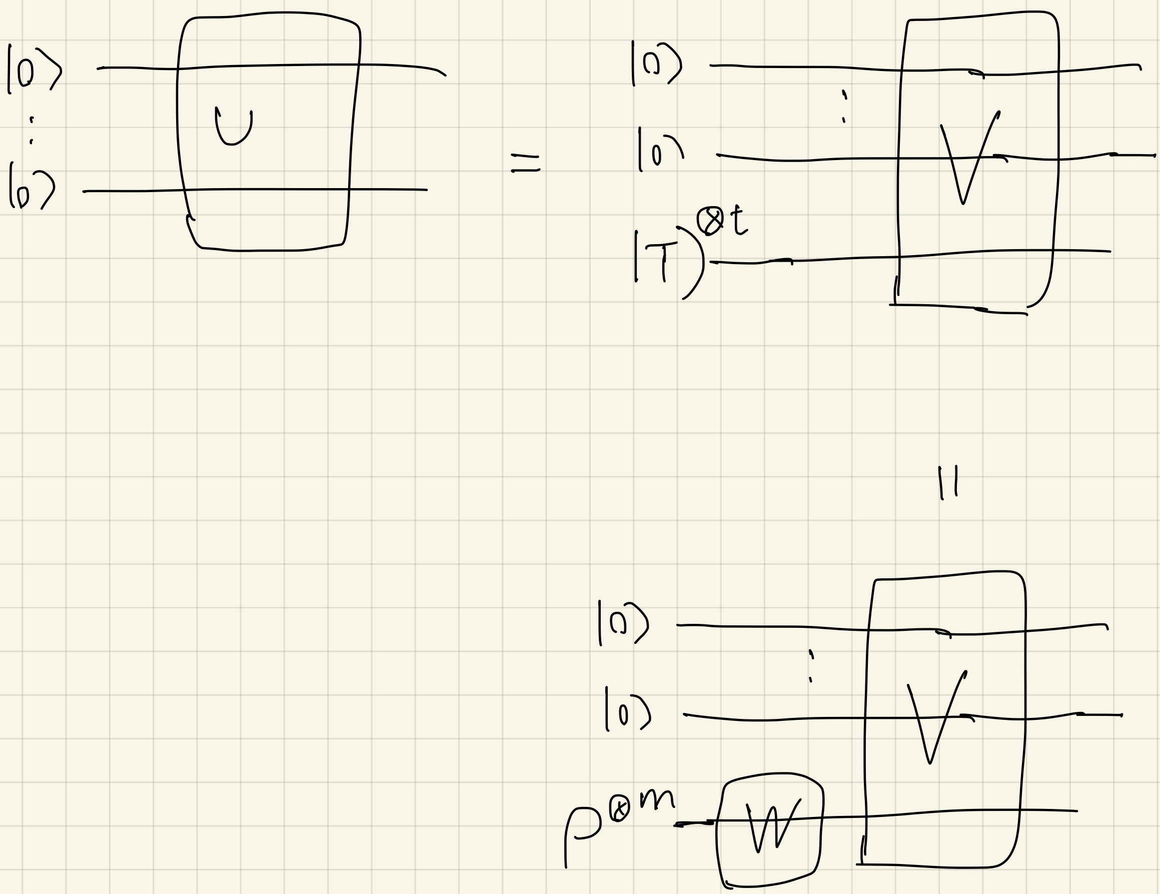
$$ST^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} = T$$



magic state distillation

$m \gg k$





Stabilizer rank

$\chi(|\psi\rangle)$ … $\min k$

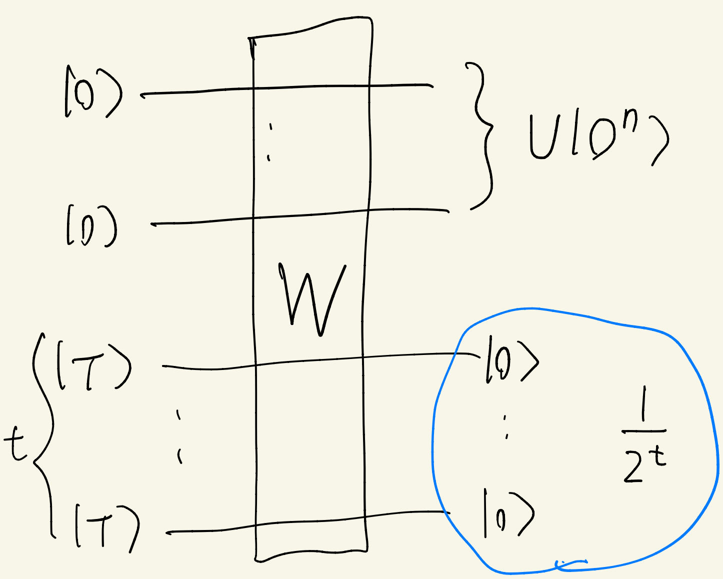
s.t. $|\psi\rangle = \sum_{i=1}^{k} c_i \, |\phi_i\rangle$ — stabilizer state $C|0\cdots0\rangle$

C ↑ クリフォード回路

c_i ↑ $c_i \in \mathbb{C}$

U … Clifford + t T

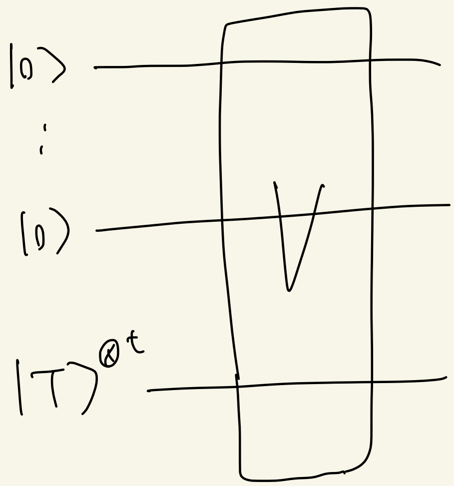
$$\langle 0^n | U | 0^n \rangle = \frac{1}{\sqrt{2^t}} \langle 0^{n+t} | \, W \left(|0^n\rangle \otimes |T\rangle^{\otimes t} \right)$$



$$= \frac{1}{\sqrt{2^t}} \sum_{i=1}^{\chi(|T\rangle^{\otimes t})} c_i \, \overbrace{\langle 0^{n+t} | W | 0^n \rangle |\phi_i\rangle}^{\text{poly}}$$

$|\phi_i\rangle$ ↑ stabilizer state

$\chi(|T\rangle^{\otimes t})$-time.



$\chi(|T\rangle^{\otimes t})$ - time

① trivial $\chi(|T\rangle^{\otimes t}) \leq 2^t$

$$|T\rangle^{\otimes t} = \left(|0\rangle + e^{i\frac{\pi}{4}}|1\rangle\right)^{\otimes t}$$

$$= \underline{|0\cdots0\rangle} + \underline{|0\cdots01\rangle} + \cdots + \underline{|1\cdots1\rangle}$$

2016

$$\chi(|T\rangle^{\otimes t}) \leq 2^{0.4t}$$

Bravyi - Gosset - Smolin

Morimae – Tamaki $\chi(|T\rangle^{\otimes t}) \geq 2^{\Omega(t)}$

Under ETH

ETH : solving 3SAT needs $2^{\Omega(m)}$ time.

m .. # of clauses

$(x_1 \vee \bar{x}_2 \vee x_3) \wedge (x_1 \vee x_6 \vee \bar{x}_7) \wedge \cdots \wedge (x_8 \vee \bar{x}_{16} \vee x_{20})$

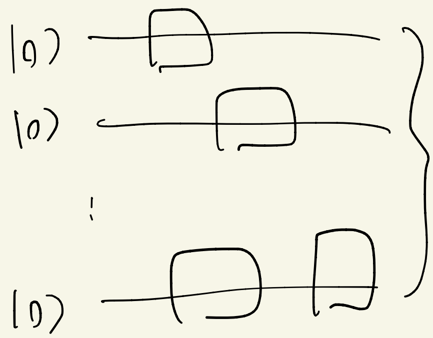
$NP \neq P$

Nielsen – Chuang 2000

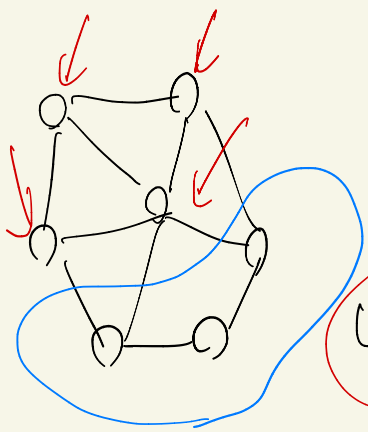
Q indistinguishability obfuscation

[Broadbent-Kazmi, arXiv: 2005.14699]

測定型量子計算



$U|0\cdots0\rangle$

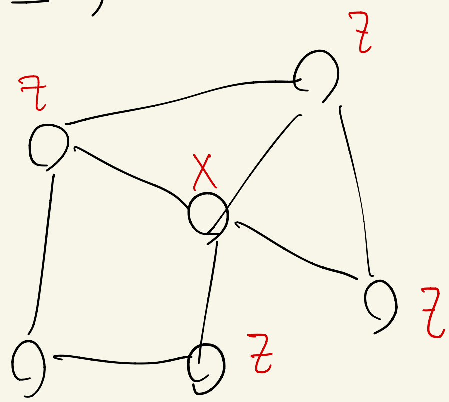


$U|0\cdots0\rangle$

Graph state $|G\rangle$

$G = (V, E)$

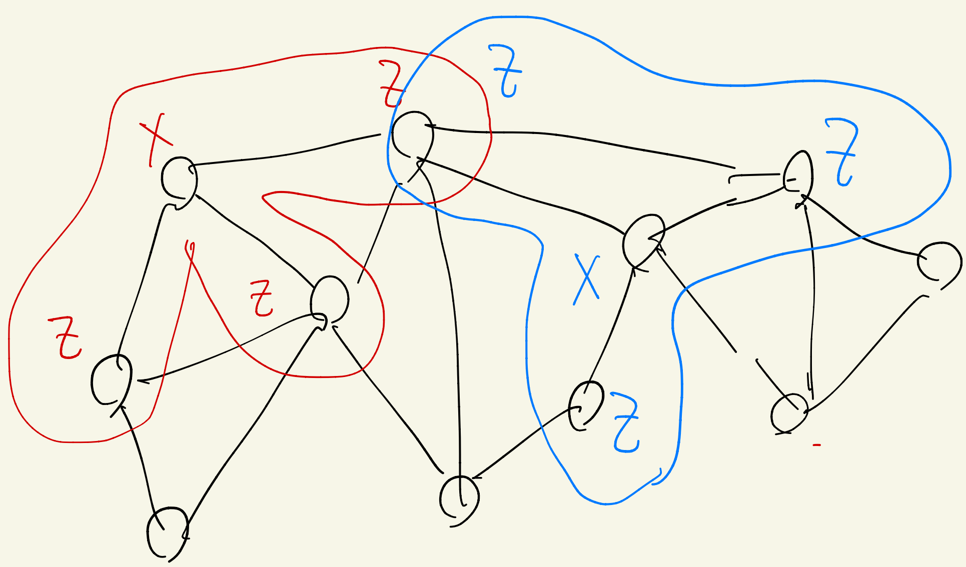
$|V| = N$



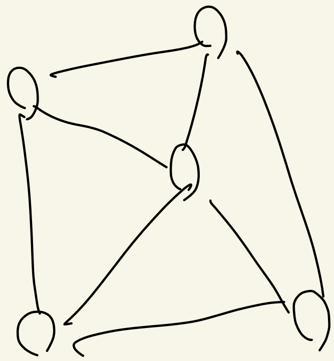
① $\{K_i\}_{i=1}^{N}$ $\quad \forall_i \; K_i |G\rangle = |G\rangle$

$$K_i \equiv X_i \otimes \bigotimes_{j \in N_i} Z_j$$

$i \neq j \quad [K_i, K_j] = 0$



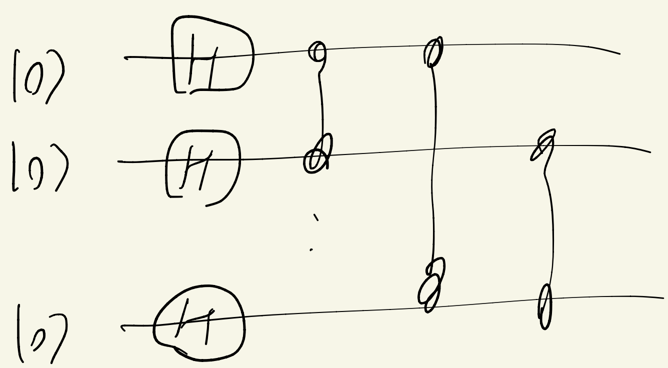
②



$$[CZ_{ij}, CZ_{kl}] = 0$$

$C|0\cdots0\rangle$

クリフォード



$$|G\rangle = \prod_{(i,j)\in E} CZ_{i,j} \; |+\rangle^{\otimes N}$$

$$K_\ell |G\rangle = |G\rangle$$

$$K_\ell |G\rangle = K_\ell \prod_{(i,j)\in E} CZ_{i,j} |+\rangle^{\otimes N}$$

$$CZ(Z\otimes I)CZ = Z\otimes I$$

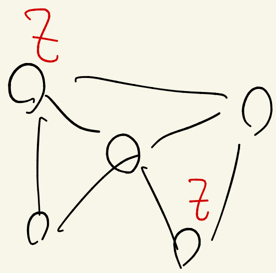
$$CZ(X\otimes I)CZ = X\otimes Z$$

$$= \prod_{(i,j)\in E} CZ_{i,j} \; X_\ell |+\rangle^{\otimes N}$$

$$= \prod_{(i,j)\in E} CZ_{i,j} |+\rangle^{\otimes N}$$

$$= |G\rangle$$

①
$$|G_\alpha\rangle \equiv \bigotimes_{j=1}^{N} Z_j^{\alpha_j} |G\rangle$$



$\alpha \in \{0,1\}^N$ $\qquad$ $\{|G_\alpha\rangle\}_{\alpha \in \{0,1\}^n}$

$$\langle G_\alpha | G_{\alpha'}\rangle = \delta_{\alpha\alpha'}$$

$$\langle G_\alpha | G_{\alpha'}\rangle = \langle G| \bigotimes_{j=1}^{N} Z_j^{\alpha_j} \bigotimes_{j=1}^{N} Z_j^{\alpha_j'} |G\rangle$$

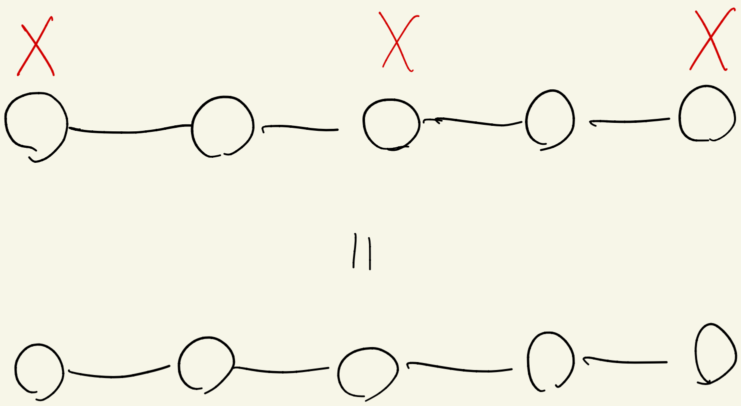
$$= \langle G| \underbrace{\bigotimes_{j=1}^{N} Z_j^{\alpha_j \oplus \alpha_j'}}_{\text{※}\ I} |G\rangle$$

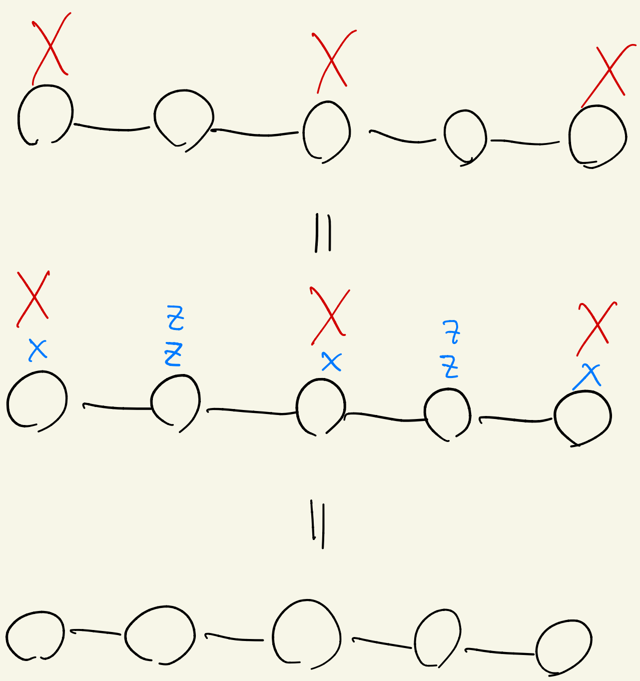
$$= \langle +|^{\otimes N} \prod_{e\in E} CZ_e \cdot \bigotimes_{j=1}^{N} Z_j^{\alpha_j \oplus \alpha_j'} \prod_{e\in E} CZ_e |+\rangle^{\otimes N}$$

$$= \langle +|^{\otimes N} \underbrace{\prod_{e\in E} CZ_e \cdot \prod_{e\in E} CZ_e}_{I} \bigotimes_{j=1}^{N} Z_j^{\alpha_j \oplus \alpha_j'} |+\rangle^{\otimes N}$$

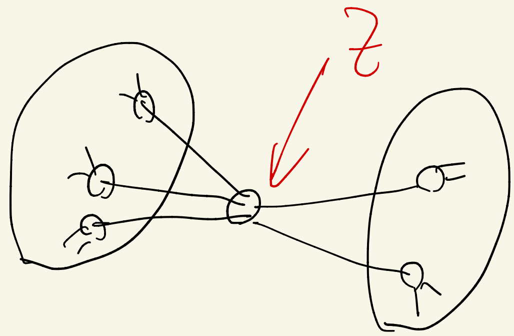
$$= \langle +|^{\otimes N} \bigotimes_{j=1}^{N} Z_j^{\alpha_j \oplus \alpha_j'} |+\rangle^{\otimes N} = \langle +|-\rangle \cdots$$

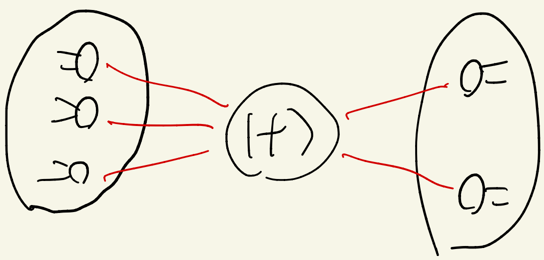
2



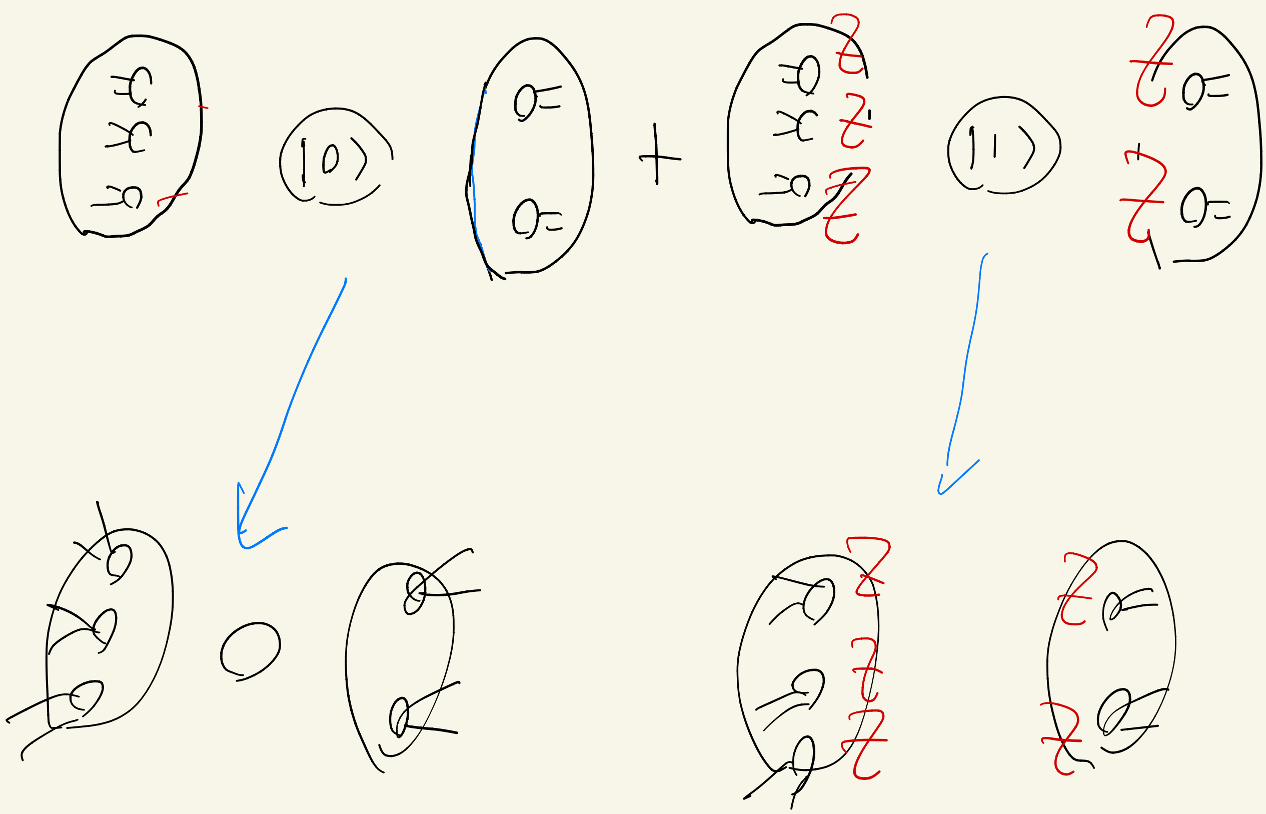


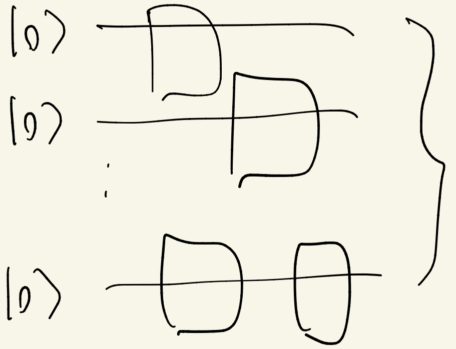
3



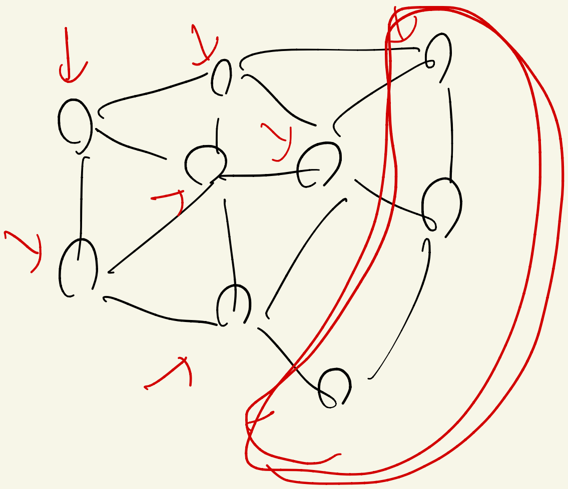


=





$U|0\cdots0\rangle$



$U|0\cdots0\rangle$

$$J(\theta) = H e^{i\theta Z}$$

$$J(0)\,J(\theta) = H \underbrace{e^{iZ0}}_{I} H e^{iZ\theta}$$

$$= H \cdot H e^{iZ\theta}$$

$$= e^{iZ\theta}$$

$$J(0)\,J(\theta)\,J(0) = H\, e^{i\theta Z}\, H$$

$$= e^{i\theta X}$$

$$\overbrace{|\psi\rangle \quad |+\rangle}^{CZ} \longrightarrow \left\{ \begin{array}{l} J(\theta)|\psi\rangle \\ XJ(\theta)|\psi\rangle \end{array} \right.$$

$$\uparrow$$

$$\{ |0\rangle \pm e^{i\theta}|1\rangle \}$$

$$CZ\left[(\alpha|0\rangle + \beta|1\rangle) \otimes |+\rangle\right]$$

$$= CZ\left[(\alpha|0\rangle + \beta|1\rangle) \otimes (|0\rangle + |1\rangle)\right]$$

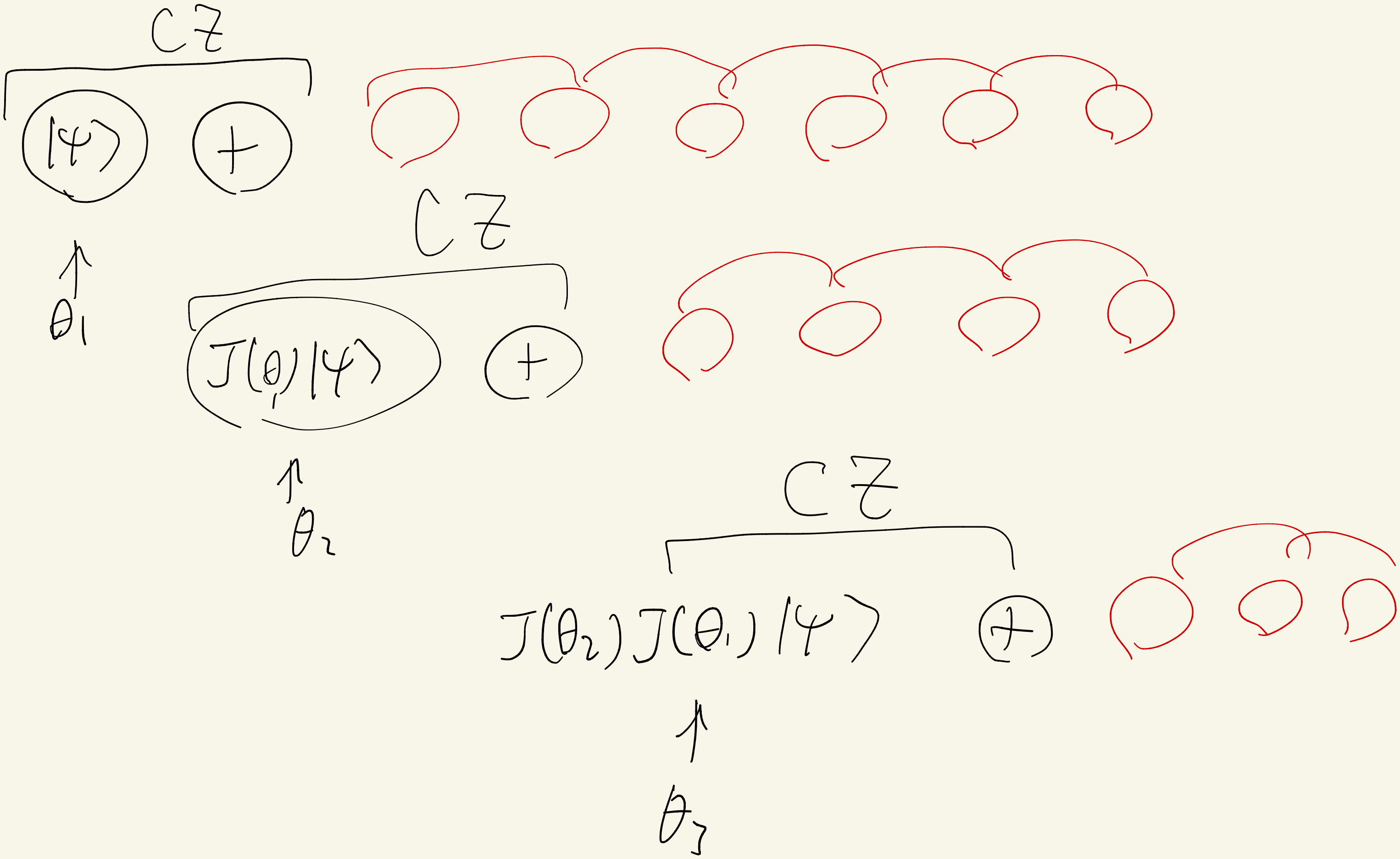
$$= CZ\left[\alpha|00\rangle + \alpha|01\rangle + \beta|10\rangle + \beta|11\rangle\right]$$

$$= \alpha|00\rangle + \alpha|01\rangle + \beta|10\rangle - \beta|11\rangle$$

$$\longrightarrow \alpha|0\rangle + \alpha|1\rangle + \beta e^{-i\theta}|0\rangle - \beta e^{-i\theta}|1\rangle$$

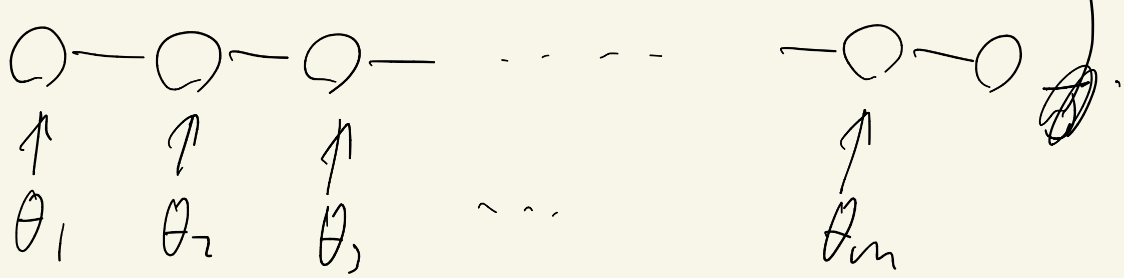
$$= \alpha|+\rangle + \beta e^{-i\theta}|-\rangle$$

$$= J(\theta)\,(\alpha|0\rangle + \beta|1\rangle)$$



$\vdots$

$$J(\theta_m)\cdots J(\theta_2)\,J(\theta_1)\,|\psi\rangle$$



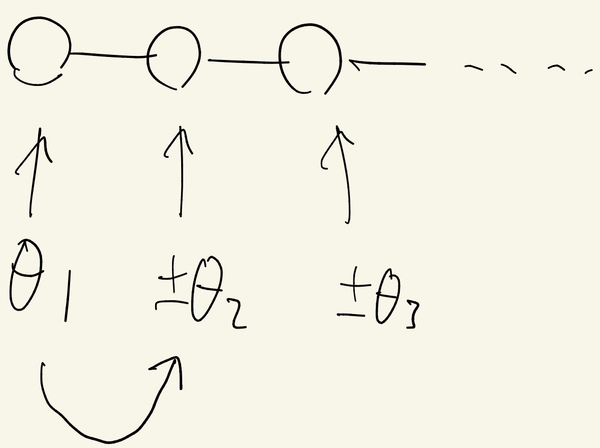
$$J(-\theta_2)\,X\,J(\theta_1)|\psi\rangle$$

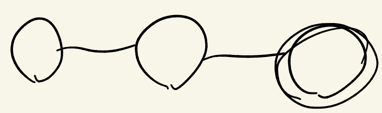
$$= H e^{-i\theta_2 Z}\; X \;H e^{i\theta_1 Z}\;|\psi\rangle$$

$$= H\; X\; e^{i\theta_2 Z}\; H e^{i\theta_1 Z}\;|\psi\rangle$$

$$= Z\; \underbrace{H e^{i\theta_2 Z}}\; \underbrace{H e^{i\theta_1 Z}}\; |\psi\rangle$$

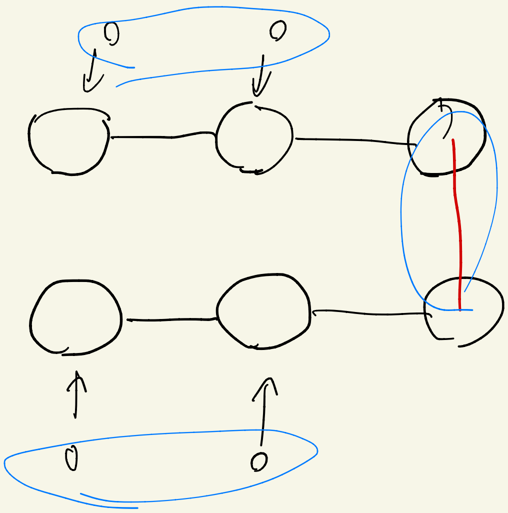
$$= Z\; \underbrace{J(\theta_2)\quad J(\theta_1)\quad |\psi\rangle}$$





$$\square\; J(\theta_m)\cdots J(\theta_1)|\psi\rangle$$

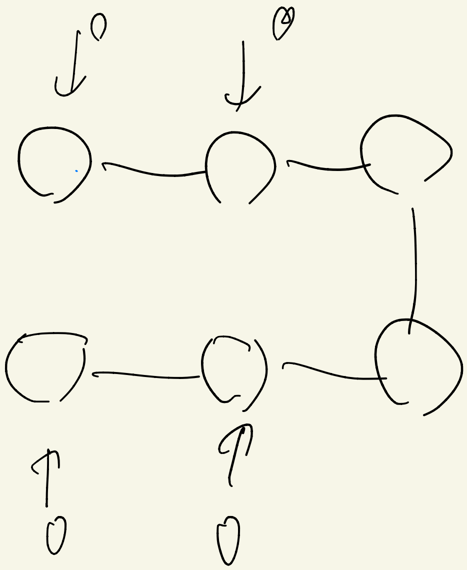
Pauli byproduct



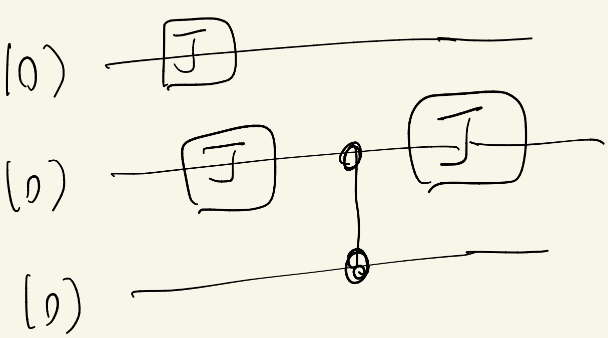
$J(0)J(0)|\psi_1\rangle = |\psi_1\rangle$

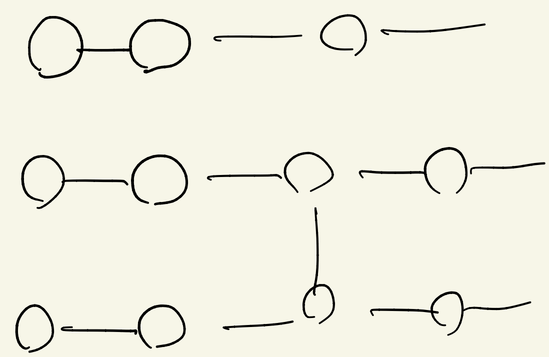
$CZ(|\psi_1\rangle \otimes |\psi_2\rangle)$

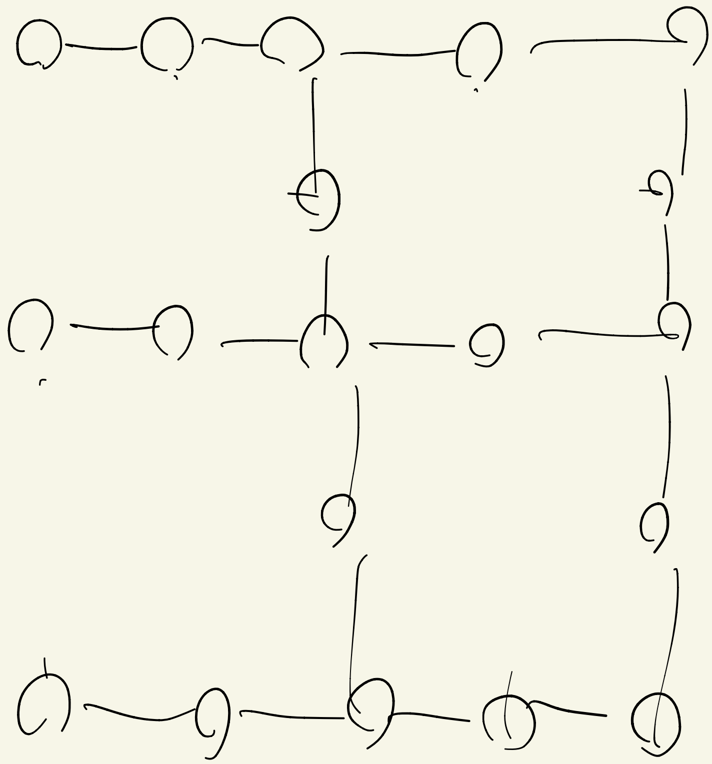
$J(0)J(0)|\psi_2\rangle = |\psi_2\rangle$

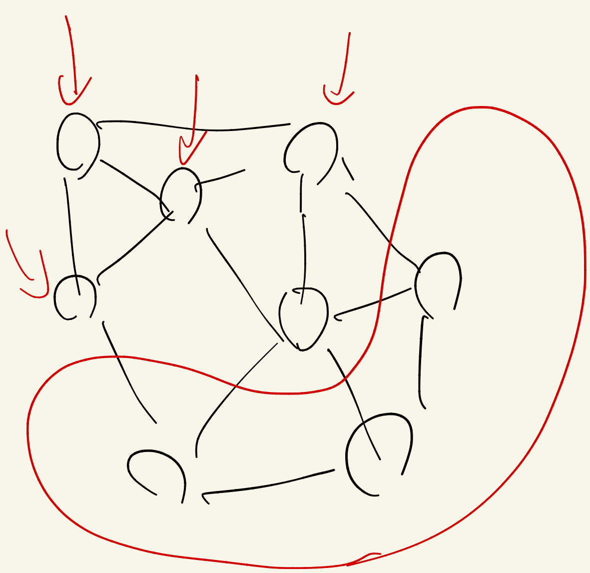


CZ ができる

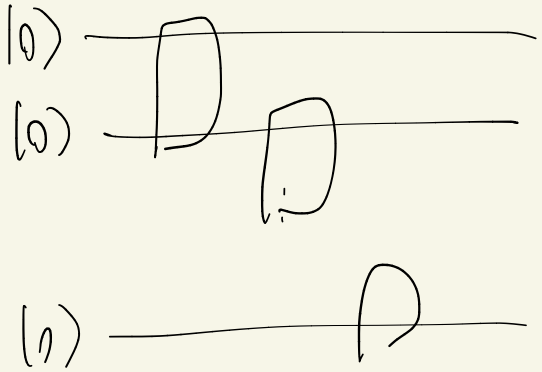


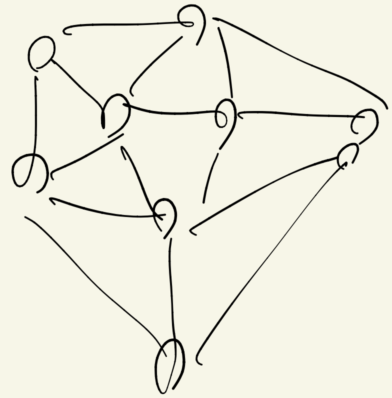


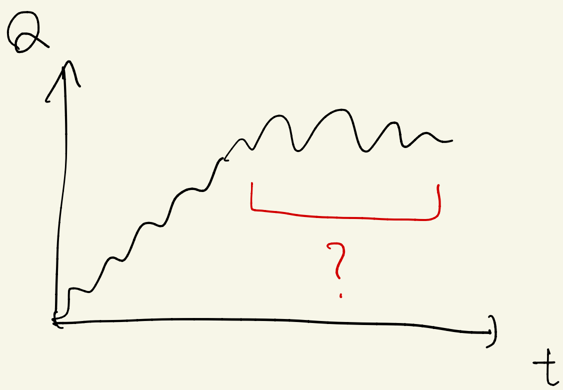


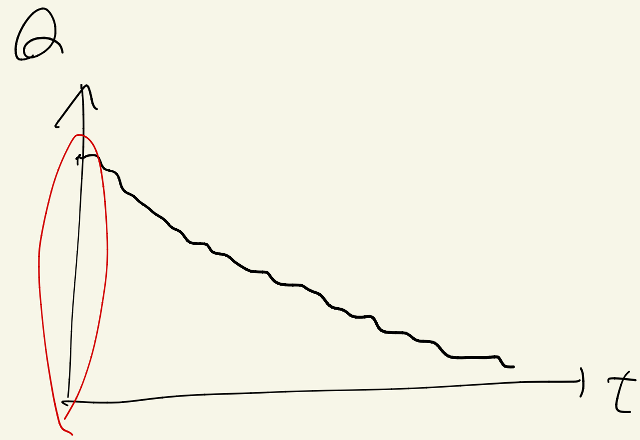


$U|0..0\rangle$

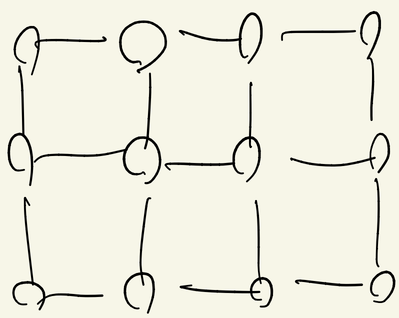






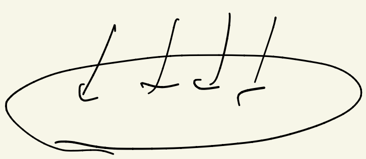


グラフ state

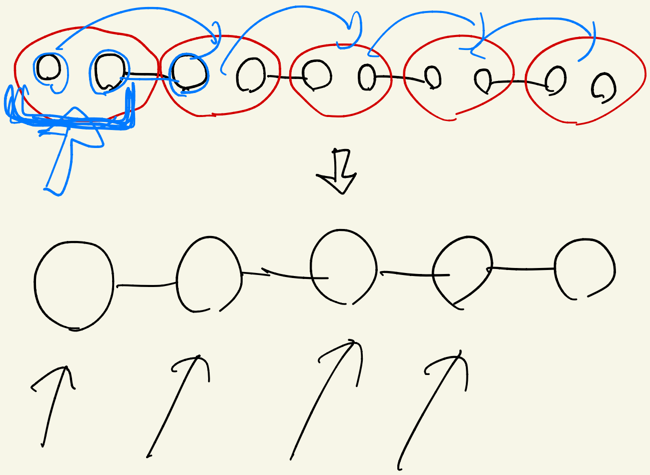


5-body $-\sum_i K_i$

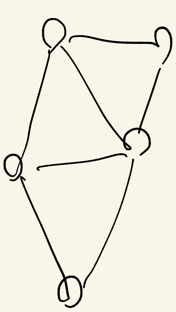
AKLT



PEPS



$$|\psi\rangle$$



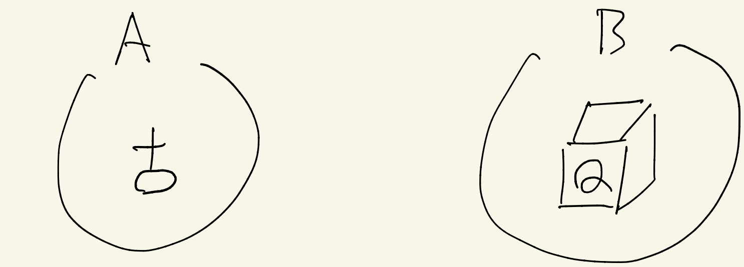
$$H = \sum_{ij} J_{ij}\, \sigma_i \sigma_j$$

$$\mathrm{Tr}\left(e^{-\beta H}\right)$$

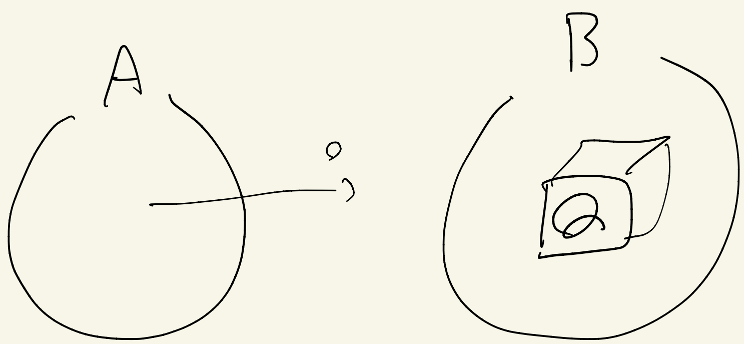
$$= \langle \alpha | \sigma \rangle$$

$\uparrow$ product state

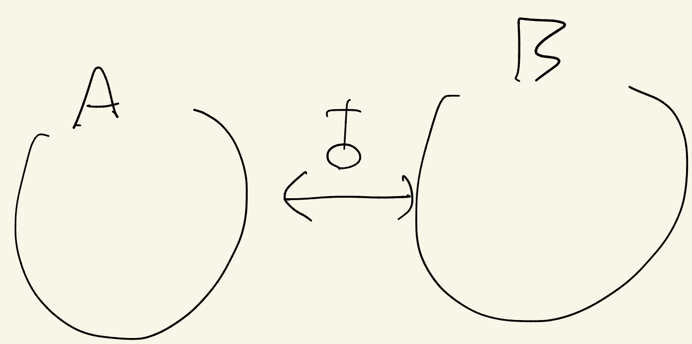
ブラインド量子計算



BFK-protocol

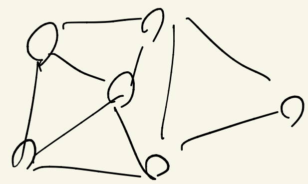


$$\{|0\rangle + e^{i\theta}|1\rangle\}$$



A $\longrightarrow$ B

$$\bigotimes_{j=1}^{N} e^{iZ\theta_j}|+\rangle^{\otimes N}$$



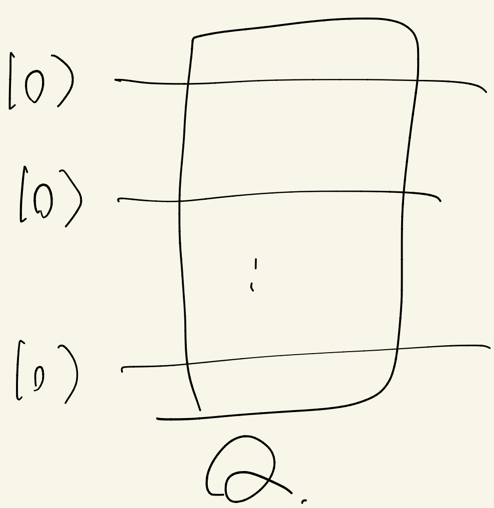
$$\tilde{CZ}\bigotimes_{j=1}^{N} e^{iZ\theta_j}|+\rangle^{\otimes N}$$

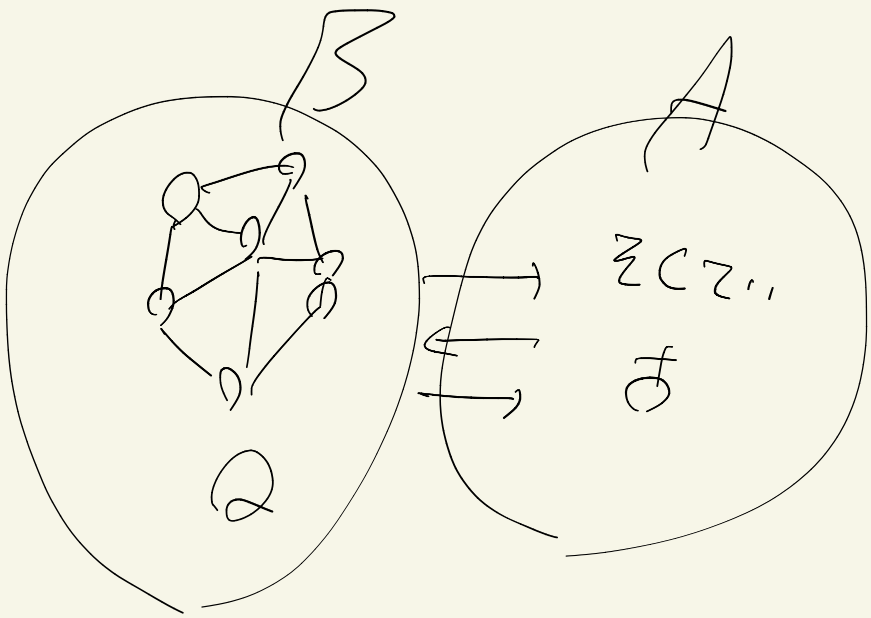
$$= \bigotimes_{j=1}^{N} e^{iZ\theta_j}\underbrace{\tilde{CZ}|+\rangle^{\otimes N}}_{|G\rangle}$$

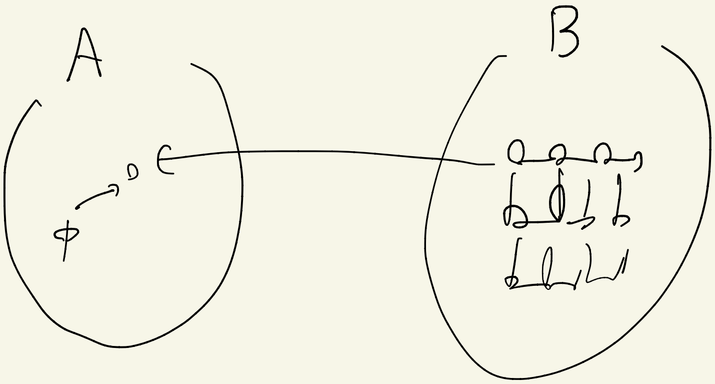
$\delta_1 = \phi_1 + \theta_1$ $\longrightarrow$

$\xleftarrow{m_1}$

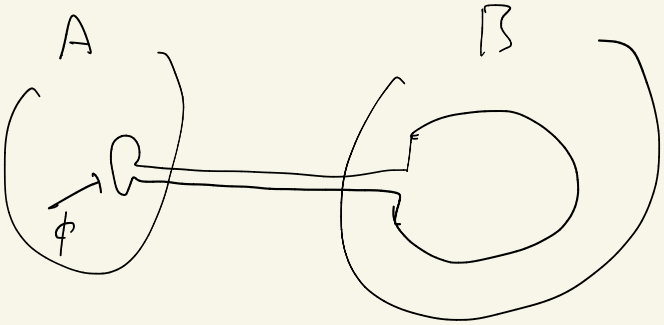
$\delta_2 = \phi_2 + \theta_2$ $\longrightarrow$







no-signaling



MPS

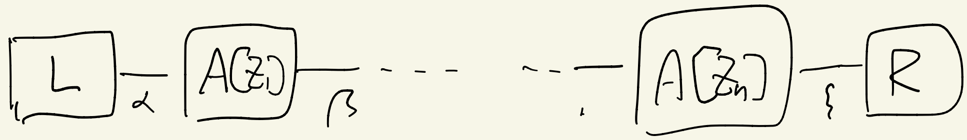
$$|\psi\rangle = \sum_{z_1=0}^{1}\cdots\sum_{z_n=0}^{1} C_{z_1\cdots z_n}\,|z_1\cdots z_n\rangle$$

$$\{0,1\}^n \longrightarrow \mathbb{C}$$

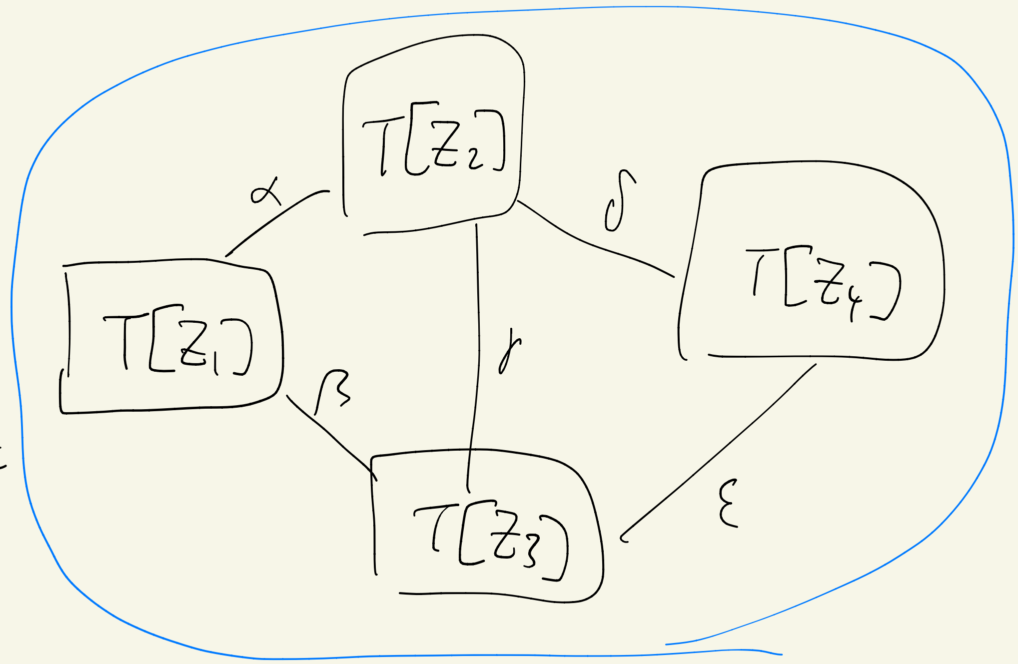
$$|\psi\rangle = \sum_{z_1=0}^{1}\cdots\sum_{z_n=0}^{1} \overbrace{\langle L|\,A[z_1]\cdots A[z_n]\,|R\rangle}^{C(z_1\cdots z_n)}\,|z_1\cdots z_n\rangle$$

$$\underbrace{\left(\cdots\cdots\right)}_{D} \qquad D\overbrace{\left(\quad\;\right)}^{D} \qquad \left(\vdots\right)D$$

TNS



$\sum_{z_1 \cdots z_4}$



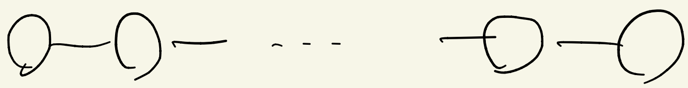
$|z_1 \cdots z_4\rangle$

$$\sum_{\alpha,\beta,\gamma,\delta,\xi} T[z_1]_{\alpha\beta}\, T[z_2]_{\alpha\delta\gamma}\, T[z_3]_{\beta\gamma\xi} \times T[z_4]_{\delta\xi}$$

MPS

TNS

1-d graph state



$$\sum_{z_1=0}^{1}\cdots\sum_{z_n=0}^{1}\langle L|\underbrace{A[z_n]\cdots A[z_1]}|R\rangle\,|z_n\cdots z_1\rangle$$

$$\langle L| = \langle 0|$$

$$|R\rangle = |+\rangle$$

$$A[0] = |+\rangle\langle 0|$$

$$A[1] = |-\rangle\langle 1|$$

$$A[0]A[0] = +$$

$$A[0]A[1] = +$$

$$A[1]A[0] = +$$

$$A[1]A[1] = -1$$

$$\prod_{i=1}^{n-1} CZ_{i,i+1}\,|+\rangle^{\otimes n} = \prod_{i=1}^{n-1} CZ_{i,i+1}\,\frac{1}{\sqrt{2^n}}\sum_x |x\rangle$$

$$= \frac{1}{\sqrt{2^n}}\sum_x \underbrace{(-1)^{\sum_{i=1}^{n-1} x_i\cdot x_{i+1}}}\,|x\rangle$$

$$\sum_{z_n=0}^{1} \cdots \sum_{z_2=0}^{1} \sum_{z_1=0}^{1} \langle L| A[z_n] \cdots A[z_2] A[z_1] |R\rangle \, |z_n \cdots z_1\rangle$$

$|\eta_\pm\rangle = |0\rangle \pm e^{i\theta} |1\rangle$

$\longrightarrow$

$$\sum_{z_n=0}^{1} \cdots \sum_{z_2=0}^{1} \sum_{z_1=0}^{1} \langle L| A[z_n] \cdots A[z_2] A[z_1] |R\rangle \, |z_n \cdots z_2\rangle \otimes |\eta_\pm\rangle\langle \eta_\pm | z_1\rangle$$

$$= \sum_{z_n=0}^{1} \cdots \sum_{z_2=0}^{1} \langle L| A[z_n] \cdots A[z_2] \left[\sum_{z_1=0}^{1} \langle \eta_\pm | z_1\rangle A[z_1] \right] |R\rangle \, |z_n \cdots z_2\rangle \otimes |\eta_\pm\rangle$$

$$\langle \eta_\pm | 0\rangle A[0] + \langle \eta_\pm | 1\rangle A[1]$$

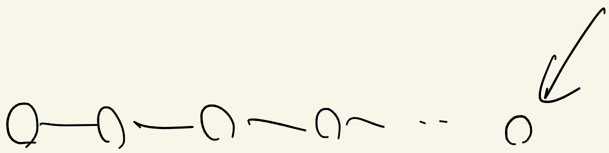
$$= |+\rangle\langle 0| \pm e^{-i\theta} |-\rangle\langle 1|$$

$$= H \cdot e^{i\theta/2 \, Z}$$

$$= J(\theta)$$

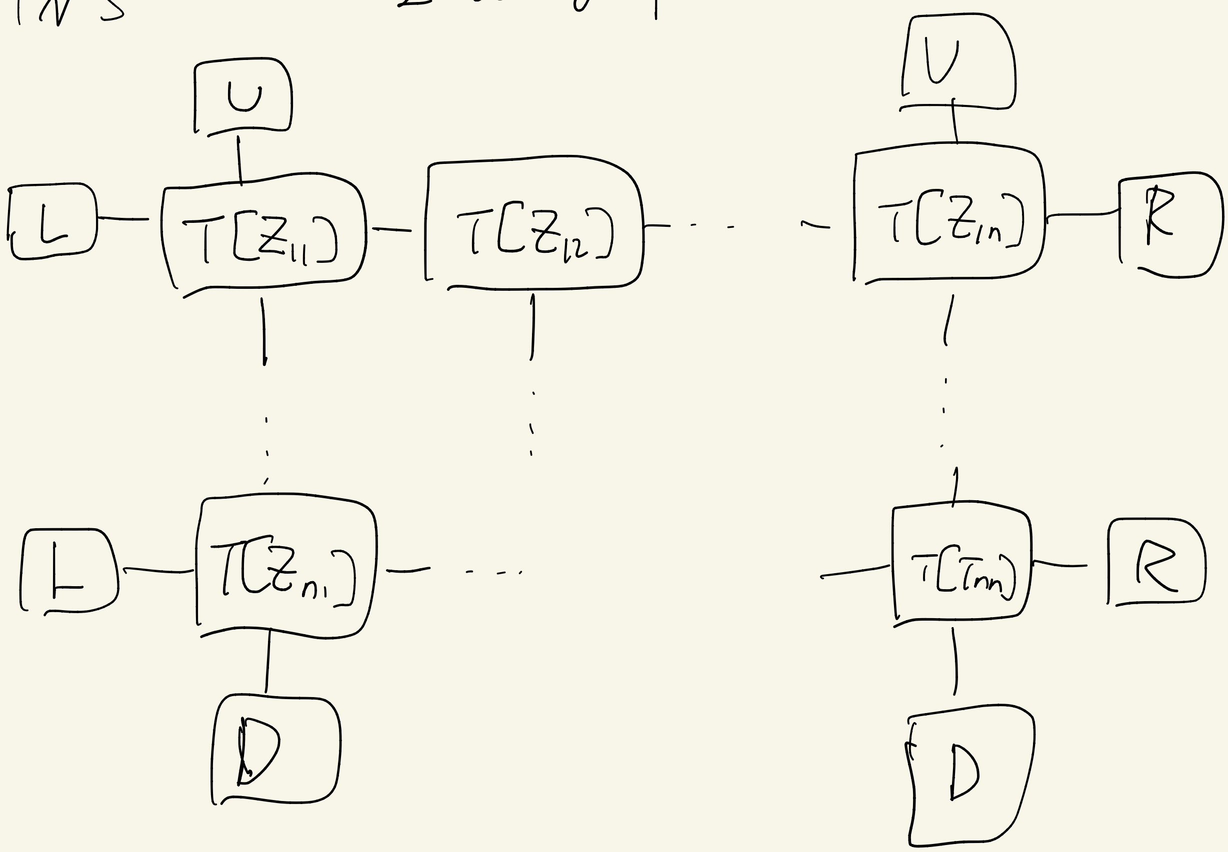
$$\sum_{z_n=0}^{1} \cdots \sum_{z_2=0}^{1} \langle L| A[z_n] \cdots \underbrace{A[z_2]}_{J(\theta')} \overset{A[z_1]}{J(\theta)} |R\rangle \, |z_n \cdots z_2\rangle \otimes |\eta_\pm\rangle$$

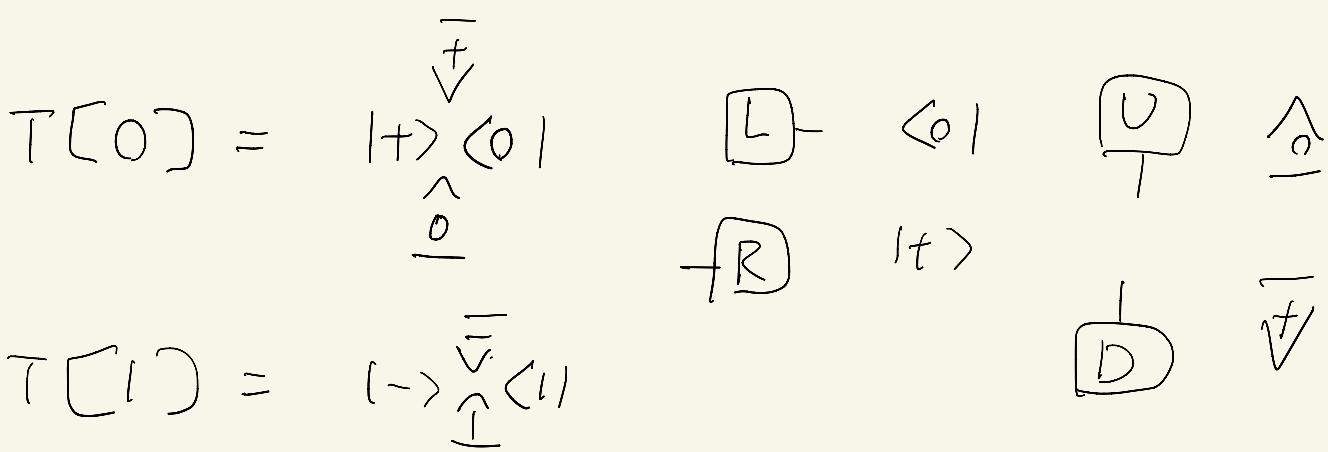
$$\boxed{J(\theta)\, J(\theta)\, |R\rangle}$$



TNS

2-d graph state





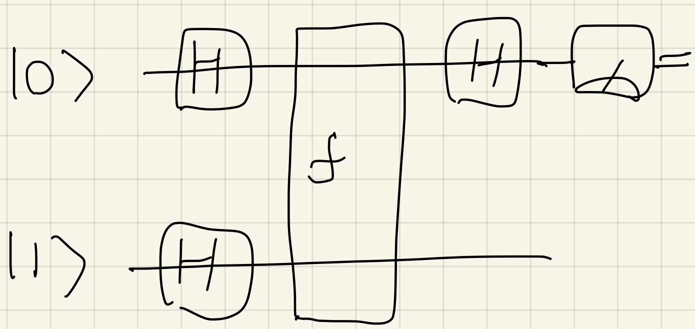
Deutch algorithm.

problem given $f : \{0,1\} \to \{0,1\}$ decide

- constant $f(0) = f(1)$
- balanced $f(0) \neq f(1)$

古典 … 2 query 必要

量子 …



$$|0\rangle|1\rangle \longrightarrow (|0\rangle+|1\rangle)(|0\rangle-|1\rangle)$$

$$= |0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle$$

$$\longrightarrow |0\rangle|f(0)\rangle - |0\rangle|f(0)\oplus 1\rangle$$

$$+ |1\rangle|f(1)\rangle - |1\rangle|f(1)\oplus 1\rangle$$

constant

$$\longrightarrow \quad |0\rangle|f(0)\rangle - |0\rangle|f(0)\oplus 1\rangle$$

$$+ \; |1\rangle\underline{|f(0)\rangle} - |1\rangle|\underline{f(0)}\oplus 1\rangle$$

$$= \; |+\rangle\left(|f(0)\rangle - |f(0)\oplus 1\rangle\right)$$

balanced

$$\longrightarrow \quad |0\rangle|f(0)\rangle - |0\rangle|f(0)\oplus 1\rangle$$

$$+ \; |1\rangle\underline{|f(0)\oplus 1\rangle} - |1\rangle|\underline{f(0)}\rangle$$

$$= \; |-\rangle\left(|f(0)\rangle - |f(0)\oplus 1\rangle\right)$$

Naor-Yung signature from OWF

f: OWF

$pk_0 = f(x_0)$
$pk_1 = f(x_1)$

x_0 と x_1 はランダムにとる

$\mathrm{Sign}(b) = x_b$

$\mathrm{Verify}(b, \sigma)$: compute $f(\sigma)$
accepts iff $f(\sigma) = pk_b$

これを量子でやると single-shot になる。[Amos-Georgiou-Kiayias-Zhandry]

$pk = y$

$|sk\rangle = \sum_{\substack{x \\ f(x)=y}} |x\rangle$

$|sk\rangle$ から Grover で求める

$\mathrm{Sign}(b, |sk\rangle) = x$ s.t. $x|_1 = b$

$\mathrm{Verify}(b, \sigma)$: accepts iff $f(x) = y \wedge x|_1 = b$

もし $b=0$ と $b=1$ の両方で sign できると

f の claw-free に反する。