Lecture 1 1/15

Overview

- Course overview and syllabus
- Q.. Formalism for closed systems. revisited.
- The quantum density operator.
- Schmidt decomposition and purification

Quantum formalism revisited

- States $|\psi\rangle \in \mathbb{C}^d$, $0 \leq d \leq \infty$
- Unitary evolution: $U : \mathbb{C}^d \to \mathbb{C}^d$

$U^{-1} = U^\dagger$, $U : |\psi\rangle \mapsto U|\psi\rangle$

(linear, surjective map which preserves inner prod).

- Isometry linear map preserving inner prod.

$V : \mathbb{C}^m \to \mathbb{C}^n$, $V^\dagger V = I_n$ $\quad n \geq m$

- Question : can $m > n$?
- Fact : For any isometry $V : Q^{\otimes m} \to Q^{\otimes n}$

$\exists\, U$, $|0\rangle \in Q^{\otimes n-m}$ s.t.

$$V = U(\cdot \otimes |0\rangle_E)$$

- POVM : $E_j \geq 0$, $\sum_j E_j = I$

❦ Measurement operators : M_j square matrices.

$$\sum_m M_j^\dagger M_j = I$$

$$P(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$

$$|\psi_m\rangle = \frac{M_m |\psi\rangle}{\sqrt{p_m}}$$

◎ Fact : for any meas op set $M_1, \dots, M_t$ s.t. $E_j = M_j^\dagger M_j$

$$M_j = U_j \sqrt{E_j} \quad \text{for some unitary.}$$

idea : polar decomposition $M_j = U_j P_j$, $P_j \geq 0$

$$P_j = \sqrt{M_j^\dagger M_j}$$

❦ Observables $O = O^\dagger$, $\langle O \rangle = \langle \psi | O | \psi \rangle$.

❦ Implementation of general meas operators.

Let $M_1 \dots M_t$ be a set of meas operators.

Let V be the isometry map.

$$V|\psi\rangle = \sum_{j=1}^{t} M_j |\psi\rangle |j\rangle .$$

we know , $\exists\ U_j |0\rangle$ s.t.

$$V|\psi\rangle|0\rangle = \sum_{j=1}^{t} M_j |\psi\rangle |j\rangle$$

measure ancilla in comp basis

We show $p_m = \langle\psi| M_m^\dagger M_m |\psi\rangle$

$$|\psi_m\rangle = \frac{M_m|\psi\rangle}{\sqrt{p_m}}.$$

E.g. Distinguishing two q. states.

$|\psi\rangle, |\varphi\rangle$.

let $\Pi_1 = |\psi\rangle\langle\psi|$, $\Pi_2 = I - |\psi\rangle\langle\psi|$.

- if state was $|\psi\rangle$ we get Π_1 w.p. 2
- if state was $|\varphi\rangle$ we get

$$p_1 = |\langle\psi|\varphi\rangle|^2, \quad p_2 = 1 - |\langle\psi|\varphi\rangle|^2$$

$$\Pr(1|1) = 1$$

$$\Pr(2|2) = 1 - |\langle\psi|\varphi\rangle|^2$$

$$\Pr(\text{success}) = \frac{1}{2}\left(P(1|1) + P(2|2)\right)$$

$$= 1 - \frac{|\langle\psi|\varphi\rangle|^2}{2}$$

Exercise: is this optimal?

Density matrices

- To an ensemble $\{p_j, |\psi_j\rangle\}$

  assign $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$.

- $\rho \geq 0$, $\mathrm{tr}(\rho) = 1$

E.g. Upon measuring $|\psi\rangle$ according to $\{M_m\}$

we obtain $|\psi_m\rangle$ w.p. p_m.

$\Rightarrow$ $\rho = \sum_m M_m |\psi\rangle\langle\psi| M_m^\dagger$

- $\forall (p_1, \rho_1) \cdots (p_t, \rho_t)$

  $\rho = \sum_j p_j \rho_j$ is also a density matrix.

- if $\rho \geq 0$, $\mathrm{tr}(\rho) = 1$

  $\Rightarrow$ $\rho = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$ $\rightarrow$ eigen decomp

  $\sum_j \lambda_j = 1$, $\lambda_j \geq 0$

Time evol: $\rho \longmapsto U\rho U^\dagger$

Meas: $p_m = \mathrm{tr}(\rho E_m)$. (POVM)

$\rho \longmapsto \sum_m M_m \rho M_m^\dagger$ (meas).

Observable: $\langle O \rangle = \mathrm{tr}(\rho O)$

- ρ is pure if $\rho = |\psi\rangle\langle\psi|$
- ρ is pure iff $\mathrm{tr}(\rho^2) = 1$

  $(\mathrm{rank}(\rho) = 1)$

- Decomposition is not unique

  e.g. $|+\rangle\langle+| + |-\rangle\langle-| = |0\rangle\langle 0| + |1\rangle\langle 1|$

Thm: $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

$= \sum_j q_j |\varphi_j\rangle\langle\varphi_j|$

iff $|\tilde{\psi}_j\rangle = \sqrt{p_j}\,|\psi_j\rangle$

$|\tilde{\varphi}_j\rangle = \sqrt{q_j}\,|\varphi_j\rangle$

are unitarily available.

Reduced density matrix

- $tr_B : D^{AB} \longrightarrow D^A$
- $tr_B : \rho_{AB} \longmapsto \rho_A = tr_B(\rho_{AB})$.

$$= \sum_j (I_A \otimes \langle j|_B)\rho(I \otimes |j\rangle_B)$$

- $tr_B(X \otimes Y) = X \; tr(Y)$.
- $tr(|\psi\rangle\langle\varphi|) = \langle\varphi|\psi\rangle$
- $tr_B |EPR\rangle_{AB}\langle EPR| = \frac{I_A}{2}$

Schmidt decomposition

Thm. $|\psi\rangle_{AB} \in \mathcal{H}_{AB}$

$$|\psi\rangle = \sum_{j=1}^{r} \lambda_j |v_j\rangle_A \otimes |w_j\rangle_B$$

$\lambda_j \geq 0$, $\sum_j \lambda_j = 1$

- Schmidt rank $= r$.

Corr. $\rho_A = \sum_j \lambda_j^2 |v_j\rangle\langle v_j|$

$$\rho_B = \sum_j \lambda_j^2 |w_j\rangle\langle w_j|.$$

$$\Rightarrow \quad \mathrm{Tr}(\rho_A^2) = \mathrm{Tr}(\rho_B^2)$$

Pf of Thm: $\dim(A) = m, \quad \dim(B) = n$

$$|\psi\rangle_{AB} = \sum_{jk} \Omega_{jk} |j\rangle_A |k\rangle_B.$$

$\Omega \in \mathbb{C}^{m \times n}$

◎ Consider partial transpose map.

$$PT_B: X_A \otimes Y_B = X_A \otimes Y_B^T, \quad PT_B^2 = \mathbb{I}$$

$$\Rightarrow PT_B(|\psi_{AB}\rangle) = \Omega$$

Ω has singular value decomp.

$$\Omega = \sum_j \lambda_j v_j w_j^T \qquad \|v_j\| = \|w_j\| = 1$$

$$|\psi_{AB}\rangle = PT_B(\Omega) = \sum_j \lambda_j |v_j\rangle \otimes |w_j\rangle.$$

⊛ Schmidt rank is a meas of entanglement.

Application: purification

for any ρ_A $\exists$ $|\psi_{AB}\rangle$ s.t. $Tr_B(\psi_{AB}) = \rho_A$

Pf: $\rho_A = \sum_j \lambda_j |v_j\rangle\langle v_j|$.

let $|\psi\rangle_{AB} = \sum_j \lambda_j |v_j\rangle_A |v_j\rangle_B$.

⊛ Uhlmann's thm

suppose $\rho_A = tr_B(\psi_{AB}) = tr_C(\varphi_{AC})$

then $\exists$ isometry $V: B \to C$ s.t.

$$(I_A \otimes V_B)|\psi_{AB}\rangle = |\varphi\rangle_{AC}$$

Pf. Since ψ_{AB}, φ_{AC} purify to the same

$$\rho = \sum_j p_j |v_j\rangle\langle v_j|$$

then

$$|\psi\rangle_{AB} = \sum_j \sqrt{p_j}\, |v_j\rangle \otimes |q_j\rangle_B$$

$$|\varphi\rangle_{AC} = \sum_j \sqrt{p_j}\, |v_j\rangle \otimes |w_j\rangle_C .$$

$\exists$ linear map $\underset{B\to C}{V}\, |u_j\rangle_B = |w_j\rangle_C$.

since $|u_j\rangle$ & $|w_j\rangle$ are orthonormal

$\Rightarrow$ V is an isometry on subspace

spanned by $|u_j\rangle$

$\Rightarrow$ extend to the whole domain.

(trivial action).

Fact about partial trace

$$\mathrm{Tr}_B(\rho_{AB} O_A) = \mathrm{Tr}(\rho_A O_A)$$

where $\rho_A = \mathrm{Tr}_B(\rho_{AB})$.

Lecture 2 quantum channels

Recall meas op's M_j this corresponds to

a map $\mathcal{E}: D_n \to D_n$, $\mathcal{E}(\rho) = \sum_j M_j \rho M_j^\dagger$

$$\sum_{j=1}^{r} M_j^\dagger M_j = I$$

- unitary map corresponds to $r = 1$.

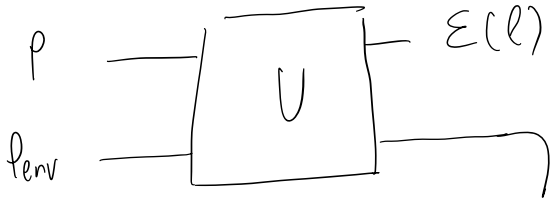
$$\mathcal{E}(\rho) = U\rho U^\dagger, \quad U^\dagger U = I$$

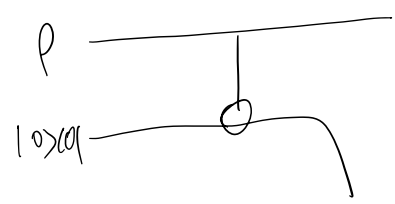
Three formulations of q. operations:

1. Completely positive Trace Preserving (CPTP).
2. Operator Sum rep.
3. System + env representation.

System + env perspective.

$$\mathcal{E}(\rho) = \mathrm{tr}_{env}\left(U(\rho \otimes \rho_{env})U^\dagger \right).$$



Example. 

◈ System + env rep $\Rightarrow$ operator sum rep.

$$\mathcal{E}(\rho) = \mathrm{tr}_{env}\left(U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger \right)$$

$$= \sum_j \langle e_j|U|e_0\rangle \rho \langle e_j|U|e_0\rangle^\dagger$$

$$=: \sum_j E_j \rho E_j^\dagger \quad , E_j = \langle e_j|U|e_0\rangle$$

furthermore

$$\sum_j E_j^\dagger E_j = \sum_j \langle e_0|U^\dagger|e_j\rangle\langle e_j|U|e_0\rangle$$

$$= I$$

therefore $\mathrm{tr}(\mathcal{E}(\rho)) = \mathrm{tr}\left(\sum_j E_j \rho E_j^\dagger\right)$

$$= \mathrm{tr}\left(\left(\sum_j E_j^\dagger E_j\right)\rho\right) = \mathrm{tr}(\rho).$$

Physical interpretation of operator sum rep.

$$\mathcal{E}(\rho) = \sum_j E_j \rho E_j^\dagger = \sum_j p_j \rho_j$$

where $p_j = \mathrm{tr}(E_j^\dagger E_j \rho)$ $\quad \rho_j = \dfrac{E_j \rho E_j^\dagger}{p_j}$

(1) Operator-sum rep $\Longrightarrow$ System + env rep.

Stinespring's dilation

(a) We can define an isometry.

$$V = \sum_j E_j \otimes |e_j\rangle .$$

$$|\psi\rangle \to V(|\psi\rangle) = \sum_j E_j|\psi\rangle \otimes |e_j\rangle , \quad \mathcal{E}(\rho) = tr_{env}(\rho).$$

---

(2) CPTP rep

- Trace preserving: $tr(\mathcal{E}(\rho)) = tr(\rho)$
- Linearity: $\mathcal{E}(\sum_j q_j \rho_j) = \sum_j q_j \mathcal{E}(\rho_j)$.
- Completely positive: $(\mathcal{E} \otimes I)(X) \geq 0$ iff $X \geq 0$.

Theorem: A map $\mathcal{E}$ is CPTP iff

$$\mathcal{E}(\rho) = \sum_j E_j \rho E_j^\dagger , \quad \sum_j E_j^\dagger E_j = I.$$

Pf

(2) $\Rightarrow$ (1) immediate.

(1) $\Rightarrow$ (2). $\mathcal{J}(\mathcal{E}) = \mathcal{E} \otimes \mathcal{I}(\phi)$ (Choi map). Jamiołkowski

$$|\phi\rangle = \sum_j |j\rangle_A |j\rangle_B$$

Thm. $\mathcal{E}$ is CPTP iff $J(\mathcal{E})$ is PSD.

Pf. If $\mathcal{E}$ is CPTP then $J(\mathcal{E})$ is PSD by def.

Suppose $J(\mathcal{E})$ is PSD, then

$$J(\mathcal{E}) = \sum_{j=1}^{k} |J_j\rangle\langle J_j|.$$

We can show $\mathcal{E}(\rho) = Tr_B\left(J(\mathcal{E})(I \otimes \rho^T)\right)$

$$= \sum_{j=1}^{k} Tr_B\left(|J_j\rangle\langle J_j|(I \otimes \rho^T)\right)$$

$$= \sum_{j=1}^{k} F_j \rho F_j^\dagger$$

where $F_j = (I_A \otimes \rho_B)|J_j\rangle$.

$$= \sum_{l,k} c_{l,k}^{(j)} |l\rangle\langle k|$$

where $|J_j\rangle = \sum_{l,k} c_{l,k}^{(j)} |l\rangle|k\rangle$.

Corr. $\mathcal{E}$ is CP iff $\mathcal{E} \otimes I$ is P.

Normalization Cond.

$$\sum_j F_j^\dagger F_j = \mathrm{tr}_A J(\mathcal{E})_{AB}$$

$$= d \times \frac{I}{d} = I .$$

Lemma : $J(\mathcal{E})$ fully specifies $\mathcal{E}$.

pf. for any $|\psi\rangle \in \mathcal{H}_A$

$$\mathcal{E}(|\psi\rangle_A\langle\psi|) = \langle\psi|_B^* \, J(\mathcal{E}) \, |\psi\rangle_B^*$$

$$J(\mathcal{E}) \geq 0 \Rightarrow J(\mathcal{E}) = \sum_\ell \sigma_\ell |V_\ell\rangle_{AB}\langle V_\ell|$$

$$\sigma_\ell \geq 0$$

then $\forall |\psi\rangle \in \mathcal{H}_A$

$$\mathcal{E}(\psi) = \langle\psi^*|_B \left(\sum_\ell \sigma_\ell |V_\ell\rangle_{AB}\langle V_\ell| \right) |\psi^*\rangle_B$$

$$= \sum_\ell \sigma_\ell \langle\psi^*|_B |V_\ell\rangle_{AB} \langle V_\ell|_{AB} |\psi^*\rangle_B .$$

Define $E_j(|\psi\rangle) = \sqrt{\sigma_j} \langle\psi_B^*|V_j\rangle_{AB}$

$$\Rightarrow \mathcal{E}(\psi) = \sum_j E_j \psi E_j^\dagger$$

Another equivalent way:

$$\mathrm{Tr}_B \left(J(\mathcal{E}) (I_A \otimes \rho_B^T) \right) = \mathcal{E}(\rho).$$

Fact. If we map E_j to $F_j = \sum_k U_{jk} E_k$

we obtain the same channel. if $U^\dagger = U^{-1}$.

To see this $\forall \rho \in D$.

$$\mathcal{E}_2(\rho) = \sum_j F_j \rho F_j^\dagger = \sum_{j} \sum_{k,\ell} U_{jk} E_k \rho E_\ell^\dagger U_{j\ell}^*$$

$$= \sum_{k,\ell} \left(\sum_j U_{j,k} U_{j,\ell}^* \right) E_k \rho E_\ell^\dagger$$

$$= \mathcal{E}_1(\rho).$$

Fact. $\mathcal{E}_1 \longleftrightarrow E_j \implies \mathcal{E}_1 \circ \mathcal{E}_2 \longleftrightarrow E_j F_k$.

$\mathcal{E}_2 \longleftrightarrow F_j$

Fact. a channel can be inverted by another channel

i.e, $\mathcal{E}_2 \circ \mathcal{E}_1 = \mathcal{I}$ iff it is unitary.

Dual of a channel

$\mathcal{E}(\rho) = \sum_j E_j \rho E_j^\dagger$ $\quad tr(X \mathcal{E}(\rho)) = tr(\mathcal{E}^*(X)\rho)$

$\mathcal{E}^*(X) = \sum_j E_j^\dagger X E_j$

Crucially $\mathcal{E}^*(I) = I$. (unital)

$\mathcal{E}^*$ not necessarily trace preserving

If $\mathcal{E}(I) = I \implies \mathcal{E}$ is unital

Thm. Suppose $\{F_j\}_{j=1}^{k}$, $\{E_i\}_{i=1}^{k'}$, $k \le k'$ be two Kraus rep of a cp map $\mathcal{E}$, then $\exists$ isometry $V : \mathbb{C}^k \to \mathbb{C}^{k'}$ s.t.

$$E_i = \sum_{j=1}^{k} V_{ij} F_j$$

- $\mathcal{J}(\mathcal{E})$ is PSD hence:

$$\mathcal{J}(\mathcal{E}) = \sum_j |J_j\rangle\langle J_j| .$$

$$= \sum_{i=1}^{k} (F_i \otimes I_B)|\Omega\rangle\langle\Omega|(F_i^\dagger \otimes I_B).$$

$$= \sum_{j=1}^{k'} (E_i \otimes I_B)|\Omega\rangle\langle\Omega|(E_i^\dagger \otimes I_B).$$

Let $X = \sum_i F_i \otimes I_B |\Omega\rangle\langle e_i|$

$$Y = \sum_j E_j \otimes I_B |\Omega\rangle\langle e_j| .$$

$$XX^\dagger = YY^\dagger$$

$\Rightarrow$ $\exists$ isometry V s.t. $X = YV^\dagger$

$XX^\dagger = YY^\dagger \iff X = YV^\dagger$, $\exists$ isom V

pf. $X = \sum_i \sigma_i |u_i\rangle\langle v_i|$

$Y = \sum_j \sigma_j |u_i\rangle\langle \tilde{v}_i|$ $\Rightarrow \exists V : |v_j\rangle \mapsto |\tilde{v}_j\rangle$ $\forall j$

◎ Example of a map that is positive but not Completely positive: Partial transpose.

$$T : \rho \mapsto \rho^T$$

T is positive since. $\rho \geq 0 \iff \rho^T \geq 0$

$$\langle \psi | \rho^T | \psi \rangle = \langle \psi^* | \rho | \psi^* \rangle \geq 0$$

Partial Transpose $T \otimes I : A \otimes B \mapsto A^T \otimes B$

$$\phi = \sum_{j,k} |j\rangle\langle k| \otimes |j\rangle\langle k|$$

$$(T \otimes I)(\phi) = \sum_{j,k} |j\rangle\langle k| \otimes |k\rangle\langle j|.$$

$$= \sum_{j,k} |j\rangle|k\rangle\langle k|\langle j|$$

$$= \text{SWAP} \neq 0$$

Physical implementation of measurement (Preskill Ch. 3).

Suppose we want to meas

$$M = \sum_a \lambda_a |a\rangle\langle a|.$$

$$|\psi\rangle = \sum_a \psi_a |a\rangle$$

$$e^{-i (M \otimes P)} \cdot \left(|\psi\rangle \otimes |x=0\rangle \right)$$

$$= \sum_a \psi_a \, e^{-i \lambda_a P} |a\rangle \otimes |x=0\rangle$$

$$= \sum_a \psi_a |a\rangle \otimes |x=\lambda_a\rangle$$

- Obtain $x = \lambda_a$ w.p. $|\psi_a|^2$ and collapse $|\psi\rangle$ to $|a\rangle$.

Basic quantum channels

① Depolarization Channel:

$$\mathcal{E}_p(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z).$$

$$V_{A\to AE}(|\psi\rangle) = \sqrt{1-p}\,|\psi\rangle\otimes|0\rangle + \sqrt{\frac{p}{3}}\,(X|\psi\rangle\otimes|1\rangle + Y|\psi\rangle\otimes|2\rangle + Z|\psi\rangle\otimes|3\rangle).$$

$$E_0 = \sqrt{1-p}\,,\ E_1 = \sqrt{\frac{p}{3}}\,X,\ E_2 = \sqrt{\frac{p}{3}}\,Y,\ E_3 = \sqrt{\frac{p}{3}}\,Z.$$

$$p = 3/4 \Rightarrow \mathcal{E}(\rho) = \frac{1}{4}(\rho + X\rho X + Y\rho Y + Z\rho Z).$$

$$= I/2 \quad \text{(Exercise)}.$$

Generalized Block sphere

$$\rho = \frac{1}{2}(I + \vec{v}\cdot\vec{\sigma}).$$

$$\vec{\sigma}\cdot\vec{v} = v_x\sigma_x + v_y\sigma_y + v_z\sigma_z$$

$$\|\vec{v}\|^2 = \mathrm{tr}(\rho)^2$$

We can show

$$\mathcal{E}_p(\rho) = \frac{1}{2} + \frac{1}{2}\left(1 - \frac{4p}{3}\right)\vec{v}\cdot\vec{\sigma}$$

$$X(\vec{v}\cdot\vec{\sigma})X + Y(\vec{v}\cdot\vec{\sigma})Y + Z(\vec{v}\cdot\vec{\sigma})Z = -\vec{v}\cdot\vec{\sigma}$$

$$(1-p)\ \frac{1}{2}(I + \vec{v}\cdot\vec{\sigma}) + \frac{p}{3}\ \frac{1}{2}(3I - \vec{v}\cdot\vec{\sigma})$$

$$= \frac{I}{2} + \frac{1}{2}\left(1 - \frac{4p}{3}\right)\vec{r}\cdot\vec{\sigma}$$

$$\boxed{\mathcal{E}_p : \vec{v} \longmapsto \left(1 - \frac{4}{3}p\right)\vec{v}}$$

Dephasing Channel

$$\mathcal{E}(\rho) = \left(1 - \frac{p}{2}\right)\rho + \frac{p}{2} Z\rho Z.$$

$$\mathcal{E}\begin{pmatrix} \rho_0 & \rho_{01} \\ \rho_{10} & \rho_1 \end{pmatrix} = \begin{pmatrix} \rho_0 & (1-p)\rho_{01} \\ (1-p)\rho_{10} & \rho_1 \end{pmatrix}$$

$$E_0 = \sqrt{1-p}\ I\ ,\ E_1 = \sqrt{p}\ |0\rangle\langle 0|\ ,\ E_2 = \sqrt{p}\ |1\rangle\langle 1|$$

$$|0\rangle_A \longmapsto \sqrt{1-p}\ |0\rangle_A \otimes |0\rangle_E + \sqrt{p}\ |0\rangle_A \otimes |1\rangle_E$$

$$|1\rangle_A \longmapsto \sqrt{1-p}\ |1\rangle_A \otimes |0\rangle_E + \sqrt{p}\ |1\rangle_A \otimes |2\rangle_E$$

$$\mathcal{E} : \vec{v} \longmapsto \vec{v}'$$

$$\begin{cases} v_1' = (1-p)\, v_1 \\ v_2' = (1-p)\, v_2 \\ v_3' = v_3 \end{cases}$$

E.x. rotating a q. state w. an unknown angle

$$\rho = \frac{1}{\sqrt{4\pi\lambda}} \int_{-\infty}^{+\infty} R_z(\theta)\,|\psi\rangle\langle\psi|\,R_z^{\dagger}(\theta)\; e^{-\theta^2/4\lambda}\, d\theta$$

$$= \begin{pmatrix} |a|^2 & ab^* e^{-\lambda} \\ a^* b\, e^{-\lambda} & |b|^2 \end{pmatrix}$$

---

② Amplitude damping Modeling spontaneous decay

$$|0\rangle_A |0\rangle_E \longmapsto |0\rangle_A |0\rangle_E$$

$$|1\rangle_A |0\rangle_E \longmapsto \sqrt{1-p}\, |1\rangle_A |0\rangle_E + \sqrt{p}\, |0\rangle_A |1\rangle_E$$

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} \longmapsto \begin{pmatrix} \rho_{00} + p\rho_{11} & \sqrt{1-p}\,\rho_{01} \\ \sqrt{1-p}\,\rho_{10} & (1-p)\rho_{11} \end{pmatrix}$$

$$\vec{V} \longmapsto \left(\sqrt{1-p}\,v_x \,,\ \sqrt{1-p}\,v_y \,,\ \gamma + v_z(1-\gamma) \right)$$

Universality in Q. Comp.

- **Def.** A gate set $G = \{U_1, \dots, U_T\}$ is universal if $\forall U, \forall \delta \geq 0$

$\exists \ \tilde{U} = U_{i_K} \cdots U_{i_1}$ s.t $\| \tilde{U} - e^{i\varphi} U \|_\infty \leq \delta$,

---

- Here $\|A\|_\infty = \sigma_{max}(A) = \lambda_{max}(|A|)$.

- **Encoded universality**: G is an encoded universal gateset if

$\exists$ isom $V : Q_n \to Q_m$, $m \geq n$ s.t.

$\forall U \in \mathcal{U}(Q_n)$, $\forall \delta > 0$, $\exists \ \tilde{U} \in \mathcal{U}(Q_m)$. ϵ $\langle G \rangle$

$\| \tilde{\tilde{U}} - e^{i\varphi} U \|_\infty \leq \delta$, for some $\varphi \in \mathbb{R}$.

Here $\tilde{\tilde{U}} = \tilde{U} V$.

E.g. $|0_L\rangle = |01\rangle$, $|1_L\rangle := |10\rangle$

E.g CNOT + R_x is encoded universal.

Result A: 2-level systems are universal.

Result B: 2 qubit gates are universal.

Result C: any Entangling gate + Single qubit gates is universal.

Result D: Clifford + 1 non Clifford gate is universal.

Result E Other universal gates.

$\{H, \Lambda(S)\}$, $\{H, T, \Lambda(X)\}$ $\{H, S, \Lambda^2(X)\}$.

Pf of A: Our gateset is $\{U^{ij}\}$ where U^{ij} acts as $U \in SU(2)$ on block spanned by $|i\rangle, |j\rangle$.

- $\mathcal{H} = \text{span}\{|0\rangle, |1\rangle, \cdots, |N-1\rangle\}$.
- we want to synthesize $U \in U(N)$
- first we show we can get from $|0\rangle$ to any $|\psi\rangle = a_0|0\rangle + \cdots + a_{N-1}|N-1\rangle$

using $N-1$ gates

$$U_1 : |0\rangle \mapsto a_0|0\rangle + b_0|1\rangle$$
$$U_2 : b_0|1\rangle \mapsto a_1|1\rangle + b_1|2\rangle$$
$$U_3 : b_1|2\rangle \mapsto a_2|2\rangle + b_2|3\rangle,$$
$$\vdots$$
$$U_{N-1} : b_{N-2}|N-2\rangle \mapsto a_{N-2}|N-2\rangle + a_{N-1}|N-1\rangle.$$

---

let $U_1 = W_0^{-1} U$, $U_1|0\rangle = |0\rangle$

next find W_1 s.t. $W_1|0\rangle = |0\rangle$
$W_1|1\rangle = U_1|1\rangle$

then recurse.

$$U = W_0 \cdots W_{N-3} W_{N-2}$$

total gates $\equiv (N-1) + (N-2) + \cdots + 2 + 1$

$$= \frac{1}{2} N(N-1)$$

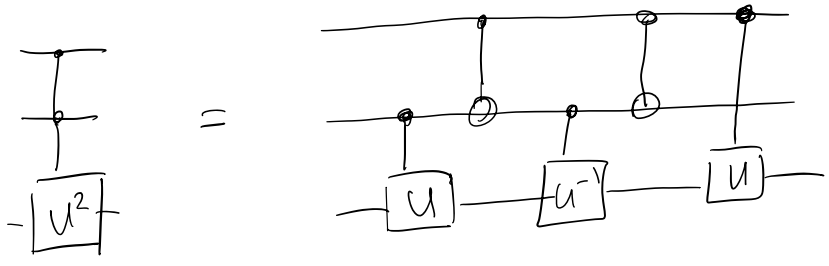
Pf of B. Suppose we want to apply V^{ij}

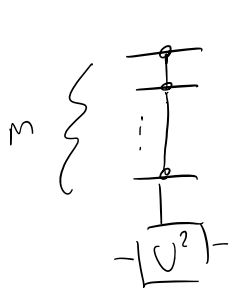
If we have a rev map Σ_{ij}: $|i\rangle \leftrightarrow |000\cdots0\rangle$, $|j\rangle \leftrightarrow |000\cdots1\rangle$, $|k\rangle \leftrightarrow |k\rangle$ $k \neq i,j$

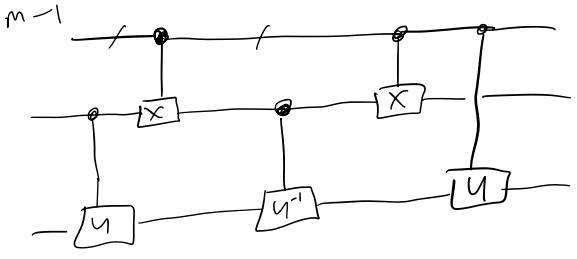
we apply V^{ij} via $\Sigma^{-1} \circ \Lambda^{n-1}(V) \circ \Sigma$

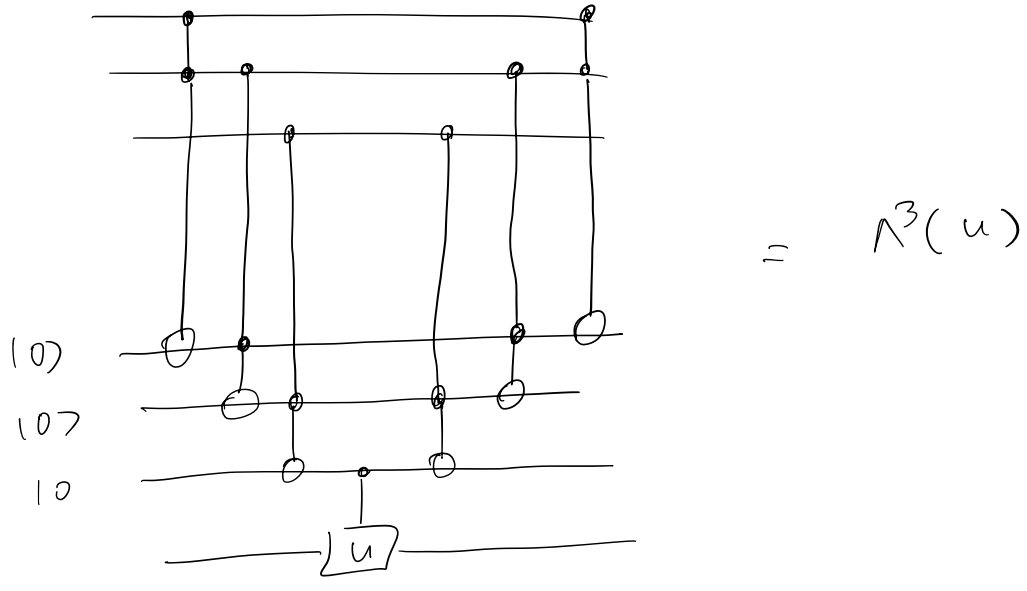
How do we get controlled $\Lambda^{n-1}(V)$ operations?

First note.









Method for proving universality for cont. gates.

Suppose we can apply e^{itH_1}, e^{isH_2}, $\forall s,t$.

$$\left(e^{itH_1/N} e^{itH_2/N}\right)^N = e^{i(tH_1+tH_2)} + O\left(\frac{t^2}{N}\right).$$

$$\left(e^{itH_1/N} e^{itH_2/N} e^{-itH_1/N} e^{-itH_2/N}\right)^{N^2} = e^{t^2[H_1,H_2]} + O\left(\frac{t^3}{N}\right).$$

- We define the Lie Algebra generated by A, B to be everything you can produce via linear combinations ($\alpha A + \beta B$, $\alpha, \beta \in \mathbb{R}$) and commutators $i[A,B]$.
- Gate set generated by $A = \{A_1, \ldots, A_k\}$.

$$L = \left\{ e^{it_m A_{i_{k_m}}} \cdots e^{it_1 A_{i_{k_1}}} : t_1 \ldots t_m \in \mathbb{R}, \; A_{i_1} \ldots A_{i_m} \in A \right\}.$$

- From L we produce the Lie alg. ℓ.

Thm. L is universal iff $\text{comm}(\ell) = \{I\}$.

Useful expressions

- Gate conjugation.

$$U e^{iHt} U^{\dagger} = e^{iUHU^{-1}}$$

- Baker Campbell Hausdorff

$$e^X e^Y = e^Z$$

$$Z = X + Y + \frac{1}{2}[X,Y] + \frac{1}{12}[X,[X,Y]] + \frac{1}{12}[Y,[Y,X]]$$

$$\Rightarrow e^{iA\Delta} e^{iB\Delta} = e^{i H_{eff} \Delta}$$

$$H_{eff} = A + B - \frac{i\Delta}{2N}[A,B] + O(t^2/N^2)$$

Thm. Any entangling gates + $SU(2)$ = universal.

pf outline. Enough to synthesize $\Lambda(Z)$.

$$\Lambda(Z) = e^{-i\pi/4}(I - Z_1 - Z_2 + Z_1 Z_2)$$

$\Rightarrow$ enough to capture $Z_1 Z_2$ Hamiltonian term.

U is entangling iff

$$U = V_1 \otimes V_2 \; e^{i(\alpha X_1 X_2 + \beta Y_1 Y_2 + \gamma Z_1 Z_2)} \; W_1 \otimes W_2$$

$Q(\alpha,\beta,\gamma)$ $\quad (\alpha,\beta,\gamma) \neq (0,0,0)$

we need to show algebra generated by.

$Q(\alpha,\beta,\alpha)$ + single qubit Hams

Contains. $Q(0,0,1)$.

main observation

$$(I \otimes X)\, Q(\alpha,\beta,\gamma)\, (I \otimes X)\, Q(\alpha,\beta,\gamma) = Q(2\alpha, 0, 0)$$

$$(I \otimes Y)\, Q(\alpha,\beta,\gamma)\, (I \otimes Z)\, Q(\alpha,\beta,\gamma) = Q(0, 2\beta, 0)$$

$$(I \otimes Y)\, Q(\alpha,\beta,\gamma)\, (I \otimes Z)\, Q(\alpha,\beta,\gamma) = Q(0, 0, 2\gamma)$$

Efficient q. compiling

the Solovay Kitaev Thm

Given $U \in SU(2)$, and any gateset G that is closed under inverses and $\varepsilon > 0$, $\exists$ ckt $\tilde{U}$ of size $\leq \text{polylog}(1/\varepsilon)$ from G which s.t.

$$\| U - \tilde{U} \|_\infty \leq \varepsilon.$$

Implies compilation of q. gates w. polylog overhead.

Pf. We say R is an ε-net in $U(N)$ if

$$\forall U \in U(N), \exists \tilde{U} \in R, \quad \| U - \tilde{U} \|_\infty \leq \varepsilon.$$

Idea $\forall$ R, ε-net in $U(N)$, $\exists$ R', ε'-net s.t. (R: inverse-closed) (R': inverse closed).

R' / (1) each gate of R' can be constructed from 5 unitaries in R

\ (2) $\varepsilon' \leq C \varepsilon^{3/2}$

Using this we prove the main Statement:

- Start w. ε_0-net R_0, $G \to R_0$ requires $L_0 = O(1)$ gates
  $\varepsilon_0 < 1/C^2$
- we invoke the recursion to get $\varepsilon_1 \le C\,\varepsilon_0^{3/2}$

using ckts of size $5L_0$.

$$C^2\varepsilon_k = \left(C^2\varepsilon_{k-1}\right)^{3/2} \Rightarrow \quad C^2\varepsilon_k = \left(C^2\varepsilon_0\right)^{(3/2)^k}$$

$$(3/2)^k = \frac{\ln\left(1/C^2\varepsilon_k\right)}{\ln\left(1/C^2\varepsilon_0\right)}$$

$$L_k = 5^k = \left((3/2)^k\right)^{\ln 5/\ln(3/2)}$$

$$= \left(\frac{\ln\left(1/C^2\varepsilon_k\right)}{\ln\left(1/C^2\varepsilon_0\right)}\right)^{\ln 5/\ln(3/2)}$$

$\Rightarrow$

$$\boxed{L_k \sim \ln\left(1/\varepsilon_k\right)^{3.97}}$$

$R \to R'$

R is ε-net $\Rightarrow$ For any $U \in SU(N)$

$\exists \tilde{U} \in R$ s.t $\| U - \tilde{U} \|_\infty \leq \varepsilon$.

$\updownarrow$

$\| U\tilde{U}^{-1} - I \|_\infty \leq \varepsilon$.

we find W using 4 elements in R s.t.

$\| U\tilde{U}^{-1} - W \|_\infty \leq \varepsilon'$, $\varepsilon' \leq C\varepsilon^{3/2}$

$\updownarrow$

$\| U - \tilde{U}W \|_\infty \leq \varepsilon'$ (5 elements).

$U\tilde{U}^{-1} = e^{iA}$

$\| U\tilde{U}^{-1} - I \| \leq \varepsilon \longrightarrow A = O(\varepsilon)$.

---

we can find $B, C = O(\varepsilon^{1/2})$ s.t

$[B, C] = -iA$

R, ε-net $\Rightarrow$ $\exists \tilde{B}, \tilde{C}$ s.t

$B - \tilde{B} = O(\varepsilon)$

$C - \tilde{C} = O(\varepsilon)$

set $W = \underbrace{e^{i\hat{B}} e^{i\tilde{C}} e^{-i\hat{B}} e^{-i\tilde{C}}}_{\text{size } 4} = I - [\hat{B}, \tilde{C}] + O(\varepsilon^{3/2})$

$$W = I - [B + O(\varepsilon), C + O(\varepsilon)] + O(\varepsilon^{3/2})$$

$$= I + iA + O(\varepsilon^{3/2}).$$

Classical cost.

At each iteration we call ε-accuracy procedure 3 times

$$t_{k+1} \sim 3 t_k$$

$$\Rightarrow \text{Cost}_m \sim 3^m \sim \gamma(\ln^{2.71} 1/\varepsilon)$$

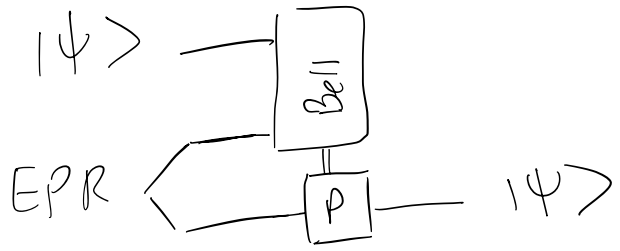
Gate teleportation

- We know Clifford gates are not universal.
- Moreover they are classically simulable starting from $|0^n\rangle$.
- Question: Can we perform universal Q.C. using Clifford gates + "magic" resourse states?

- This is important b.c:
  1. Clifford operations are easier to implement "e.g. can be implemented transversally on encoded qubits",
  2. Computation relies on copies of a fixed "magic" state.

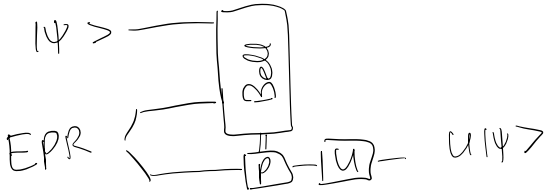
Protocol based on state teleportation

Recall :

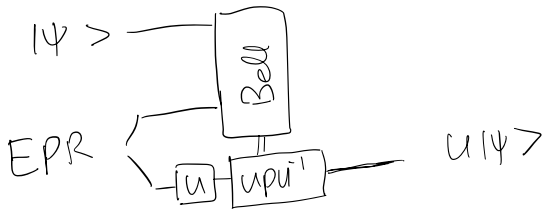


↳ Pauli Correction.

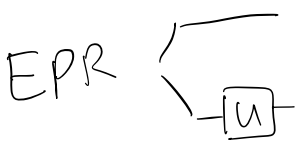
Now to apply U on |ψ>.

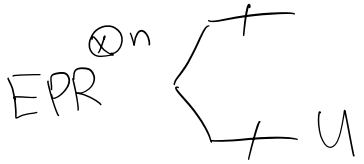


|||



MAGIC state





multiqubit U

Issue: UPU^{-1} may still be very complication.

If $U \in$ Clifford then $UPU^{-1} \in$ Pauli

The Clifford hierarchy:

let $C_0 = \mathcal{P}$

For $k \geq 1$ let

$$C_k = \{ U : UYU^{-1} \in C_{k-1}, \forall Y \in C_{k-1} \}.$$

Example: $C_1 =$ Clifford

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \in C_2$$

$$TXT^\dagger = XS \in C_1$$

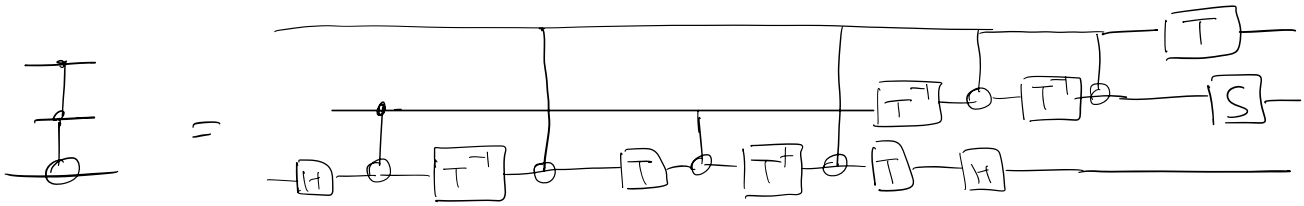
$$TZT^\dagger = Z \in C_1$$

Toffoli $\in C_2$

$$Tof(X_1)Tof = X_1 CNOT_{23}$$

$$Tof(Z_3)Tof = CZ_{12} Z_3.$$

Recall



If we choose $U = T$ we can perform universal Comp. using.

EPR + Clifford.

- Does C_k ever end? i.e., $\exists ? k_0$ s.t $\forall k \geq 0$, $C_k \subseteq C_{k_0}$?

- Answer: NO!

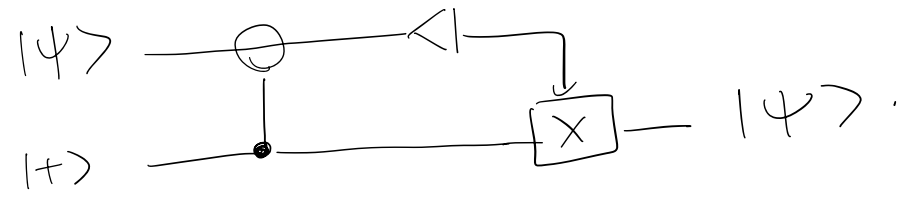
$$R_z(\theta) X R_z^{\dagger}(\theta) = X R_z(2\theta).$$

$R_z(2\theta) \in C_1$ iff, $2\theta = m\pi/4 \Rightarrow \theta = m\pi/8$

Using induction $R_z\left(\frac{m\pi}{2^{k+1}}\right) \in C_k / C_{k-1}$

$R_z(\theta) \notin C_k$ for any k if $\theta \neq m\pi/2^l$ for some l.

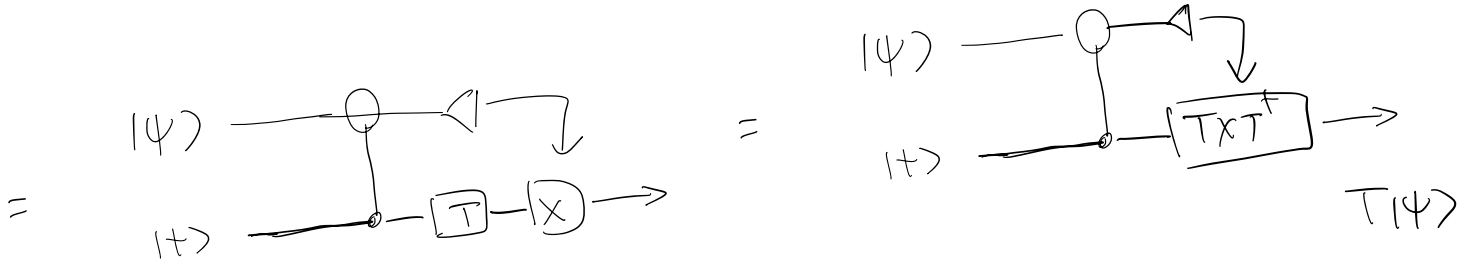
More Compressed Construction



$(|0\rangle + |1\rangle)|\psi\rangle \Rightarrow |0\rangle|\psi\rangle + |1\rangle X|\psi\rangle$

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

$+ (\beta|0\rangle + \alpha|1\rangle)|1\rangle$



$TXT^\dagger = S \in \text{Clifford}.$

Prop 13.4 (Gottesman's Book) Stab subgp.

let $|\phi\rangle = U|\psi\rangle$, $U \in C_k$, $|\psi\rangle \in$ Stab$_n$ w. $S \trianglelefteq \mathcal{P}_n$

then for all $M \in S$, $|\phi\rangle$ is the $+1$ eigenstate of

$V = UMU^{-1}$ (a). $V \in C_{k-1}$ (b). Furthermore $|\phi\rangle$ is

the only $+1$ eigenstate of all $\bar{V}$'s (c).

---

pf. (a) $V|\phi\rangle = UMU^\dagger(U|\psi\rangle)$

$= UM|\psi\rangle$

$= U|\psi\rangle = |\phi\rangle$

(b) $C_k = \{U : \forall W \in C_{k-1}, \; UWU^{-1} \in C_{k-1}\}$

$V = UMU^{-1} \in C_{k-1}$

$C_{k-1} \supseteq C_1 \quad C_k$

(c) $\Pi = \prod_V \frac{1}{2}(I + \bar{V})$

$= U \Pi_S U^{-1} \Rightarrow$

$\text{rank}(\Pi) = \text{rank}(\Pi_S) = 1$

Set $U = T \in C_3$, $|\psi\rangle = |+\rangle$, $S = \{I, X\}$

$\Rightarrow$ $|\phi\rangle = |T\rangle$ is stabilized by

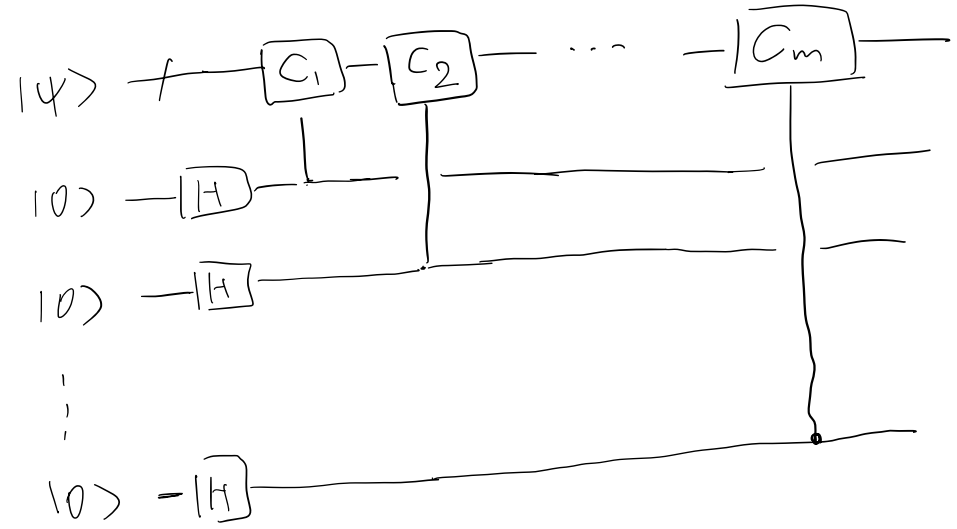
$$T X T^{-1} = \underbrace{X R_{\pi/4}^{-1}}_{C_T} \in \text{Clift}.$$

- $C_T = \frac{X+Y}{\sqrt{2}}$ also corresponds to an observable measuring C_T corresponds to the following POVM.

$$\Pi_+ = \frac{I + C_T}{2}, \quad \Pi_- = \frac{I - C_T}{2}$$

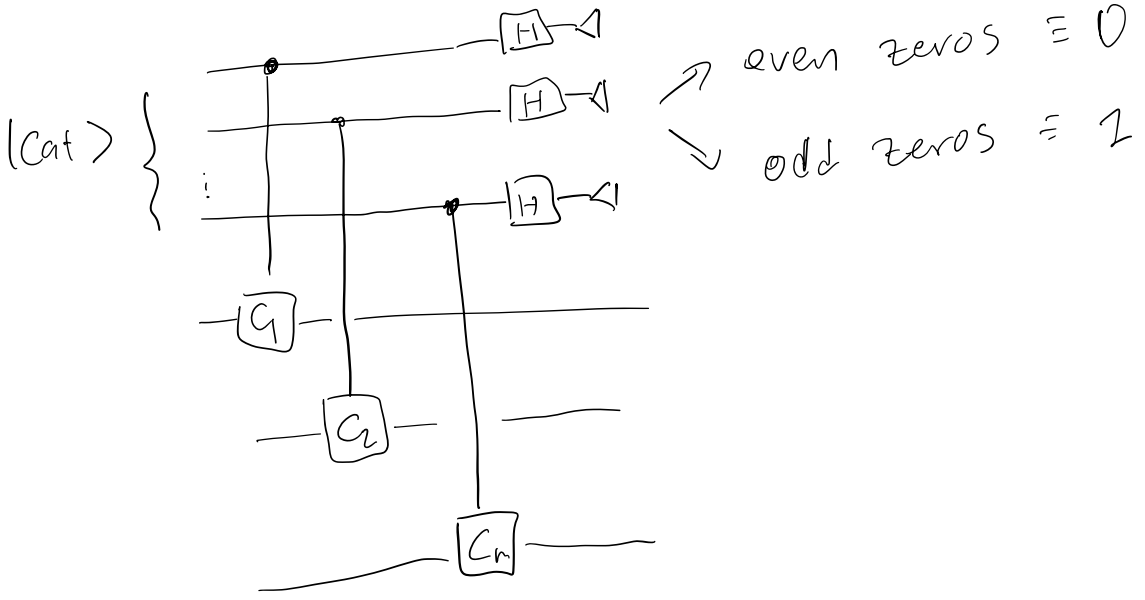
- We measure C_T and post select on $+$.

Implementation without Destruction



Issue: this implementation is not Fault tolerant.

Idea using CAT state.



Magic state distilation

Input: $\rho^{\otimes n}$, ρ bad quality magic state.

Allowed operations: Perfect Clifford + Pauli meas

Out put: $\sigma^{\otimes m}$ $m < n$, σ better quality magic.

assuming error on ρ is below a threshold.

Idea 1: 15 qubit code allows transversal implementation of T gate.

Error distance 3.

Procedure

① Start w. $T_\delta^{\otimes 15}$

where $T_\delta = (1-\delta)|T\rangle\langle T| + \delta \mathbb{6}$

② Create $|\bar{+}\rangle$ using Clifford gates.

③ use gate teleportation to apply $\bar{T}^\dagger_\delta$ transversally to $|\bar{+}\rangle$. => we get a noisy encoding of $|\bar{T}\rangle$ up to cliff correction

④ If you detect error, toss out the state, get back to 1.

maps $\delta \longrightarrow O(\delta^3)$.

$$T^{\otimes 15} |\bar{+}\rangle = \overline{T^{-1}} |\bar{+}\rangle .$$

$$|\bar{+}\rangle \propto \Pi_{15} |+\rangle^{\otimes 15}$$

$$\Rightarrow \overline{T^{-1}} |\bar{+}\rangle \propto T^{\otimes 15} \Pi_{15} |+\rangle^{\otimes 15}$$

$$= \Pi_{15} \left(T |+\rangle \right)^{\otimes 15}$$

Magic State distillation via Twirling

Let $|\psi_i\rangle$ be a basis for $\mathcal{H}$,

$\{U_a\}$ be a set of Clifford operations on $\mathcal{H}$

$U_a|\psi_i\rangle = \lambda_{a,i}|\psi_i\rangle$, let $\vec{v}_i = (\lambda_{a,i})$.

$v_i \neq v_j$ if $i \neq j$

"each $|\psi_i\rangle$ is uniquely identified w. eigenvalues.

let $U_a^{m_a} = \mathbb{I}$.

---

start w a mixed state, ρ

Proc:

for each a apply $U_a^{r_a}$ $r_a \in [0, m_a - 1]$ rand

Proc: $\rho \longmapsto \sum_j p_j |\psi_j\rangle\langle\psi_j|$ $\quad p_j = \langle\psi_j|\rho|\psi_j\rangle$

Pf. $\rho = \sum_{ij} \rho_{ij} |\psi_i\rangle\langle\psi_j|$.

$$U_a^{r_a} : \rho \mapsto \sum_{ij} \rho_{ij} \frac{1}{m_a} \sum_{r_a=0}^{m_a-1} \lambda_{a,i}^{r_a} \lambda_{a,j}^{* r_a} |\psi_i\rangle\langle\psi_j|$$

$\lambda_{a,i}$ are m_ath roots of unity.

$$\Rightarrow \lambda_{a,i} \neq \lambda_{a,i} \Rightarrow \frac{1}{m_a} \sum_{r_a=0}^{m_a-1} \lambda_{a,i} \lambda_{a,j}^{*} = 0$$

$$\lambda_{a,i} = \lambda_{a,i} \qquad = 1$$

Hence the effect $\Rightarrow$ making ρ block diag in the $|\psi_i\rangle$ basis.

---

e.g. $|T\rangle$ is the $+1$ eigen state of $U = XS^{-1}$

So if w.p. $\frac{1}{2}$ we apply U we get a mixture of. $T|\pm\rangle$

- Now suppose we have a code that allows us to implement Clifford operations transversally!
- We want to distill magic states which are Clifford eigenstates.
- One example is the 5-qubit code

we want to distill

$$|R\rangle = \cos\beta\,|0\rangle + e^{i\pi/4}\sin\beta\,|1\rangle$$

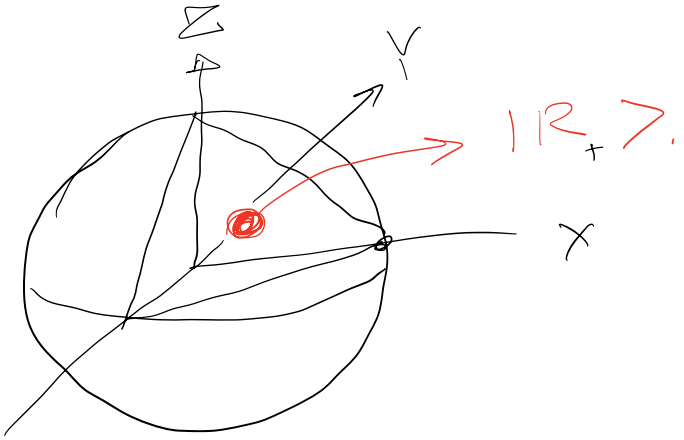
$$\cos(2\beta) = \frac{1}{\sqrt{3}}.$$

This is an eigenstate of

$$R : X \mapsto Z \mapsto Y \mapsto X.$$

for which we have a transversal implementation.

$$R = \frac{e^{i\pi/4}}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$$



There is a probabilistic procedure to transform $|R\rangle$ into a non clifford operation $\notin C_3$!

Distillation protocol.

① Start w. 5 imperfect $|R\rangle$ states

② Twirl R, i.e, apply I, R, R^2 w.p. $1/3$.

③ Measure the error syndrome of the 5-qubit code

if nonzero syndrome $\Rightarrow$ throw out restart.

④ Decode the 5-qubit code keeping only the decoded qubit

⑤ apply Y_H on the remaining qubit

We can show:

$$R|R_a\rangle = e^{i\pi/3 q}|R_a\rangle$$

$$\overline{R} = R^{\otimes 5}$$

$$\rho_{R_\pm} = \frac{1}{2}\left(1 \pm \frac{1}{\sqrt{3}}(X+Y+Z)\right)$$

$$\rho_{R_\pm}^{\otimes 5} = \frac{1}{2^5}\sum_{p\in P_5}\left(\pm 1/\sqrt{3}\right)^{|p|} p.$$

$$\Pi_5 = 1/2^4 \sum_{M\in S} M.$$

$$tr\left(\rho_{R_\pm}^{\otimes 5}\Pi_5\right) = \frac{1}{2^4}\sum_{M\in S}\left(\frac{\pm 1}{\sqrt{3}}\right)^{|M|}(\Delta M)$$

$\Delta M = \pm 1$, e.g. $\Delta\ -X^{\otimes 5} = -1$

$\Delta\ Z^{\otimes 5} = +1$

Main idea :

$$\rho_+ = \frac{1}{2}\left(I + \frac{1}{\sqrt{3}}(X+Y+Z)\right) = |R_+\rangle\langle R_+|$$

$$\rho_- = \frac{1}{2}\left(I - \frac{1}{\sqrt{3}}(X+Y+Z)\right) = |R_-\rangle\langle R_-|$$

$$F(\rho, R_+) = 1-\delta$$

Suppose. noisy $\rho = \frac{1}{2}\left(I + \vec{v}\cdot\vec{\sigma}\right)$.

after Twirling $\longrightarrow$ $\rho \mapsto \frac{1}{2}\left(I + (1-\delta)\rho_+ + \delta\rho_-\right)$.

$$\mathrm{tr}\left(\rho_{R_\pm}^{\otimes 5} \Pi_5 \right) = \frac{1}{16} A(\pm 1/\sqrt{3}) = 1/6$$

$$A(x) = 1 + 15 x^4$$

$$\bar{R} = e^{i\phi} R^{\otimes 5}$$

$$\bar{R}\, \Pi_5 |R_\pm\rangle^{\otimes 5} = e^{i\varphi} R^{\otimes 5} \Pi_5 |R_\pm\rangle^{\otimes 5}$$

$$= e^{i\varphi} \Pi_5 R^{\otimes 5} |R_\pm\rangle^{\otimes 5}$$

$$= e^{i\varphi} e^{\pm 5i\pi/3} \Pi_5 |R_\pm\rangle^{\otimes 5}$$

$\Rightarrow$ $|R_\pm\rangle^{\otimes 5}$ are eigenvectors of $\bar{R}$

w. eigenvalue $e^{i\phi \mp \pi/3}$

Choose $\phi = 0$

find: $|\overline{R_{\mp}}\rangle = \sqrt{6}\, \Pi_5 |R_\pm\rangle^{\otimes 5}$

$$Y_H |R_+\rangle = |R_-\rangle .$$

We finally get $O(p) \longrightarrow O(p^2)$ suppression.

Clifford gp and the Symplectic formalism

$$\mathbb{P}_n = \{ c\, P_1 \otimes \cdots \otimes P_n : P_j \in \{I, X, Y, Z\},\ c \in \{\pm 1, \pm i\} \}.$$

Any operator in $\mathbb{P}_n$ can be written as.

$$W(\alpha,\beta) = c\, X^{\alpha} Z^{\beta} \qquad \alpha,\beta \in \mathbb{F}_2^{\,n}$$

$$c = i^{\langle \alpha,\beta \rangle} \qquad \langle \alpha,\beta \rangle = \textstyle\sum_j \alpha_j \beta_j$$

$$\Rightarrow W(\alpha,\beta)^2 = I$$

$$W(\underbrace{\alpha,\beta}_{z})\, W(\underbrace{\alpha',\beta'}_{z'}) = (-1)^{\alpha\beta' + \beta\alpha'} W(\alpha',\beta')\, W(\alpha,\beta).$$

$$[z, z'] = \alpha\beta' + \beta\alpha' \Rightarrow \text{symplectic inner product.}$$

$$(z, z') = z^T J z', \qquad J = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}.$$

$$Sp(2n, \mathbb{F}_2) = \{ M \in \mathbb{F}_2^{\,2n \times 2n} : J = M^T J M \}.$$

---

we can show $W(\alpha) W(\beta) = i^{[\alpha,\beta]} W(\alpha+\beta)$.

Clifford $= \{ U : \forall P \in \mathbb{P}_n ,\ U P U^\dagger \in \mathbb{P}_n \}$.

$$\Rightarrow \quad U\, W(z)\, U^\dagger = c_U(z) \cdot W(\phi_U(z))$$

$W(z)^2 = \mathbb{I} \Longrightarrow$ $\boxed{c_U(z) \in \{\pm 1\}}$

$$(U W(z) U^\dagger)\cdot(U W(z') U^\dagger)$$

$$= c_U(z)\, c_U(z')\, W(\phi(z))\cdot W(\phi(z'))$$

$$= c_U(z)\, c_U(z')\, i^{[\phi(z),\phi(z')]}\, W(\phi(z)+\phi(z')).$$

$$= U W(z) W(z') U^\dagger = i^{[z,z']}\, c_U(z+z')\, W(\phi(z+z'))$$

$$\Rightarrow \boxed{\phi(z+z') = \phi(z) + \phi(z')} \quad \text{linear}$$

$$c_U(z)\cdot c_U(z') = c_U(z+z')\, i^{[z,z']-[\phi(z),\phi(z')]}.$$

we will see.

$$\Rightarrow \boxed{c_U(z) = (-1)^{[\lambda_U, z]}}, \quad \lambda_U \in \mathbb{F}_2^{2n}.$$

$$[W(z_1), W(z_2)] = 0 \iff [U W(z_1) U^\dagger, U W(z_2) U^\dagger] = 0$$

$$[z_1, z_2] = 0 \iff [\phi_U(z_1), \phi_U(z_2)] = 0$$

$$z_1^T J z_2 = 0 \iff z_1^T \phi_U^T J \phi_U z_2 = 0$$

$\forall\, z_1, z_2$

$$\Rightarrow \boxed{\phi_U^T J \phi_U = J}, \quad \phi \in Sp(2n, \mathbb{F}_2).$$

Generators of the Clifford gp

$$\text{Cliff} = \langle e^{i\theta}\mathbb{I},\ H_i,\ S_i,\ \text{CNOT}_{ij} \rangle$$

Symplectic rep.

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

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

$$\text{CNOT} = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right)$$

$HXH = Z$
$HZH = X$

$SXS^{-1} = XZ$
$SZS^{\dagger} = Z$

$X_1 \to X_1 X_2$
$X_2 \to X_2$
$Z_1 \to Z_1$
$Z_2 \to Z_1 Z_2$

$$U = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right), \quad U^T = \left(\begin{array}{c|c} A^T & C^T \\ \hline B^T & D^T \end{array}\right)$$

$$U^T J U = \begin{pmatrix} A^T & C^T \\ B^T & D^T \end{pmatrix} \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

$$= \begin{pmatrix} A^T & C^T \\ B^T & D^T \end{pmatrix} \begin{pmatrix} C & D \\ A & B \end{pmatrix}$$

$$= \begin{pmatrix} A^TC + C^TA & A^TD + C^TB \\ B^TC + D^TA & B^TD + D^TB \end{pmatrix}$$

$$\Rightarrow \quad A^T C + C^T A = B^T D + D^T B = 0$$
$$B^T C + D^T A = I$$

Gate	left action	right action
H_i	Switches ith row of $(A\|B)$ w. $(C\|D)$	Switches ith col of $(A\|C)$ w. $(B\|D)$
S_i	Adds the ith row of $(A\|B)$ to ith row of $(C\|D)$	Adds the ith Col of $(A\|C)$ to ith row of $(B\|D)$
$CNOT_{i,j}$	Adds the ith row of $(A\|B)$ to jth row of $(A\|B)$ Adds the ith row of $(C\|D)$ to jth row of $(C\|D)$	Adds the jth col of $(A\|C)$ to ith row of $(A\|C)$ Adds the jth Col of $(B\|D)$ to jth row of $(B\|D)$
$C\text{-}Z_{i,j}$	Adds the ith row of $(A\|B)$ to jth row of $(C\|D)$ Adds the ith row of $(C\|D)$ to jth row of $(A\|B)$	Adds the jth col of $(B\|D)$ to ith row of $(A\|C)$ Adds the jth Col of $(B\|D)$ to jth row of $(A\|C)$
$SWAP_{i,j}$	SWAP ith rows of A,B,C,D w. jth rows of A,B,C,D	SWAP ith cols of A,B,C,D w. jth cols of A,B,C,D

Procedure for decomposing $U \in \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$ into Clifford.

Short answer: Gaussian elimination.

① ϕ_U is full rank, $\Rightarrow \exists$ 1 in some col.

move this 1 to first row/col. (H, SWAP)

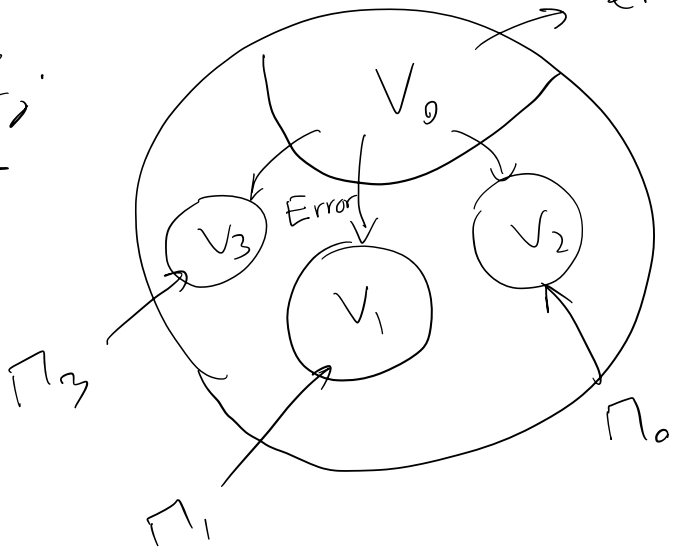
② use CNOT to remove any other 1's in the first col.

③ use CNOT to remove any other 1's in the first row

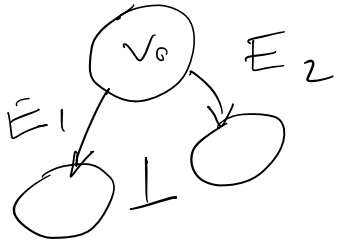
④ continue until you reach $\mathbb{I}$.

General Theory of Error-Correcting Codes

X_j, Y_j, Z_j



$V_0 \perp V_1 \perp V_2 \cdots$



Let $\mathcal{E}$ be our noise channel.

$|+\rangle, |-\rangle$
$|+\rangle, |0\rangle$

We define recovery map $\mathcal{R}$

(combining error detection and correction)

s.t.

if ρ is supported on V_0 then:

$$\boxed{\mathcal{R} \circ \mathcal{E}(\rho) = \rho} \quad (*)$$

In general $\mathcal{E}(\rho) = \sum_{j=1}^{m} E_j \rho E_j^\dagger$.

Knill Laflamme QECC conditions.

Let V_0 be a QECC and Π_0 be the projector onto it. Let $\mathcal{E}$ be a noise map $\rightsquigarrow$ Krause operations $\{E_1, \cdots, E_m\}$.

a recovery $\mathcal{R}$ map exists iff. $\forall i,j$ Π_0

$$(**) \qquad \forall j,k \quad \Pi_0 E_j^\dagger E_k \Pi_0 = \alpha_{j,k} \Pi_0$$

$$\alpha = [\alpha_{j,k}] \qquad \alpha^*_{j,k} = \alpha_{k,j}$$

Proof. $(**) \Longrightarrow (*)$

Since $\alpha^\dagger = \alpha$, then $\exists$ unitary U s.t.

$$U^\dagger \alpha U = d, \qquad d = \mathrm{diag}(d_1, \cdots)$$

Let $F_k := \sum_i U_{ik} E_i$

We know $\mathcal{E} = \sum_j E_j(\cdot) E_j^\dagger = \sum_j F_j(\cdot) F_j^\dagger$

Suppose E_j, E_k were unitary.

$E_j|\psi\rangle$

$E_k|\psi\rangle$

$$\Pi_0 E_j^\dagger E_k \Pi_0 = \Pi_0 \delta_{j,k}.$$

$$\Updownarrow$$

$$\forall |\psi\rangle \in V_0 \;, \quad \langle\psi| E_j^\dagger E_k |\psi\rangle = \delta_{j,k}.$$

$$M = U\sqrt{M^\dagger M}.$$

$$z = e^{i\varphi}\cdot|z|$$

$$= e^{i\varphi}\sqrt{z^* z}$$

Hence

$$\Pi_0 F_k^\dagger F_\ell \Pi_0 = \sum_{ij} u^\dagger_{ki} u_{j\ell} \Pi_0 E_i^\dagger E_j \Pi_0$$

$$= \sum_{ij} u^\dagger_{ki} \alpha_{ij} u_{j\ell} = \delta_{k,\ell} d_k$$

$$\boxed{\Pi_0 F_k^\dagger F_\ell \Pi_0 = d_k \delta_{\ell,k} \Pi_0} \quad (A)$$

$$\sum_k d_k = 1$$

Using polar decomposition:

$$F_k \Pi_0 = U_k \sqrt{\Pi_0 F_k^\dagger F_k \Pi_0}$$

$$= \sqrt{d_k}\, U_k \Pi_0$$

Let $\Pi_k = U_k \Pi_0 U_k^\dagger = \dfrac{F_k \Pi_0 U_k^\dagger}{\sqrt{d_k}}$

$(A) \Rightarrow$ $\Pi_k \Pi_\ell = \Pi_k^\dagger \Pi_\ell$

$$= \frac{U_k \Pi_0 F_k^\dagger F_\ell U_\ell^\dagger}{\sqrt{d_k d_\ell}}$$

$$= \delta_{\ell,k} \Pi_k .$$

Syndrome measurement is projective measurement.

given by Π_k.

Adding a dummy projector $\Rightarrow \sum_j \Pi_j = \mathbb{I}$.

$$\mathcal{R}(\sigma) = \sum_k U_k^\dagger \Pi_k \sigma \Pi_k U_k$$

Now suppose $\rho \in V_0$

we want to show

$$\mathcal{R} \circ \mathcal{E}(\rho) = \rho$$

First note $\rho \in V_0$

$$M_j = U_k^\dagger \Pi_k F_\ell \sqrt{\rho} = U_k^\dagger \Pi_k^\dagger F_\ell \Pi_0 \sqrt{\rho}$$

$$= U_k^\dagger \left(\frac{U_k \Pi_0 F_k^\dagger}{\sqrt{d_k}} \right) F_\ell \Pi_0 \sqrt{\rho}$$

$$= \frac{1}{\sqrt{d_k}} \Pi_0 F_k^\dagger F_\ell \Pi_0 \sqrt{\rho}$$

$$= \frac{1}{\sqrt{d_k}} d_k \delta_{\ell,k} \Pi_0 \sqrt{\rho} \qquad g \in V_0$$

$$= \sqrt{d_k}\, \delta_{\ell,k} \sqrt{\rho}$$

$\Downarrow$

$$\sum_j M_j^\dagger M_j.$$

$$\mathcal{E}(\rho) = \sum_\ell F_\ell \rho F_\ell^\dagger .$$

Therefore

$$\mathcal{R}(\mathcal{E}(\rho)) = \sum_{k,\ell} U_k^\dagger \Pi_k F_\ell \rho F_\ell^\dagger \Pi_k U_k$$

$$\sqrt{\rho}\sqrt{\rho}, \qquad \Pi_k = R_k R_k^\dagger$$

$$= \sum M_j M_j^\dagger$$

$$= \sum_{k,\ell} d_k \delta_{\ell,k} \rho = \rho .$$

Next we show

$$(*) \Rightarrow (**) .$$

$$\exists \mathcal{R} \quad \text{s.t} \quad \forall \rho \in V_0 , \quad \mathcal{R} \circ \mathcal{E}(\rho) = \rho$$

Hence, $\forall \sigma$

$$\mathcal{R} \circ \mathcal{E}(\Pi_0 \sigma \Pi_0) \propto \Pi_0 \sigma \Pi_0$$

linearity $\Rightarrow$

$$\mathcal{R} \circ \mathcal{E}(\Pi_0 \sigma \Pi_0) = c\, \Pi_0 \sigma \Pi_0 .$$

Let $\mathcal{R} = \sum_j R_j (\cdot) R_j^\dagger$

$\Rightarrow$

$$\sum_{j,k} R_j E_k (\Pi_0 \sigma \Pi_0) E_k^\dagger R_j^\dagger = c\, \Pi_0 \sigma \Pi_0$$

let $\mathcal{E}_1$ correspond to $R_j E_i$

$\mathcal{E}_2$ correspond to $\sqrt{c}\,\Pi_0$

$\mathcal{E}_1 \equiv \mathcal{E}_2$ therefore $\Rightarrow$ $u_{jk} R_j E_k = \sqrt{c}\,\Pi_0$

$$R_k E_i \Pi_0 = C_{ki} \Pi_0$$

$$\Rightarrow \quad \Pi_0 C^*_{ki} = \Pi_0 E_i^\dagger R_k^\dagger$$

$$\Rightarrow \quad \sum_k \Pi_0 E_j R_k^\dagger R_k E_l \Pi_0 = \sum_k C^*_{jk} C_{kl} \Pi_0$$

$$\Rightarrow \quad \Pi_0 E_j E_l \Pi_0 = \alpha_{jl} \Pi_0$$

Corrolary

Suppose $\mathcal{R}$ can correct set of errors- $\{E_j\}$

then $\mathcal{R}$ can correct a set $\{F_j\}$

$$F_j = \sum_l m_{lj} E_l.$$

Pf.

$$\Pi_0 E_i E_j^\dagger \Pi_0 = \alpha_{ij} \Pi_0$$

w.l.o.g. α is diagonal.

$\mathcal{R}$ has elements $V_k^\dagger \Pi_k$

then $\forall \rho \in V_0$,

$$V_k^\dagger \Pi_k E_i \sqrt{\rho} = \delta_{ki} \sqrt{\alpha_{k,k}} \sqrt{\rho}$$

$$F_j = \sum_i m_{ji} E_i$$

$$V_k^\dagger \Pi_k F_j \sqrt{\rho} = \sum_i m_{ji} \delta_{ki} \sqrt{\alpha_{kk}} \sqrt{\rho}$$

$$= m_{jk} \sqrt{\alpha_{kk}} \sqrt{\rho}$$

$$\Rightarrow \mathcal{R}(\mathcal{F}(\rho)) = \sum_{k,j} V_k \Pi_k F_j \rho F_j^\dagger \Pi_k V_k$$

$$= \sum_{k,j} |m_{jk}|^2 \alpha_{k,k} \rho \propto \rho.$$

Degenerate Codes

- If $\text{rank}(\alpha) = |\mathcal{E}|$ then we can go to a proper error basis where $\alpha \longmapsto I$
- If $\{E_i\}$ are linearly dep α is necessarily singular $(\text{rank}(\alpha) < |\mathcal{E}|)$.
- If we choose a minimal set $\{E'_i\}$ consisting only of lin indep terms, α may still be singular.

"In this case we call the code degenerate"

- For a degenerate code two different errors may lead to the same syndrome.
- Example: Shor's 9 qubit code

$Z_1, Z_2, Z_3 \longrightarrow$ lead to the same Synd.

Distance of a code

We consider set of errors to be t-qubit operators-
(Pauli spectrum of wt $\leq t$).

Def. The distance for a code C is the minimum d
s.t. $\exists F$, $wt(F) = d$:
$\langle\psi|F|\phi\rangle \neq C(F)\langle\psi|\phi\rangle$.

Thm. Distance d codes corrects errors of wt $\lfloor \frac{d-1}{2} \rfloor$

pf. If $wt.(E_a) \leq \lfloor \frac{d-1}{2} \rfloor \quad \forall a$

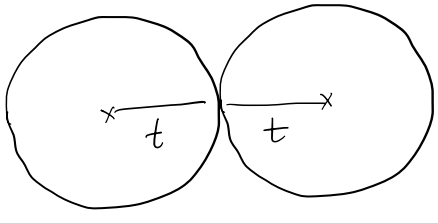
then $wt(E_a^\dagger E_b) \leq d-1$

$$\Rightarrow \langle\psi|E_a^\dagger E_b|\phi\rangle = C_{ab}\langle\psi|\phi\rangle.$$

Equivalent formulation:

If code can correct up to $wt(f)$ errors

then $d = 2t+1$.



Three properties of a QECC:

A code $C \subseteq (\mathbb{C}^2)^{\otimes n}$ is $[[n, k, d]]$ if it encodes k logical qubits. w. distance d.

Detecting errors.

An error E is detectable if

$$\Pi_0 E \Pi_0 = \alpha(E)\, \Pi_0$$

So if $|\psi\rangle \in V_0$ gets mapped to $E|\psi\rangle$

then $\Pi_0 E|\psi\rangle = \alpha(E)|\psi\rangle$.

in particular $\forall\, |\psi\rangle, |\phi\rangle \in V_0$

$$\langle\phi| E |\psi\rangle = \alpha(E)\, \langle\phi|\psi\rangle$$

if $\alpha(E) = 0 \implies E|\psi\rangle \perp V_0 \implies$ detectable

if $\alpha(E) \neq 0 \implies \overline{E} = \alpha(E)\, \mathbb{I}_{V_0}$ acts trivially

Review of Stabilizer Formalism

Thm. $|S| = 2^r \Rightarrow \dim(V_S) = 2^{n-r}$

Logical operations

Elements of the stabilizer gp S

act as $\mathbb{I}$ on the code space.

$$N(S) = \{ N \in \mathbb{P}_n \mid \forall Q \in S, NQN \in S \}.$$

Since $\forall N \in \mathbb{P}_n$, $[N, Q] = 0$ or $\{N, Q\} = 0$

$$\Rightarrow N(S) = \{ N \in \mathbb{P}_n \mid \forall Q \in S, [Q, N] = 0 \}$$

the same as centralizer

$$N(S) \supseteq S, \pm iS,$$

Logical operations correspond to $N(S)/S$.

i.e. nontrivial maps that map states within the code space to each other.

$A \in N(S)$, $S = \langle g_1, \ldots, g_r \rangle$

$\Updownarrow$

$[A, g_i] = 0, \forall i$

$A \in \mathbb{P}_n$, $A \notin N(S)$

$\Downarrow$

A is detectable

Thm. The set of undetectable errors correspond to $N(S) \setminus S$.

Furthermore. $d = \min_{P \in N(S) \setminus S} wt(P)$.

Pf. Set of undetectable Pauli errors is

$\{Q \mid [Q, M] = 0, \forall M \in S\}$.

This includes both S and things other than S.

$N(S) \setminus S$. $\Rightarrow$ undetectable nontrivial error.

Suppose $E \in N(S) \setminus S$ then

$\Pi_0 E \Pi_0 = E \Pi_0 \propto \Pi_0$

More carefully:

$E \in N(S) \setminus S \Rightarrow E \notin S \Rightarrow \exists |\phi\rangle \in V_0$ s.t.

$|\psi\rangle = E|\phi\rangle \neq |\phi\rangle$.

$\forall M \in S$, $M(E|\phi\rangle) = E(M|\phi\rangle)$ ← since $E \in N(S) \Rightarrow |\psi\rangle \in V_0$

$= (E|\phi\rangle)$ → $\alpha(E)$

Suppose as a way of contradiction E was detectable.

$\langle\psi|E|\phi\rangle = 1 = \frac{1}{\langle\psi|\phi\rangle}\langle\psi|\phi\rangle$

However $\langle\phi|E|\phi\rangle = (\langle\phi|\psi\rangle)\langle\phi|\phi\rangle$. ← $\alpha(E)$

$\Rightarrow$ if E was detectable then

$|\langle\psi|\phi\rangle| = 1 \Rightarrow E|\phi\rangle = e^{i\theta}|\phi\rangle$

Detectability $\Rightarrow \forall |\lambda\rangle \in V_0$, $\langle\lambda|E|\lambda\rangle = e^{i\theta}\langle\lambda|\lambda\rangle$.

$|\lambda\rangle =$

$E^2|\lambda\rangle = e^{i\theta}E|\lambda\rangle$ $\Rightarrow$ $E|\lambda\rangle = e^{i\theta}|\lambda\rangle$ $\forall |\lambda\rangle \in V_0$

$\Rightarrow e^{i\theta} = e^{-i\theta}$

$\Rightarrow 2\theta = 2\pi \Rightarrow \theta = \pi$

$\Rightarrow E \in S$. Contradiction.

Corrolary The stabilizer code S corrects $\mathcal{E} \subseteq \mathbb{P}_n$ iff

$E^\dagger F \notin N(S) \setminus S$, $\forall E, F \in \mathcal{E}$.

Degeneracy:

$C_{ab} = 0$ if $E_a^\dagger E_b \notin N(S)$

$C_{ab} = 1$ if $E_a^\dagger E_b \in S$

Since the set of Pauli operators are lin indep.

Cod is degenerate iff C is not max rank.

Suppose $E_a^\dagger E_b \in S$ then for any F,

$E_a^\dagger F \in S \iff E_b^\dagger F \in S \Rightarrow$ row a = row b

$\Rightarrow$ degenerate.

---

if $E_a^\dagger E_b \notin S \Rightarrow E_a^\dagger F$ & $E_b^\dagger F$ cannot simultaneously $\in S$

Hence rows a and b cannot simultaneously have ones in the same location.

This implies.

---

prop. A stab. code is degenerate iff

$\exists E_1, E_2 \in \mathcal{E}$ s.t. $E_1^\dagger E_2 \in S$.

Def. A stabilizer code w. distance d is degenerate

if $\exists M \in S \setminus I$ $\quad wt(M) < d$.

Degeneracy only involves operators of weight $\leq d$. $M \sim I$ already implies degeneracy

E.g. 9-qubit code has $d = 3$ and generators wt < 3 (e.g $Z_1 Z_2$)

Logical operations

set of operations that preserve V_0.

Since $V_0 = V_S$ so set of operations preserving V_0 is $N(S)$.

P preserves $V_0 \iff P \in N(S)$.

$S \iff I$

$N(S)/S$ is the set of inequiv logical operations.

S has $n-k$ independent generators.

$\dim \mathbb{P}_n = 2n$

$\dim N(S) = 2n - (n-k) = n+k$

$\dim N(S)/S = (n+k) - (n-k) = 2k$

$N(S)/S \cong \mathbb{P}_k$.

Error syndrome

Let $S = \langle M_1, \dots, M_r \rangle$. Let $|\psi\rangle$ be a joint eigen vector of $M_1 \cdots M_r$. The error syndrome for $|\psi\rangle$ is an r-bit string $\lambda_\psi \in \mathbb{Z}_2^r$ s.t.

$$\lambda_\psi(j) = \begin{cases} 1 & M_j|\psi\rangle = -|\psi\rangle \\ 0 & M_j|\psi\rangle = +|\psi\rangle \end{cases}$$

Now suppose $|\phi\rangle \in V_0$ is a code word. We define

$$\sigma : \mathbb{P}_n \longrightarrow \mathbb{Z}_2^r \quad \text{s.t.} \quad \sigma_j(E) = c(M_j, E)$$

where $c(A,B) = \begin{cases} 1 & [A,B] = 0 \\ 0 & \{A,B\} = 0 \end{cases}$

$A, B \in \mathbb{P}_n$

Properties

(a) $c(P_1 P_2, Q) = c(P_1, Q) + c(P_2, Q)$

(b) $c(P, Q) = c(Q, P)$

(c) $\sigma(EF) = \sigma(E) + \sigma(F)$.

Proposition $E, F \in \mathbb{P}_n$, S a stabilizer gp. Then E and F are in the same coset of $N(S)$ iff E and F have the same error syndrome.

Pf. $\Rightarrow$: If E and F are within the same coset,

then $F = EN$, where $N \in N(S)$.

let $M \in S$ then $c(F, M) = c(E, M) + c(N, M)$, with $c(N, M) = 0$

therefore E and F correspond to the same syndrome.

$\Leftarrow$: Suppose E, F have the same syndrome.

let $N = E^{\dagger}F$, if $\sigma(E) = \sigma(F)$ then $c(N, M) = 0$ $\forall M \in S$.

$\Downarrow$

$N \in N(S)$.

$$c(N, M) = c(E, M) + c(F, M)$$

$$= 0$$

Full Hilbert space can be divided into $orth$ pieces corresponding to different syndromes.

The whole $\mathbb{P}_n$ can be partitioned into 2^r different cosets of $N(S)$.

Prop: $|N(S)| = 4 \cdot 2^{n+k}$

Pf. $2^r \cdot |N(S)| = 4 \cdot 4^n \Rightarrow |N(S)| = 4 \cdot 2^{2n-r}$

$= 4 \cdot 2^{n+k}$.

Prop Suppose $N_1, N_2 \in N(S)$. Then N_1, N_2 are in the same coset of S iff $N_1|\psi\rangle = N_2|\psi\rangle$, $\forall |\psi\rangle \in V_0$.

Pf.

$$N_1|\psi\rangle = N_2|\psi\rangle \quad \forall\ |\psi\rangle \in V_0$$

$$\Updownarrow$$

$$M|\psi\rangle = |\psi\rangle, \quad \forall\ |\psi\rangle \in V_0$$

$$M = N_1^\dagger N_2$$

$$\Updownarrow$$

$$M \in S \iff N_1 = N_2 M \text{ for some } M \in S.$$

$N \in N(S) \Rightarrow N|\psi\rangle \in V_0, \ \forall |\psi\rangle \in V_0$

Hence N is a logical operation.

N and NM are the same logical op. $\forall M \in S$.

Hence $N(S)/S$ corresponds to the set of distinct logical op-

---

Thm. $N(S)/S \cong P_k$ $\quad \dim(V_0) = 2^k$.

Thm. If S is non-deg stab code we get distinct error syndromes. If S is deg, $\delta(E) = \delta(F)$ iff $\hat{E}^\dagger \hat{F} \in \hat{S}$

($\hat{A} = A$, phase tossed out)

Pf. Two errors $E \neq F \in \mathcal{E}$ have the same syndrome

iff $E^\dagger F \in N(S)$. Since they are correctable,

$\hat{E}^\dagger \hat{F} \notin \hat{N}(S) \setminus \hat{S}$ so

$E^\dagger F \in N(S)$ iff $\hat{E}^\dagger \hat{F} \in S$.

So $\sigma(E) = \sigma(F)$ iff $\hat{E}^\dagger \hat{F} \in \hat{S}$ •

⇓ degenerate.

S	$\bar{X}$	FS	$F\bar{X}$
$\bar{Z}$	$\bar{Y}$	$F\bar{Z}$	$F\bar{Y}$
ES	$E\bar{X}$	GS	$G\bar{X}$
$E\bar{Z}$	$E\bar{Y}$	$G\bar{Z}$	$G\bar{Y}$

synd 00 I

01 E

10 F

10 G

Back to the symplectic formalism:

$$W(z) = i^{-\langle x,\alpha\rangle} X^x Z^\alpha, \qquad z = (x,\alpha) \in \mathbb{F}_2^{2n}$$

Pauli notation	Symplectic notation
$P \in \mathcal{P}_n$	$W(z_P)$, $z_P \in \mathbb{F}_2^{2n}$
Mult. $P.Q$	Addition $z_P + z_Q$
$c[P,Q]$	$[z_P, z_Q]$.
phase	no equivalent
Stabilizer S	$S \subseteq S^\perp$ Weakly self-dual subspace
	$S \subseteq \mathbb{F}_2^{2n}$ Lagrangian
$N(S)$	Dual $S^\perp$ wrt $[\cdot,\cdot]$.
generators for S	basis for S.

Eg five qubit code

	1 0 0 1 0	0 1 1 0 0
	0 1 0 0 1	0 0 1 1 0
	1 0 1 0 0	0 0 0 1 1
	0 1 0 1 0	1 0 0 0 1
$\bar{X}$	1 1 1 1 1	0 0 0 0 0
$\bar{Z}$	0 0 0 0 0	1 1 1 1 1

Def. Let $V \subseteq \mathbb{F}_2^{2n}$ be a lin subspace

$$V^\perp = \{ w \in \mathbb{F}_2^{2n} \mid [z, w] = 0, \ \forall z \in V \}.$$

- V is self dual if $V = V^\perp$
- V is weakly self dual if $V \subseteq V^\perp$

- Lin alg lemma: let $P_1, \dots, P_m$ be indep n-qubit Paulis

$$s \in \mathbb{F}_2^m. \quad \exists Q \in \mathcal{P}_n \text{ s.t.}$$

$$\forall j \quad c(P_j, Q) = s_j.$$

There are 2^{2n-m} such Paulis.

Pf. Convert to Lin system of Equations.

$$[V_{P_i}, V_Q] = s_i \qquad m \text{ eqs in } 2n \text{ dim}$$

the dim of space of sol $= 2n - m$.

Corollary. Let S be a stab w. gen $\langle M_1, \dots, M_r \rangle$

then for any err syndrome s, $\exists P \in \mathcal{P}_n$ s.t.

$$\sigma(P) = s.$$

Consequences

$N(S)/S \cong \mathbb{P}_k$

Pf. For pauli gp $\mathbb{P}_k$ we have

$$c[X_i, X_j] = c[Z_i, Z_j] = 0$$

$$c(X_i, Z_j) = \delta_{ij}$$

If we can find $\bar{X}_j, \bar{Z}_k$ w. commutation relations isomorphic to $N(S)/S$.

$$N(S) \longleftrightarrow S^\perp$$

$$N(S)/S \longleftrightarrow S^\perp \setminus S$$

$$\dim(S^\perp) = 2^n - r = n + k$$

$$\dim(S^\perp \setminus S) = n - r + k = 2k = |\mathbb{P}_k|.$$

$$S^\perp = \{ V \mid [V, w] = 0 \ , \forall w \in S \}.$$

$$S^\perp \setminus S = \{ V \notin S \mid [V, w] = 0 \ , \forall w \in S. \}.$$

$$\Rightarrow S^\perp / S \cong \mathbb{F}_2^{2k}.$$

Goal find $x_j, z_j \in S^\perp \setminus S$

s.t $[x_j, x_j] = [z_j, z_j] = 0$

$$[x_j, z_k] = \delta_{jk}.$$

It is enough to find generators.

We proceed inductively

Suppose we have successfully established $\bar{X}_i, \bar{Z}_j$ up to a certain point and we want to add one more

using Corr * we can always find such element.

we need to verify it can be indep.

Since they have distinct Commutation relationship.

every new element must be indep of others.

Thm. $S = S(V(S))$

If $M \in S$, then $M|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in V(S)$.

So $S \subseteq S(V(S))$.

Next we show if $N \notin S$ then $N \notin S(V(S))$.

If $N \notin N(S)$ then $N|\psi\rangle$ for any $|\psi\rangle \in V$ has a

diff eigenvalue for some $M \in S \Rightarrow$ $N|\psi\rangle \perp V$.

$\Rightarrow$ $N|\psi\rangle \notin S(V(S))$.

Classical error correction

Def. A classical ECC $(e, \mathcal{E})$ is a map

$e : [K] \to [N]$, correctable errors $\mathcal{E}$

$(\mathcal{E} : [N] \to [M])$

s.t. $\exists$ a map $d : [M] \to [K]$ s.t.

$\forall E \in \mathcal{E}, \forall x \in [K]$

$$d(E(e(x))) = x$$

d decoder

$\mathcal{E}$ error

e encoder

Distance: $\min \{ wt(E) \mid \exists x \neq y \in C, E(x) = y \}$.

A classical code w. dist d.

① correct up to $\lfloor (d-1)/2 \rfloor$ coordinates.

② detect up to $d-1$ coordinates

Linear codes

$$\mathbb{Z}_N = \mathbb{Z}_2^n$$

Def. An ECC $C \subseteq \mathbb{Z}_2^n$ is a lin code if

$$\forall\, x, y \in C \Rightarrow x+y \in C.$$

$$C = \langle x_1, \dots, x_k \rangle \Rightarrow |C| = ?^k$$

Def. Generator matrix $G = \left(\begin{array}{c} \vdots \\ \hline x_i \\ \hline \vdots \end{array} \right)$

Prop. $C \subseteq \mathbb{Z}_2^n$ lin code w. k encoded bits.

and gen G, $e : v \in \mathbb{Z}_2^k \mapsto G^T v \in \mathbb{Z}_2^n$

is the encoder.

$$x \in C \iff x = G^T v, \exists\, v \in \mathbb{Z}_2^k.$$

Def. Let C be a lin code w. gen G

Parity check matrix $H = \left(\begin{array}{c} y_1 \\ \hline \vdots \\ \hline y_{n-k} \end{array}\right)$, $Gy_i = 0 \ \forall i$

$\{y_i\}$ max lin indep set w. this property.

Thm. If C has k encoded bits and n physical bits.

$G \in \mathbb{Z}_2^{k \times n}$, $H \in \mathbb{Z}_2^{(n-k) \times n}$ s.t.

$$GH^T = HG^T = 0$$

pf. The only nontrivial part is $n-k$ rows for H.

the dimension of the sol space of $G^T\lambda = 0$

is $n-k$. ← k lin indep eq.

Error model.

Bit flip e. $x \mapsto x+e$

$wt(e)$

Parity Check matrix $H(x+e) = Hx + He$

$= HG^T v + He$

$= He$

Def. Error syndrome for C is He.

Thm. Let C be a lin code w. H parity check correcting $\mathcal{E} \subseteq \mathbb{Z}_2^n$.

Define a stab w. symplectic rep $(0 \mid H)$.

Then S corrects $\{ W(e,0) \mid e \in \mathcal{E} \}$

rows of G are logical Pauli's in $N(S)/S$.

Distance:

Thm. $d = \min \{ wt(e) \mid e \in C, e \neq 0 \}$.

Pf $d = \min \{ wt\, e \mid x \neq y \in C, x + e = y \}$

$\downarrow$

$e = x + y$

Thm. C corrects $\mathcal{E}$ iff

$e + f \notin C \quad \forall e \neq f \in \mathcal{E}$.

Equivalently, $He \neq Hf \quad \forall e \neq f . e \in \mathcal{E}$

(all errors have their unique syndrome)

Pf. If error syndromes are unique

then we can invert He to find e

$$x + e + e = x.$$

If $e + f \in C$ then $H(e+f) = 0$

$$\downarrow$$

$$H(e) = H(f).$$

Conversely if $e + f \notin C$ then $H_C(e+f) \neq 0$.

$(\ker(H) = C)$. incomplete

Classical	Quantum
Error $e \in \mathbb{F}_2^n$	Pauli $E \in \mathbb{P}_n$
Syndrome He	$s(E)$, $g_i E = (-1)^{s_i(E)} E g_i$
Code words C $C = \ker(H) = \mathrm{Im}(G)$	$+1$ eigenstate of S $\ker(\Pi_0)$
Indistinguishable if $e - f \in C$	indistinguishable if $E^\dagger F \in N(S)$
trivial diff $e - f = 0$	$E^\dagger F \in S$
$C \setminus \{0\}$	$N(S) \setminus S$
No degeneracy	degeneracy $\mathrm{wt}(M) < d$, $M \in S$

Example Hamming codes

$0 \to 000$, $1 \to 111$ Rep code is linear

$C = \{000, 111\} = \langle 111 \rangle$

$G = (1\ 1\ 1)$, $H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$

d- rep code $[d, 1, d]$

Observation: every col of H is distinct.

$d = 4$

$(1\ 1\ 1\ 1)$

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

Hamming code $[2^r - 1, 2^r - r - 1, 3]$

$H = \underbrace{\begin{pmatrix} \text{all distinct} \\ r \text{ bit str.} \\ -0 \end{pmatrix}}_{2^r - 1} r$

The CSS code:

Calderbank, Shor, Steane

Recall linear codes are special cases of Stabilizer codes

Bit flip

$$S = (\ O \mid H\ )$$

to correct $\{(e \mid 0) \mid e \in \mathcal{E}\}$

then $x \in C$ iff $|x\rangle \in V_0$

Phase flip

$$S = (\ H \mid O\ )$$

to correct $\{(0 \mid e) \mid e \in \mathcal{E}\}$

then $x \in C$ iff $H^{\otimes n}|x\rangle \in V_0$

In CSS codes we combine both.

Def. C is a CSS code if there exists a choice of generators for Stabilizers of the form

$$\left(\begin{array}{c|c} O & A \\ \hline B & O \end{array}\right)$$

A: $r_1 \times n$ Z generators

B: $r_2 \times n$ X generators

E.g. 7 qubit code

$$\begin{array}{ccccccc}
Z & Z & Z & Z & I & I & I \\
Z & Z & I & I & Z & Z & I \\
Z & I & Z & I & Z & I & Z \\
X & X & X & X & I & I & I \\
X & X & I & I & X & X & I \\
X & I & X & I & X & I & X
\end{array}$$

$$\begin{array}{cccccccc}
\bar{X} & X & X & X & X & X & X & X \\
\bar{Z} & Z & Z & Z & Z & Z & Z & Z
\end{array}$$

$$S = \left(\begin{array}{c|c} O & H \\ \hline H & O \end{array}\right)$$

H: correct bit flip, Hamming code $[7, 4, 3]$

H: correct phase flip

$[[7, 1, 3]]$

$4 + 4 - 7 = 1$

Theorem. $C_1 = [n, k_1, d_1]$, H_1

$C_2 = [n, k_2, d_2]$, H_2

suppose $C_1^{\perp} \subseteq C_2$.

Then $S = \left(\begin{array}{c|c} 0 & H_1 \\ H_2 & 0 \end{array}\right)$

is an $[[n, k, d]]$ q. code w.

$k = k_1 + k_2 - n$,

and $d \geq \min\{d_1, d_2\}$

Note $C_1^{\perp} \subseteq C_2 \iff C_2^{\perp} \subseteq C_1$

$n > k_1 + k_2$ is impossible b.c.

$\dim(C_1^{\perp}) = n - k_1$

$\dim(C_2) \geq \dim(C_1^{\perp}) \Rightarrow k_2 \geq n - k_1$

$\Rightarrow \boxed{n \leq k_1 + k_2}$

Pf. We first check X generators commute w. Z generators. Any x generator is of the form $(x|0)$, $x \in C_2^{\perp}$ (row of the parity check matrix) $H_1 G = 0$

Any Z generator has the form $(0|z)$, $z \in C_1^{\perp}$

$$[W(x,0), W(0|z)] = \langle x, z \rangle = 0$$

$x \in C_1^{\perp}$, $z \in C_2^{\perp}$

$\Rightarrow$ if $z \in C_1^{\perp} \Rightarrow z \in (C_2^{\perp})^{\perp} = C_2$

then $C_1^{\perp} \subseteq C_2$

Next we derive the parameters

H_1 has $n - k_1$ rows, H_2 has $n - k_2$ rows

So S has $2n - k_1 - k_2$ rows.

So $\dim(V_S) = n - (2n - k_1 - k_2) = k_1 + k_2 - n$

Code can detect up to $d_1 - 1$ bit flip errors and $d_2 - 1$ phase flip errors.

So distance cannot be smaller than $\min\{d_1, d_2\}$.

Codewords for the CSS code

$$\Pi_0 = \Pi_2 \cdot \Pi_1$$

Π_1 projects onto the subspace spanned by C_1.

$$\Pi_2 = \frac{1}{2^{n-k_2}} \sum_{x \in C_2^\perp} W(x,0).$$

To construct code words we take $x \in C_1$

and apply

$$\Pi_2 |x\rangle = \frac{1}{2^{n-k_2}} \sum_{y \in C_2^\perp} |y + x\rangle$$

$$=: |x + C_2^\perp\rangle.$$

when is

$$|u_1 + C_2^\perp\rangle = |u_2 + C_2^\perp\rangle \; ?$$

only if $u_2 + u_1 \in C_2^\perp$.

Each code word corrosponds to

a coset of $C_2^\perp$ inside C_1.

C_1 has 2^{k_1} elements.

$C_2^\perp$ has 2^{n-k_2} elements.

$C_1/C_2^\perp$ has $2^{k_1+k_2-n}$ elements.

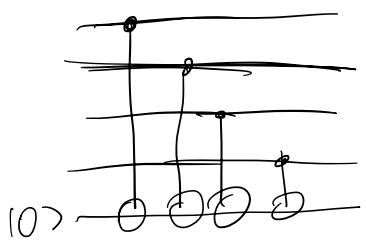
$$H^{\otimes n}|u + C_2^\perp\rangle = \sum_{x \in C_2/C_1^\perp} (-1)^{u\cdot x} |x + C_1^\perp\rangle.$$

Fourier transform.

Error correction

Parity check measurement

for bit flip.

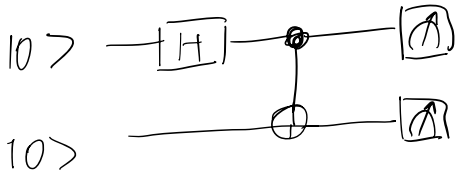


do the same in the H basis

for phase flip.

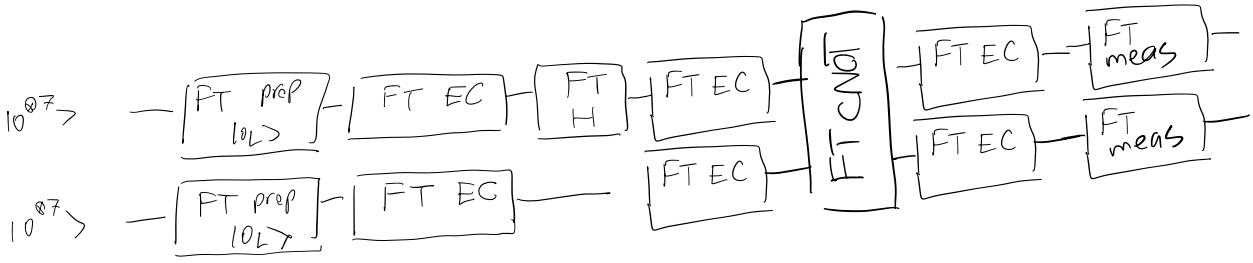
Fault tolerance

Basic idea: perform computation on encoded states so that we don't need decoding.



Noise affects everything: state prep, quantum gates measurement, even identity wires.

each qubit will be replaced w. an encoded block
each operation will be replaced w. FT procedure



Periodic EC is not sufficient Two issues.

① Encoded gates can themselves cause errors to propagate

We should design encoded gates to transmit fault to only a small subset of qubits

② Error correction itself can introduce errors.

Fault tolerant procedure.

Failure of one component within a block, results in at most one output failure of that block.

Component: noisy gate, measurement, wire, state prep, etc.

If probability of failure of a component is p then meas result should have failure prob $O(p^2)$. in out put meas.

Same for state preparation

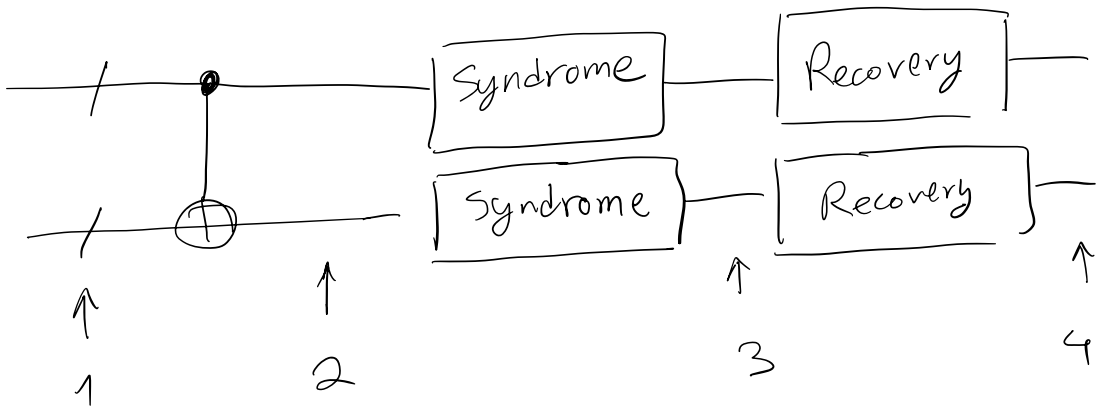
Error model. i.i.d I, X, Y, Z on each wire.

gate U may be approximated w. a channel $\tilde{U}$ s.t. $\| U - \tilde{U} \|_\diamond \leq \varepsilon$.

$$\tilde{U} = (\tilde{U} \circ U^{-1}) \, U$$

↓ gets propagated.

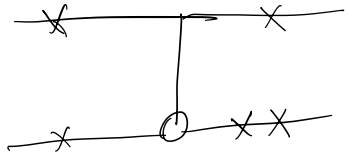
FT implementation of CNOT $\bar{}$



Four possibilities

① Single pre existing error from prev Block.
on each encoded block of qubits.

May cause two errors on the first block once passed through CNOT



However each block has prob $O(p)$ so this event occurs w.p. $O(p^2)$.

② Single pre existing error on top or bottom err.
+ single error in the encoded implementation of CNOT.

w.p $O(p^2)$.

(3) Two errs during CNOT $O(p^2)$

(4) One failare occurs during CNOT
one during syndrome meas.

The only possibility is if syndrome meas
gives one err $\Rightarrow$ w.p $O(p^2)$.

(5) Two or more errors during Syndrome meas
$O(p^2)$.

(6) 1 err Syndrome meas
1 err recovery

(7) Two or more error during recovery.

very large constant. $\sim 10^4$
Steane code.

Concatenated FT construction

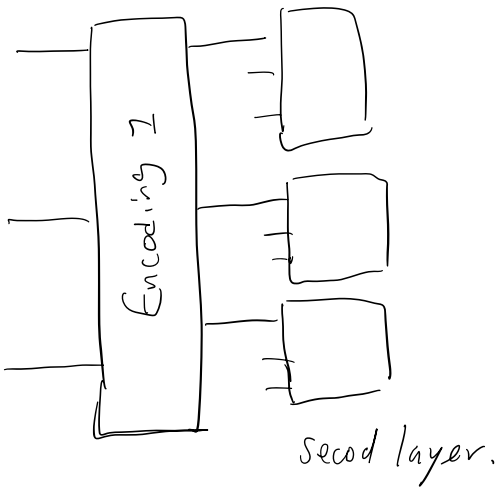
recursively apply the construction above

$C_0 \to C_1 \to C_2 \to \cdots$

$\downarrow$

original ckt

① Each qubit in the original ckt is encoded in a quantum code whose qubit is encoded in a quantum code, and so on.



Second layer.

Failure prob at the physical layer

$cp \to c(cp)^2 \to c(c(cp^2)^2 \to \cdots$

Failure prob $(cp)^{2^k}/c$

size of the ckt d^k

Suppose we want to solve a problem requiring $p(n)$ size ckt. We want final accuracy ε.

We want each gate to suffer $\leq \varepsilon/p(n)$ errors.

$$\frac{(cp)^{2^k}}{c} \leq \varepsilon/p(n) \qquad \text{provided} \quad p < p_{th} = 1/c$$

$$d^k = \left(\frac{\log(p(n)/c\varepsilon)}{\log(1/pc)} \right)^{\log(d)} = O\left(\text{poly}\log \frac{p(n)}{\varepsilon}\right)$$

Hence, simulating ckt contains:

$$O\left(\text{poly}\log\left(\frac{p(n)}{\varepsilon}\right) p(n)\right) \text{ gates.}$$

Fault tolerant gates for 7 qubit code

$$\bar{X} = X_1 X_2 X_3 X_4 X_5 X_6 X_7$$

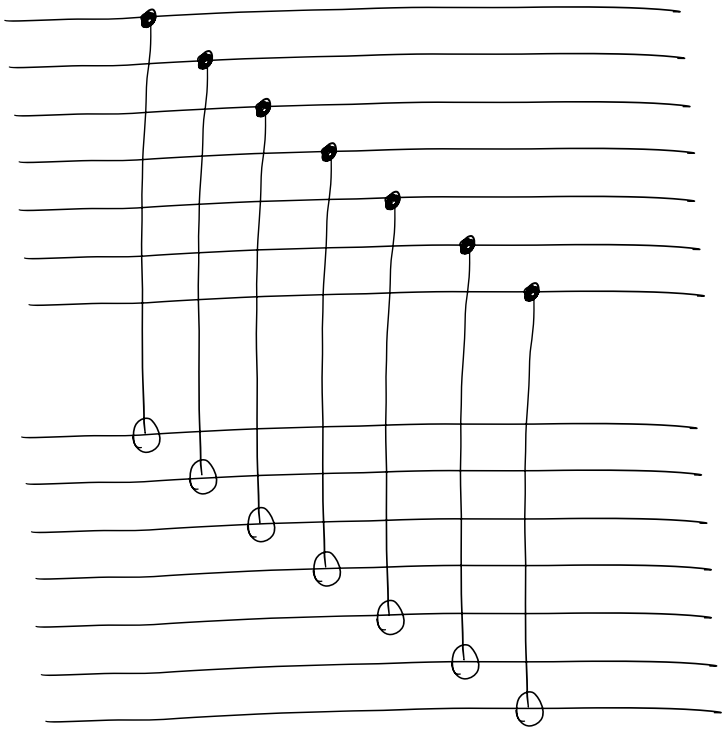
$$\bar{Z} = Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7$$

$$\bar{H} = H_1 H_2 H_3 H_4 H_5 H_6 H_7$$

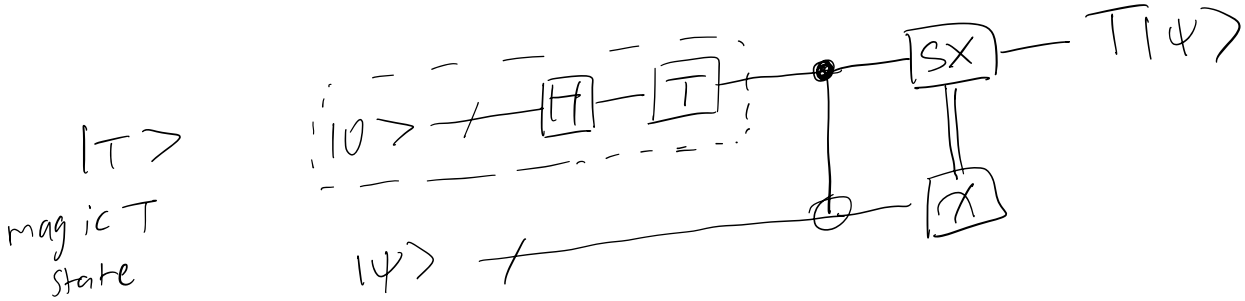
Transversal implementation.

1 error in block $\longrightarrow$ 1 error in block.

Transversal implementation of CNOT



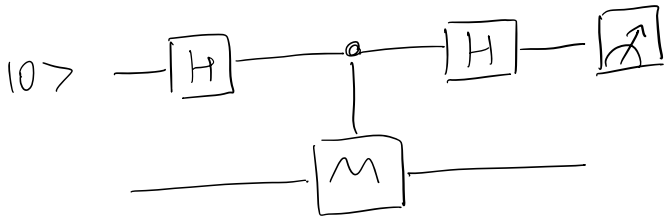
Fault tolerant implementation of T.

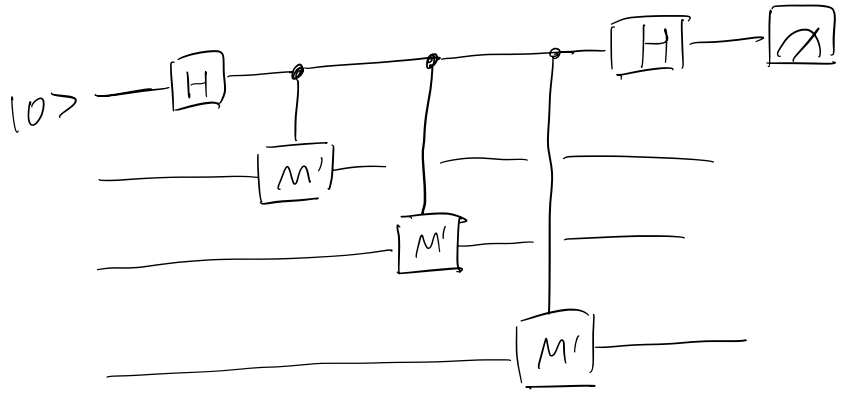


we discussed ideas about preparing |T>

e.g. Fault tolerant meas of SX. → +1 good
→ -1 apply Z.

Fault tolerant measurement.

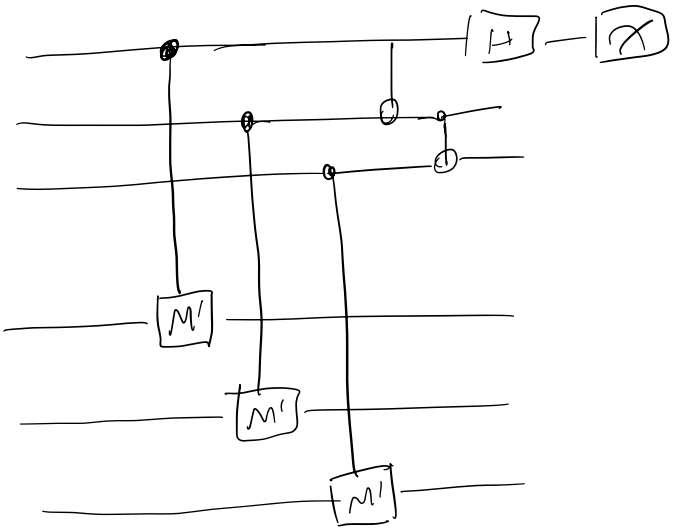




Idea

$|GHZ\rangle$

$= |0000\rangle + |1111\rangle$



The quantum Fourier transforms and the Hidden Subgp problem

for a gp G, rep $\rho : G \to GL(V)$

$$\begin{cases} \rho(gh) = \rho(g)\rho(h) & g,h \in G \\ \rho(e) = \mathbb{I} \end{cases}$$

Character $\chi_\rho : G \to \mathbb{C}$ is given by

$$\begin{cases} \chi_\rho(g) = \overline{\mathrm{Tr}(\rho(g))} \cdot & C_g = \{hgh^{-1} \mid h \in G\} \\ \chi_\rho(hgh^{-1}) = \chi_\rho(g). \to \text{Conjugacy class.} \end{cases}$$

ρ is irreducible if V is irreducible

for two irreps i, j

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} = \delta_{ij}$$

In general

$|\mathrm{Irr}(G)|$ = number of conjugacy classes of G.

for abelian gp $\quad |\mathrm{Irr}(G)| = |G|$.

General QFT

$$F_G : |g\rangle \longmapsto \sum_{\rho \in \mathrm{Irr}(G)} \sqrt{\frac{d_\rho}{|G|}} \sum_{i,j=1}^{d_\rho} \rho(g)_{i,j} |\rho, i, j\rangle$$

for the abelian case $\quad \rho(g) = \chi_\rho(g)$.

$d_\rho = 1$

General orthogonality rel.

$$\frac{d_\rho}{|G|} \sum_{g \in G} \rho_{ij}(g) \overline{\sigma(g)}_{kl} = \begin{cases} \delta_{ik}\delta_{jl} & \text{if } \rho = \sigma \\ 0 & \text{if } \rho \neq \sigma \end{cases}$$

$$\Downarrow$$

$$F_G^{\dagger} = F_G^{-1}$$

Let G be an Abelian gp.

$$F_G := \frac{1}{\sqrt{|G|}} \sum_{x \in G} \sum_{y \in \hat{G}} \chi_y(x) |y\rangle\langle x|.$$

$\hat{G} \equiv$ set of characters of G.

$\chi_y(x) \equiv$ y'th character eval. at $x \in G$.

Since $G \cong \hat{G}$, we can label elements of $\hat{G}$ w. that of G

$$F_G F_G^\dagger = \frac{1}{|G|} \sum_{\substack{x \in G \\ y, y' \in \hat{G}}} \chi_y(x) \overline{\chi_{y'}(x)} |y\rangle\langle y'|$$

$$= \mathbb{I}.$$

E.g. $G = \mathbb{Z}_2^n$, $\chi_y(x) = (-1)^{\langle x, y \rangle}$

$$F_{\mathbb{Z}_2^n} = \frac{1}{\sqrt{2^n}} \sum_{x,y \in \mathbb{Z}_2^n} (-1)^{\langle x,y \rangle} |x\rangle\langle y| = H^{\otimes n}$$

E.g. $G = \mathbb{Z}_N$

$$F_{\mathbb{Z}_{2^n}} = \frac{1}{\sqrt{2^n}} \sum_{x,y \in \mathbb{Z}_{2^n}} \omega_N^{xy} \, |y\rangle\langle x|$$

$$\omega = e^{2\pi i / N}$$

---

any finite abelian gp. G can be written as a direct product of cyclic gps.

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_K} \cong \hat{G}$$

The discrete log problem

$$G = \langle g \rangle := \{ g^k : k \in \mathbb{Z} \}.$$

for $x \in G$, the discret log denoted ω.

$$\log_g(x) = \min \{ r : g^r = x \}.$$

- $\log_g(1) = 0$
- $G = \mathbb{Z}_7^\times$, $\log_3(2) = 2$

There is an efficient quantum alg

for discrete log :

The Hidden subgroup problem :

Let G be a finite group.

We are given black-box access to $f : G \to S$,

where S is a finite set.

Let $H \leq G$ be a subgroup of G.

$$f(x) = f(y) \quad \text{iff} \quad x^{-1}y \in H$$

$$(y = xh, \quad h \in H).$$

We say f hides H.

Note: $f(x) = f(1)$ iff $x \in H$.

- $g \in G$, $g \notin H$: $f(g) = f(x)$ iff $x \in \underline{gH}$.
  left coset of H in G.

- So f is constant and distinct on different cosets of H.

- We could define the problem for right cosets and obtain a computationally equivalent problem.

- Simon's problem was a special case.

$$G = \mathbb{Z}_2^n, \quad H = \langle s \rangle, \quad s \in \mathbb{Z}_2^n$$

- Period finding

$$G = \mathbb{Z}_N^+, \quad H = \langle s \rangle, \quad s \in \mathbb{Z}_N^+.$$

- Classical complexity.

$$\#\text{cosets of } H = \frac{|G|}{|H|}$$

Birth day paradox $\Theta\left(\sqrt{\frac{|G|}{|H|}}\right)$ queries.

necessary and sufficient.

Shor's algorithm for discrete log

$G = \langle g \rangle$

We want $\log_g x$, $x \in G$. $(x \neq g)$.

$(\min \{ r : g^r = x \})$

$N := |G|$. is known.

We cast the problem as an Abelian HSP. over additive gp $\mathbb{Z}_N \times \mathbb{Z}_N$.

Define $f : \mathbb{Z}_N \times \mathbb{Z}_N \to G$

$$f(\alpha, \beta) = x^\alpha g^\beta$$

$$= g^{\alpha \log_g x + \beta}$$

f is constant on the line

$$L_\lambda = \{ (\alpha, \beta) \in \mathbb{Z}_N^2 : \alpha \log_g x + \beta = \lambda \}$$

It hides the line

$$H = L_0$$
$$= \{(0,0), (1, -\log_g x), (2, -2\log_g x), \cdots, (N-1, -(N-1)\log_g x)\}$$

the set of cosets of H in $\mathbb{Z}_N \times \mathbb{Z}_N$ take the form $(\gamma, \delta) + H$, $\gamma, \delta \in \mathbb{Z}_N$.

$$(0,\delta) + H = \{(\alpha, \delta - \alpha \log_g x) : \alpha \in \mathbb{Z}_N\} = L_\delta$$

forms a complete set of cosets

The algorithm proceeds as follows:

① prepare

$$|\mathbb{Z}_N \times \mathbb{Z}_N\rangle = \frac{1}{N} \sum_{\alpha,\beta \in \mathbb{Z}_N} |\alpha, \beta\rangle.$$

② then prepare.

$$\frac{1}{N} \sum_{\alpha,\beta \in \mathbb{Z}_N} |\alpha, \beta, f(\alpha,\beta)\rangle.$$

③ Discard the f register

If the measurement outcome in ③ is g^δ,

we are left w. a super position over coset $(0,\delta)+H$.

$$|(0,\delta)+H\rangle = |L_\delta\rangle = \frac{1}{\sqrt{N}} \sum_{\alpha \in \mathbb{Z}_N} |\alpha, \delta - \alpha \log_g x\rangle$$

④ Apply QFT on the remaining reg.

$$\frac{1}{N^{3/2}} \sum_{\alpha,\mu,\nu} \omega^{\mu\alpha + \nu(\delta - \alpha \log_g x)} |\mu,\nu\rangle$$

$$= \frac{1}{N^{3/2}} \sum_{\mu,\nu} \omega^{\nu\delta} \left(\sum_\alpha \omega^{\alpha(\mu - \nu \log_g x)} \right) |\mu,\nu\rangle.$$

$$\frac{1}{N} \sum_\alpha \omega^{\alpha\beta} = \delta_{\beta=0}$$

we will obtain.

$$\frac{1}{\sqrt{N}} \sum_{\nu \in \mathbb{Z}_N} \omega^{\nu\delta} \left| \overbrace{\nu \log_g x}^{\mu}, \nu \right\rangle.$$

if ν has a multiplicative inverse mod N then

$$\log_g x = \nu^{-1}\mu \quad \text{w.p.} \quad \frac{\phi(N)}{N} = \frac{1}{O(\log\log N)}$$

General Algorithm for Abelian HSP

$H \leq G$

$$f(x) = f(y) \quad \text{iff} \quad x - y \in H$$

Algorithm

① we begin by preparing

$$|G\rangle = \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle$$

② then create

$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x, f(x)\rangle .$$

③ Discard the f register. and obtain

$$x + H = \{ x + h : h \in H \}$$

$$|x + H\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |x + H\rangle .$$

(corresponding to $\rho_H = \frac{1}{|G|} \sum_{x \in G} |x+H\rangle\langle x+H|$.)

④ Apply F_G:

$$|\widehat{x+H}\rangle := F_G\,|x+H\rangle$$

$$= \frac{1}{\sqrt{|H|\cdot|G|}} \sum_{y\in\hat{G}} \sum_{h\in H} \chi_y(x+h)\,|y\rangle$$

$$= \sqrt{\frac{|H|}{|G|}} \sum_{y\in\hat{G}} \chi_y(x)\,\chi_y(H)\,|y\rangle .$$

where $\chi_y(H) = \frac{1}{|H|} \sum_{h\in H} \chi_y(h)$.

Note $U_x : |y\rangle \longmapsto |y+x\rangle$

$U(x)\,\rho_H = \rho_H\,U(x)$

so $\hat{\rho}_H = F_G\,\rho_H\,F_G^{\dagger}$ is diagonal

- If $\chi_y(h) = 1 \quad \forall h\in H \Rightarrow$ $\boxed{\chi_y(H) = 1.}$
- $\exists\, h'\in H,\ \chi_y(h') \neq 1$ since $h'+H = H$

$$\chi_y(H) = \frac{1}{|H|} \sum_{h\in h'+H} \chi_y(h) = \frac{1}{|H|} \sum_{h\in H} \chi_y(h'+H)$$

$$= \chi_y(h')\,\chi_y(H) \Rightarrow \boxed{\chi_y(H) = 0}$$

Also note

$$\frac{1}{|H|} \sum_{x \in H} \chi_y(x) \overline{\chi_{y'}(x)} = \delta_{y,y'}$$

Set $y' = 0 \Rightarrow \chi_y(H) = 0$ if y nontrivial

---

therefore

$$|\widehat{x+H}\rangle = \sqrt{\frac{|H|}{|G|}} \sum_{y : \chi_y(H)=1} \chi_y(x) |y\rangle$$

---

(5) measure $|\widehat{x+H}\rangle$ in the comp basis.

we measure $y \in G$ s.t.

$$\chi_y(h) = 1 \quad \text{for all } h \in H$$

$$y \in H^\perp := \{ y \in \hat{G} : \chi_y(h) = 1, \forall h \in H \}$$

$H^\perp \leq \hat{G}$ all char trivial on H.

Importantly $(H^\perp)^\perp = H$

$$H = \{ y \in G : \chi_y(h) = 1 , \forall h \in H^\perp \}$$

Turn this into a linear system.

$$G \cong \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_k}.$$

$$x \in G , x = (x_1, \ldots, x_k).$$

$$\chi_y(x) = \exp\left(2\pi i \sum_{j=1}^{k} \frac{x_j y_j}{N_j} \right).$$

$y \in H^\perp \iff \chi_y(h) = 1 , \forall h \in H$

$$\iff \sum_{j=1}^{k} \frac{h_j y_j}{N_j} \in \mathbb{Z} , \quad \forall h \in H$$

$$= 0 \mod 1$$

Now suppose we have obtained $y^{(1)}, \ldots, y^{(m)}$

each satisfying $\langle y^{(j)}, h \rangle = 0$.

then $H = \{ h \in G : \langle y^{(j)}, h \rangle = 0 \ \forall j \}$.

obtaining $O(\log |H|)$ random samples

from H is sufficient

General HSP

Eftinger, Høyer, Knill

$\Leftarrow$ $g_H^{\otimes \text{polylog}|G|}$ contains sufficient

information about H.

Non abelian HSP and applications

Non abelian HSP encodes sol to well-known Comp problems.

e.g. graph automorphism or graph isomorphism problems.

Graph automorphism problem

Input Graph Γ on n vertices.

output yes if Γ has a nontrivial automorphism.

i.e $\exists \pi \in S_n$ s.t $\pi(\Gamma) = \Gamma$.
$\pi \neq e$

Def. $Aut(\Gamma) = \{ \pi \in S_n \mid \pi(\Gamma) = \Gamma \} \leq S_n$.

Def. if $|Aut(\Gamma) = \{e\}$ we say Γ is rigid.

Let $f: S_n \to Mat^{n \times n}$, $f(\pi) = \pi(\Gamma)$.

f hides $Aut(\Gamma)$: $f(\pi_1) = f(\pi_2)$ iff. $\pi_1 \in \pi_2 Aut(\Gamma)$.

$\Rightarrow$ Graph automorphism $\leq$ $HSP(S_n)$.

Graph Isomorphism :

Input : Γ, Γ'

Output yes if $\exists \pi \in S_n \quad \pi(\Gamma) = \Gamma' \quad (\Gamma \cong \Gamma')$.

$$S_n \wr S_2 = \langle S_{I_1}, S_{I_2}, \underset{I_1, I_2}{SWAP} \rangle. \leq S_{2n}$$

$[2n] = I_1 \cup I_2$ Swap of I_1 w. I_2

$\{1, \dots, n\} \quad \{n+1, \dots, 2n\}$

$(\sigma, \tau, b) \in S_n \wr S_2$ σ perm Γ

τ perm Γ'

$b = 1$ swap Γ, Γ'

$b = 0$ don't swap Γ, Γ'

$$f(\sigma, \tau, b) = \begin{cases} (\sigma(\Gamma), \tau(\Gamma')) & b = 0 \\ (\sigma(\Gamma'), \tau(\Gamma)) & b = 1 \end{cases}$$

f hides automorphisms of $\Gamma \cup \Gamma'$

this automorphism contains $b = 1$ iff $\Gamma \cong \Gamma'$

Suppose Γ, Γ' are rigid

$\Gamma \ncong \Gamma' \Rightarrow \quad \mathrm{Aut}(\Gamma \cup \Gamma') = \{e\}.$

$\Gamma \cong \Gamma'$
$(\pi(\Gamma) = \Gamma') \Rightarrow \quad \mathrm{Aut}(\Gamma \cup \Gamma') = \{e, (\pi, \pi^{-1}, 1)\}.$

Connection w. Lattice problems.

SVP : given generators of an integer lattice

goal is to find a point within $g(n)$ factor of the shortest vector.

$g(n) > \exp(n) \longrightarrow \in P$

$g(n) = O(1) \longrightarrow$ NP hard.

$g(n) = \text{poly}(n) \longrightarrow$?? hard

Regev. Q.A for HSP over Dihedral group

implies Q.A. for $g(n) = \text{poly}$.

Standard method.

① Prepare $|G\rangle := \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle$

② Query f $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, f(g)\rangle$

③ Discard f $|gH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle$ random $g \in G$.

or $P_H = \frac{1}{|G|} \sum_{g \in G} |gH\rangle\langle gH|$.

Query Complexity:

Ettinger Høyer Knill.

$\rho_{H}^{\otimes \text{poly}\log(|G|)}$ has enough information to specify H.

Resolves the problem in the query setting

Fidelity: $F(\rho,\rho') = \text{tr}|\sqrt{\rho}\sqrt{\rho'}|$.

Barnum - Knill

Suppose ρ is selected from $\{\rho_1,\dots,\rho_N\}$ w.p p_j for ρ_j.

then $\exists$ POVM (pretty good measurement). that identifies.

ρ_j w.p. at least $1 - N\sqrt{\max_{i\neq j} F(\rho_i,\rho_j)}$

$$1 - N\sqrt{\max_{i\neq j} F(\rho_i^{\otimes k},\rho_j^{\otimes k})}$$

$$= 1 - N\sqrt{\max_{i\neq j} F^{k}(\rho_i,\rho_j)}.$$

$$k \geq \Omega\left(\frac{\log(N/\varepsilon)}{\log(1/\max F)}\right) \Rightarrow \geq 1-\varepsilon.$$

We first argue the number of subgroups of G is at most $N = 2^{O(\log^2|G|)}$.

"every subgp $H \leq G$ can be generated by at most $\log_2|H| \leq \log|G|$ elements.

Hence there are $\leq \binom{|G|}{\log|G|}$ subgroups.

Now consider. Fidelity between

$$F(\rho_H, \rho_{H'}) \leq 1/\sqrt{2} \qquad H \neq H'$$

To see this:

$$|gH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle$$

$$\langle g'H' | gH \rangle = \frac{1}{\sqrt{|H| \cdot |H'|}} \sum_{\substack{h \in H \\ h' \in H'}} \langle gh | g'h' \rangle .$$

$$= \frac{|gH \cap g'H'|}{\sqrt{|H| \cdot |H'|}}$$

if $gH \neq g'H' \Rightarrow |gH \cap g'H'| \leq \frac{1}{2}|H| \cdot |H'|$.

The Quantum adiabatic theorem

Idea: Starting from a non degenerate g.s. of a time dependent Hamiltonian that is growing slow enough, the state remains in the ground state.

Schrödinger's equation:

- time independent.

$$i\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle \Longrightarrow |\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$$

$$H|E\rangle = E|E\rangle \longrightarrow \text{phase } e^{-iEt}$$

- Now if $H(t)$ grows slowly enough, starting with an eigenstate the system remains in that state.

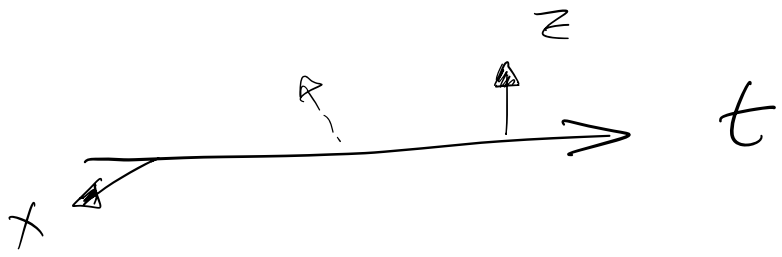
- Time dep eq: $i\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle$

Example $H(t) = -\cos\left(\frac{\pi t}{2T}\right)\sigma_x - \sin\left(\frac{\pi t}{T}\right)\sigma_z$

$H(0) = -\sigma_x$ $\quad |\psi(0)\rangle = |+\rangle$

$\downarrow$?

$H(1) = -\sigma_z$ $\quad |\psi(1)\rangle = |0\rangle$



$s = t/T$ $\quad s \in [0, 1]$

$$i\frac{d}{ds}|\psi(s)\rangle = T H(s) |\psi(s)\rangle .$$

adiabatic thm $\quad \lim_{T\to\infty} |\psi(1)\rangle = \arg\min \langle\psi|H_{(1)}|\psi\rangle$

enough if $T \gtrsim 1/(\text{gap}(H))^2$

Theorem Suppose $H(s)$ has a non-deg g.s. for $s \in [0,1]$

$|\phi(s)\rangle$.

and

$$T \geq \Omega\left(\frac{1}{\varepsilon}\right) \cdot \left[\frac{\|\dot{H}(0)\|}{\Delta(0)^2} + \frac{\|\dot{H}(1)\|}{\Delta(1)^2} + \int_0^1 ds \left(\frac{\|\dot{H}\|^2}{\Delta^3} + \frac{\|\ddot{H}\|}{\Delta^2} \right) \right]$$

if $|\psi(0)\rangle = |\phi(0)\rangle$ then $\| |\psi(1)\rangle - |\phi(1)\rangle \| \leq \varepsilon$

$|\phi(1)\rangle$ = g.s of $H(1)$.

An adiabatic optimization problem:

$h : \{0,1\}^n \to \mathbb{R}$.

Question: $\exists z$, $h(z) = 1$? NP-complete

Question: $\operatorname{argmin} h(z)$ NP-hard.

Beginning Hamiltonian: H_B

Problem Hamiltonian:

$$H_p = \sum_{z \in \{0,1\}^n} h(z) |z\rangle\langle z|.$$

$$\text{g.s}(H_p) = |\operatorname{argmin}(h)\rangle.$$

Adiabatic path:

$$H_T(t) = H(t/T) = (1 - f(t/T))H_B + f(t/T)H_P$$

$f(0) = 0$, $f(1) = 1$ (twice diff.).

$H(0) = H_B$, $H(1) = H_P$

$$H_B = -\sum_{j=1}^{n} \sigma_x^{(j)}$$

$$|S\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle.$$

Alg. ① prep g.s of H_B

② evolve $H(s)$

③ meas in comp basis

Running time $f(s) = s$

$$\dot{H} = H_P - H_B$$

$$\ddot{H} = 0$$

$$\Delta_{min} = \min_{s \in [0,1]} \Delta(s).$$

$$T \geq \Omega(1/\varepsilon) \cdot \left(\frac{\|H_p - H_B\|}{\Delta_{min}^2} + \frac{\|H_p - H_B\|^2}{\Delta_{min}^3} \right)$$

$\Rightarrow \| |\psi(1)\rangle - |\phi(1)\rangle \| \leq \varepsilon.$

to show efficiency $\Rightarrow$ $\Delta_{min} \geq 1/\text{poly}.$

Unstructured search is equiv to minimizing.

$$h = \begin{cases} 0 & x \text{ marked} \\ 1 & \text{oth.} \end{cases}$$

$\Rightarrow H_p = \mathbb{1} - |m\rangle\langle m|$

Choose $H_B = \mathbb{1} - |s\rangle\langle s|.$

$$H(s) = \mathbb{1} - \left[(1 - f(s)) |s\rangle\langle s| + f(s) |m\rangle\langle m| \right]$$

$f : [0,1] \longrightarrow [0,1].$

$H(s)$ only acts nontrivially on

$\text{Span}\{ |m\rangle, |s\rangle \}.$

$a := \langle s|m\rangle = 1/\sqrt{N}$

$$H = \begin{pmatrix} (1-f)(1-a^2) & -(1-f)a\sqrt{1-a^2} \\ -(1-f)a\sqrt{1-a^2} & 1-(1-f)(1-a^2) \end{pmatrix}$$

$$= 1/2 - (1-f)a\sqrt{1-a^2}\,\sigma_x + \left[(1-f)(1-a^2) - 1/2\right]\sigma_z$$

$$E_0 = 1/2\left(1 - \sqrt{1-4f(1-f)(1-a^2)}\right)$$

$$E_1 = 1/2\left(1 + \sqrt{1-4f(1-f)(1-a^2)}\right)$$

$$\Delta = \sqrt{1-4f(1-f)(1-a^2)}$$

minimum at $f = \frac{1}{2}$. $\Delta_{min} = a = 1/\sqrt{N}$

But for $f(s) = s$ this gives $T \sim O(N^{3/2})$.

full adiabatic thm

$$\int \frac{df}{\Delta^3} = \int_0^1 \frac{df}{\left[1-4f(1-f)(1-a^2)\right]^{3/2}}$$

$$= 1/a^2 = N.$$

We can however do better by choosing a different function for f.

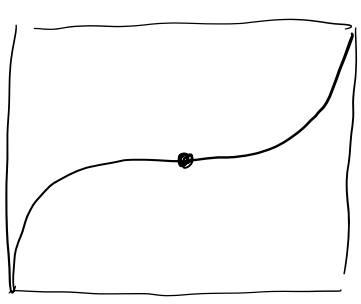
Intuition: • gap is smallest around $f(s) = 1/2$ so evolve more slowly around that value.

• gap is around $1/\sqrt{N}$ for $|f - 1/2| \approx 1/\sqrt{N}$.

$\Rightarrow$ runtime $O(\sqrt{N})$ is conceivable.

• Idea: Choose $\dot{f} = \alpha \Delta^p$ $(p = 3/2)$.

$$\int_0^1 ds = \int_0^1 df/\dot{f} \Rightarrow \alpha \approx N^{1/4}$$



$$\|\dot{H}(s)\| = \|\dot{f}(s)(H_p - H_B)\|$$
$$= |\dot{f}(s)| \sqrt{1 - a^2}$$
$$= \alpha \sqrt{1 - a^2}\, \Delta^{3/2}$$

$$\Rightarrow \frac{\|\dot{H}(0)\|}{\Delta(0)^2} = \frac{\|\dot{H}(1)\|}{\Delta(1)^2} = \alpha \sqrt{1 - a^2} = O(N^{1/4}).$$

$$\int_0^1 \frac{\|\dot{H}\|^2}{\Delta^3}\, ds = (1-a^2)\int_0^1 \frac{\dot{f}^2}{\Delta^3}\frac{df}{\dot{f}}$$

$$= \alpha(1-a^2)\int_0^1 \frac{df}{\Delta^{3/2}}$$

$$= \alpha^2(1-a^2)$$

$$= O(\sqrt{N})$$

$$\|\ddot{H}\| = |\ddot{f}(s)|\sqrt{1-a^2}$$

$$= 3/2\,\alpha\sqrt{1-a^2}\,\Delta^{1/2}\dot{f}\left|\frac{d\Delta}{df}\right|$$

$$\frac{d\Delta}{df} = \frac{2(2f-1)(1-a^2)}{\Delta}$$

$$\Rightarrow \int_0^1 \frac{\|\ddot{H}\|}{\Delta^2}\, ds = \frac{6\alpha(1-a^2)^{3/2}}{\sqrt{a}(1+\sqrt{a})(1+a)}$$

$$= O(\sqrt{N}).$$

Universal Q. comp w. adiabatic comp.

AQC $\subseteq$ BQP via Hamiltonian Simulation.

AQC $\supseteq$ BQP ? $\Rightarrow$ yes, even using linear interpolation.

Feynman Q.C.

Any classical rev. logic can be implemented using a Hamiltonian system. We can actually do more: we can simulate BQP.

Idea:

embed the output of a unitary circuit $U_k U_{k-1} \cdots U_1$ into evol by Hamiltonian

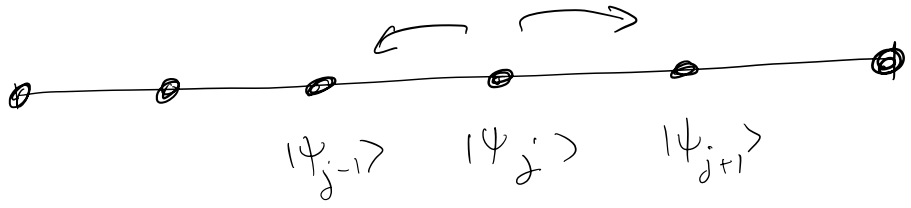
$$H_F = \sum_{j=1}^{k} H_j \quad , \quad H_j = U_j \otimes |j\rangle\langle j-1| + U_j^\dagger \otimes |j-1\rangle\langle j|$$

If we start from $|\psi\rangle \otimes |0\rangle$, then

the evolved state $\in$ span $\{|\psi_j\rangle\}$

where $|\psi_j\rangle = U_j \cdots U_1 |\psi\rangle \otimes |j\rangle$

$$\langle \psi_j | H_F | \psi_{j\pm 1} \rangle = 1$$



- we can show

$$|\langle \psi_k | e^{-iH_F K/2} |\psi_0\rangle|^2 = \Omega(K^{-2/3})$$

Repeat $O(K^{2/3})$ times

- Another idea

We can make success prob ≥ 1 in one shot.

$$H_{FG} = \sum_{j=1}^{K} \sqrt{j(K+1-j)}\, H_j$$

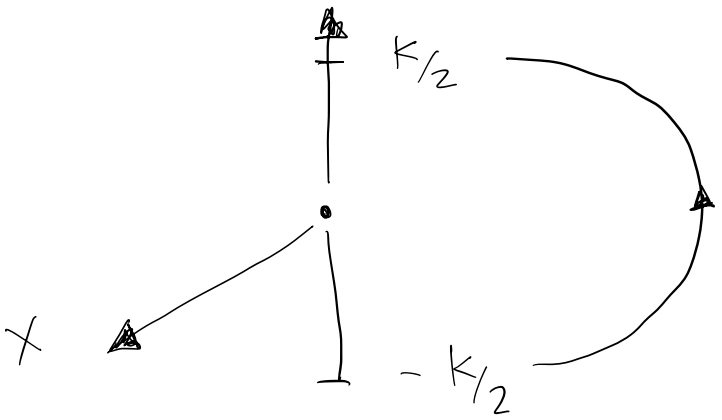
- It happens that $e^{-iH_{FG}t}|\psi_0\rangle = |\psi_k\rangle$

$t = \pi$

- Idea $|\psi_j\rangle$ state of total angular momentum

$\frac{k}{2}(k/2+1)$, $z = j - k/2$

- Then H_{FG} is the x direction of angular momentum



qubit encoding of the clock

$$|j\rangle = |\underbrace{0\cdots0}_{j}\,1\,\underbrace{0\cdots0}_{K-j}\rangle$$

$$|j\rangle\langle j-1| \longrightarrow (|01\rangle\langle 10|)^{(j-1,j)}$$

Conclusion: even single time indep Hamiltonian is enough to encode BQP.

An adiabatic variant:

Idea: Design time dep Hamiltonian s.t.

g.s(H(0)) = initial state.

g.s(H(1)) = History state.

Clock $|0\rangle, |1\rangle, \cdots, |K\rangle$.

$$H_B = -I \otimes |0\rangle\langle 0| + H_{penalty}$$

$$H_{penalty} = \sum_{j=1}^{n} (|1\rangle\langle 1|)^{(j)}$$

g.s. is $|0\cdots0\rangle \otimes |0\rangle$.

$H_C = -H_F + H_{penalty}$. $|\eta_\psi\rangle :=$

$$g.s\,(-H_F) = \operatorname*{Span}_{\psi}\left\{ \frac{1}{\sqrt{k+1}} \sum_{j=0}^{k} |\psi_j\rangle \right\}$$

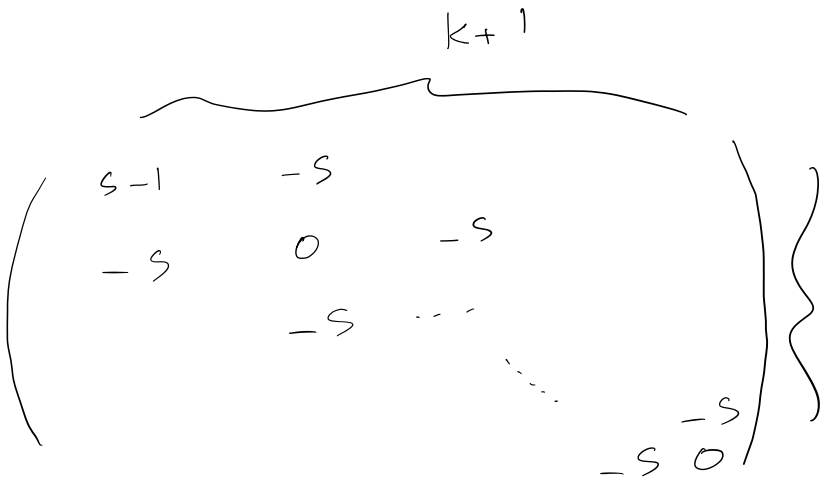
$H_{penalty}$ penalizes states whose initial state $\neq |0\cdots0\rangle$.

- so $|\eta_{0\cdots0}\rangle$ is the unique g.s. of H_C.
- upon measuring clock reg in $|\eta_{0\cdots0}\rangle$ we obtain $|\psi_k\rangle$ w.p. $\frac{1}{k+1}$

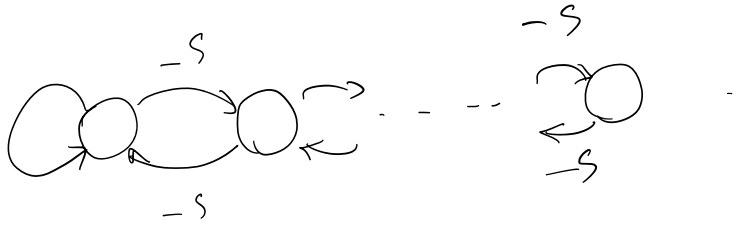
- $H(s) = (1-s) H_B + s H_C$.
- we choose $H_T(t) = H(t/T)$
- remains to estimate $\Delta(s)$.
- Enough to work with

$$V_0 = \operatorname{Span}\{|\psi_j\rangle\} \quad \text{for } \psi = 0^n$$

$H(s) \cong$



Lemma. $s \in [0,1]$ $\Delta(s) \geq \Omega(1/k^2)$.



Claim $\langle \psi_j | E_p \rangle = \sin(p(k-j+1))$.

$E_p = -2s \cos p$.

$\langle \psi_j | H(s) | \psi_p \rangle = E_p \langle \psi_j | E_p \rangle$

$\Rightarrow \quad -s \sin(kp) + (s-1) \sin((k+1)p)$

$= E_p \sin((k+1)p)$.

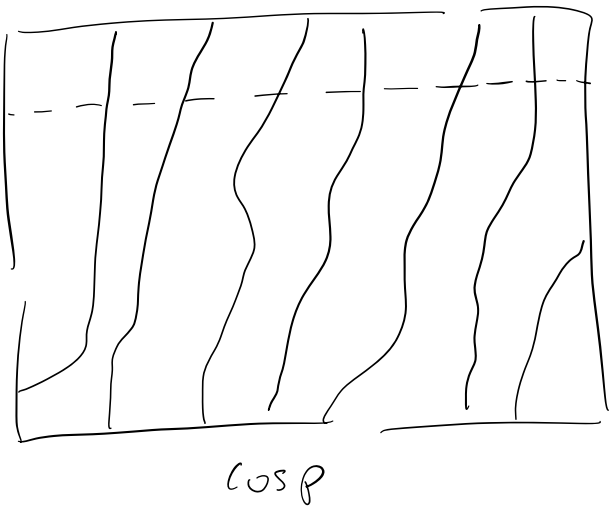
$\Rightarrow \quad s \sin((k+2)p) = (1-s) \sin((k+1)p)$

Chebychev poly $\dfrac{U_{k+1}(\cos p)}{U_k(\cos p)} = \dfrac{1-s}{s}$

$$U_k(\cos\theta) = \frac{\sin((k+1)\theta)}{\sin\theta}$$

Roots of $U_k(x)$ are $\cos\left(\frac{j\pi}{k+1}\right)$

$\frac{U_{k+1}(\cos\rho)}{U_k(\cos\rho)}$



$$\text{gap} \geq 2\left(\cos\frac{\pi}{k+2} - \cos\frac{\pi}{k+1}\right) \geq \Omega(1/k^3).$$

Define

The quantum k-local Hamiltonian problem

QMA

Result: The k-local Hamiltonian problem is QMA-complete.

- k-LH $\subseteq$ QMA

  use phase estimation

- QMA $\subseteq$ k-LH

History state for a QMA protocol.

$$|\eta\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |\psi(t)\rangle \otimes |t\rangle.$$

$$|\psi(0)\rangle = |x\rangle \otimes |0\rangle \otimes \underbrace{|\psi_x\rangle}_{\text{witness}}.$$

$$H = H_{in} + H_{out} + H_{prop} + H_{clock}.$$

$$H_{in} = \sum_j (|1\rangle\langle 1|)^{(j)} \otimes I^{\text{witness}} \otimes (|0\rangle\langle 0|)^{(\text{clock})}$$

$$H_{out} = (|0\rangle\langle 0|)^{(\text{output})} \otimes I^{\text{witness}} \otimes (|T\rangle\langle T|)^{(\text{Clock})}$$

If output qubit close to 0,

then +1 energy penalty

If output qubit close to 1, it is "0"

$$H_{prop} = \sum_{t=1}^{T} H_{prop}(t)$$

$$H_{prop}(t) = \tfrac{1}{2}\left(I \otimes |t\rangle\langle t| + I \otimes |t-1\rangle\langle t-1| - U_t \otimes |t\rangle\langle t-1| - U_t^{+} \otimes |t-1\rangle\langle t| \right)$$

$H_{prop}|\eta\rangle = 0$ if $|\eta\rangle$ is valid History state.

If $|\psi\rangle$ is acc w.p. $1-\varepsilon$ then

$$E_0 \leq \varepsilon/T+1 \leq E_{low}$$

- Difficult part If $|\psi\rangle$ is rejected

  then $E_0 \geq E_{high} \geq E_{low} + 1/poly$.

- Make H_{prop} local (it is $\log n$-local now).

Let $V = \sum_{t=0}^{T} V_t \otimes |t\rangle\langle t|$

$$V^\dagger H_{prop} V = \sum_{\tau=0}^{T} \frac{1}{2}\left(|t\rangle\langle t| + |t-1\rangle\langle t-1| - |t\rangle\langle t-1| - |t-1\rangle\langle t| \right)$$

$$= \begin{pmatrix} 1/2 & -1/2 & & & \\ -1/2 & 1 & -1/2 & & \\ & -1/2 & 1 & \ddots & \\ & & \ddots & & 1/2 \end{pmatrix}$$

$$= I - \tfrac{1}{2} M$$

$$M = \begin{pmatrix} 1 & 1 & & & \\ 1 & 0 & 1 & & \\ & 1 & 0 & 1 & \\ & & \ddots & \ddots & 1 \\ & & & 1 & 1 \end{pmatrix}$$

$$|w\rangle = \sum_{t=0}^{T} e^{iwt} |t\rangle$$

$$\Rightarrow \quad M\left(e^{iw/2}|w\rangle + e^{-iw/2}|-w\rangle \right)$$

$$= 2\cos w \left(e^{iw/2}|w\rangle + e^{-iw/2}|-w\rangle \right)$$

Boundary condition at $t = T$

$$w_k(T+1) = \pi k, \qquad k = \text{integer}.$$

$$E_0 = 0$$

$$E_1 = 2\sin^2\left(\frac{\pi}{2(T+1)}\right) \approx \frac{\pi^2}{2(T+1)^2}$$

Next we consider the spectrum of

$$H = H_{in} + H_{out} + H_{prop}.$$

$$(H_{in} + H_{out}) \,|\, \text{valid input} / \text{acc output}\rangle = 0$$

$$\langle H_{in} + H_{out} \rangle \geq 1$$

space orth

gap $= 1$

Tool: H_1, H_2 Herm.

$\lambda_{min}(H_1) = \lambda_{min}(H_2) = 0$

gap $\geq \Delta$.

$\Rightarrow \quad H_1 \geq \Delta(I - \Pi_1)$

$H_2 \geq \Delta(I - \Pi_2)$.

$\Rightarrow H_1 + H_2 \geq \Delta(2I - \Pi_1 - \Pi_2)$.

$\Rightarrow \langle H_1 + H_2 \rangle \geq 2\Delta - \Delta \langle \Pi_1 + \Pi_2 \rangle$.

$|\langle \psi_1 | \psi_2 \rangle| = \cos\theta \quad \Rightarrow 0 \leq \theta \leq \pi/2$.

$|\psi_1\rangle \cong \begin{pmatrix} \cos\theta/2 \\ \sin\theta/2 \end{pmatrix}, \quad |\psi_2\rangle \cong \begin{pmatrix} \cos\theta/2 \\ -\sin\theta/2 \end{pmatrix}$

$\Rightarrow \psi_1 + \psi_2 = \begin{pmatrix} 2\cos^2\theta/2 & \\ & 2\sin^2\theta/2 \end{pmatrix}$

$\langle \psi_1 + \psi_2 \rangle \leq 2\cos^2\theta/2 \leq 1 + \cos\theta$

If overlap between $\mathrm{Im}(\Pi_1), \mathrm{Im}(\Pi_2)$

$\max |\langle \phi, \psi \rangle| = \cos\theta$

$\Rightarrow \langle \Pi_1 + \Pi_2 \rangle \leq 1 + \cos\theta$

$$\Rightarrow \quad \langle H_1 + H_2 \rangle \geq 2\Delta - \Delta \langle H_1 + H_2 \rangle$$

$$\geq \Delta(1 - \cos\theta)$$

$$= 2\Delta \sin^2 \theta/2$$

H_2 = H prop.

$$\ker(H_2) = \left\{ \frac{1}{\sqrt{T+1}} \sum_t |\psi(t)\rangle \otimes |t\rangle \right\}.$$

we show in the no case

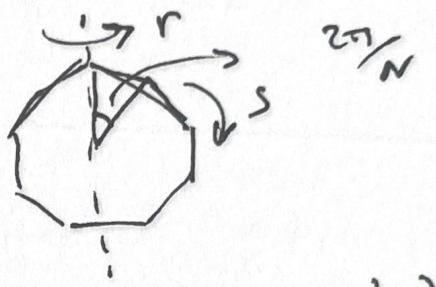
$$\langle \ker(H_1) , \ker(H_2) \rangle \geq \text{large}.$$

March 31, 2026

The Dihedral HSP

$$D_N = \langle r, s : r^2 = s^N = 1 \quad rsr = s^{-1} \rangle .$$

$|D_N| = 2N$, Symmetries of N-gon.



- $(s^x r^a)(s^y r^b)$

$= s^{x + (-1)^a y} r^{a+b}$

Notation — Multiplication

$(x, a) \cdot (y, b) = (x + (-1)^a y, a + b)$.

semidirect product $\mathbb{Z}_N \rtimes_\varphi \mathbb{Z}_2$

$\varphi : \mathbb{Z}_2 \to Aut(\mathbb{Z}_N)$.

$\varphi(a)(y) = (-1)^a y$.

Inverse

$(x, a)^{-1} = (-(-1)^a x, a)$.

Subgroups of D_N → Cyclic: $\langle (x, 0) \rangle$, $x \mid N$.

→ Dihedral: $\langle (y, 1) \rangle$, $y \in \mathbb{Z}_N$

$\langle (x, 0), (y, 1) \rangle$

Ettinger-Høyer: Dihedral HSP for general H

$\leq_{BQP}$

Dihedral HSP for $H = \langle (y,1) \rangle$

Main idea general $H = \langle (x,0), (y,1) \rangle$

use Shor to find x.

Fourier Sampling in the Dihedral gp.

$H = \langle (y,1) \rangle$

consider cosets of the form

$$|(\mathbb{Z},0)H\rangle = \frac{1}{\sqrt{2}}(|z,0\rangle + |y+z,1\rangle)$$

goal: Specify y using m copies from $|(\mathbb{Z},0)H\rangle^{\otimes m}$

Idea Weak Fourier Sampling

$$|gH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle$$

QFT over G decomposes the state into

$$\bigoplus_{\rho \in G} \mathbb{C}^d \otimes \mathbb{C}^d \qquad |i,j,\rho\rangle \quad (1)$$

- weak Fourier sampling measures $\hat{\rho}$ register only.
- strong Fourier sampling measures $\hat{\rho}, i, j$

⊛ We can show by applying $F_{\mathbb{Z}_N} \otimes I_2$ to the first register we can do weak Fourier sampling

$$(F_{\mathbb{Z}_N} \otimes I_2)\,|(z,0)H\rangle = \frac{1}{\sqrt{2N}} \sum_{k \in \mathbb{Z}_N} \left(\omega_N^{kz}\,|k,0\rangle + \omega_N^{k(y+z)}\,|k,1\rangle\right)$$

$$= \frac{1}{\sqrt{N}} \sum_{k \in \mathbb{Z}_N} \omega_N^{kz}\,|k\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + \omega_N^{ky}\,|1\rangle\right).$$

we measure k and $|\psi_k\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \omega_N^{ky}\,|1\rangle\right)$.

Combining states

Some values of k are useful:

⊛ $|\psi_{N/2}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^y\,|1\rangle\right) \Rightarrow$ parity of y.

Main idea Combine $|\psi_k\rangle$ for different values of k and come up w. $|\psi_{k'}\rangle$ for more useful values of k.

Combining the states.

$$|\psi_p\rangle|\psi_q\rangle = \frac{1}{2}\left(|0\rangle + \omega^{yp}|1\rangle\right)\left(|0\rangle + \omega^{yq}|1\rangle\right)$$

$$= \frac{1}{2}\left(|0,0\rangle + \omega^{yp}|1,0\rangle + \omega^{yq}|0,1\rangle + \omega^{(p+q)y}|1,1\rangle\right)$$

$$\mapsto \frac{1}{2}\left(|0,0\rangle + \omega^{yp}|1,1\rangle + \omega^{yq}|0,1\rangle + \omega^{(p+q)y}|1,0\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(|\psi_{p+q}, 0\rangle + \omega_N^{yq}|\psi_{p-q}, 1\rangle\right).$$

Measuring the second register gives

$|\psi_{p\pm q}\rangle$ w.p $1/2$ $\quad +:0$, $-:1$

Kuperberg Sieve $\quad N = 2^n$

it is enough to evaluate the least sign bit of y (then apply the proc recursively):

D_N contains two subgroups isomorphic to $D_{N/2}$

$$A = \{(2x,0), (2x,1) : x \in \mathbb{Z}_{N/2}\}$$

$B = \{(2x, 0), (2x+1, 1) : x \in \mathbb{Z}_{N/2}\}$.

if $lsb(y) = 1 \Rightarrow$ recurse to A

$lsb(y) = 0 \Rightarrow$ recurse to B.

Idea : Start w. a large number of states.

- Collect them in pairs $|\psi_p\rangle, |\psi_q\rangle$.
  that share many of their lsb s.t
- $p-q$ has many of its lsb 0.

- Trying to get $N/2 = 010^{n-2}$ requires exp time.
- so we do this in stages.

Alg: ① prep $\Theta(16^{\sqrt{n}})$ $|\psi_k\rangle$'s

② $m = \lceil \sqrt{n} \rceil$, for each $j = 0, 1, \ldots, m-1$
assume all $|\psi_k\rangle$'s w. at least
mj of the lsb of $k = 0$.
collect them into $|\psi_p\rangle, |\psi_q\rangle$. s.t they
share at least the next m lsb's.

(2) (Cont.) Discarding those that cannot be paired.

Create $|\psi_{p \pm q}\rangle$, discard if "+".

$|\psi_{p-q}\rangle$ will have the next m lsb set to 0's.

(3) once done choose $|\psi_{2^{n-1}}\rangle \Rightarrow$ get lsb(y).

Running time $2^{O(\sqrt{n})}$.

Analysis

- we show the alg reaches final step w. nontrivial prob.
- Suppose we try to cancel m bits in each step $\Rightarrow$ (get n/m steps) Starting w. 2^l states
- each combining succeeds w.p $1/2$. at each step we retain $\sim 1/4$ of the states.
- There are at most 2^m states that are not pair on any m bits. if $\geq 2 \cdot 2^m$ states at each stage we will get $\geq 1/8$ ~~probability of~~ fraction (4)

(cont.)

retained for the next stage.

- so we require $2^{\ell - 3n/m} > 2^{m+1}$

  or $\ell > m + 3n/m + 1 \Rightarrow$ minimize $m \approx \sqrt{n}$

  $\ell \approx 4\sqrt{n}$.
