$\boxed{\text{Ph452}}$ Lecture 24

(A) Quick Review

- Q. State Discrim.
- QEC Criteria $\langle i | E_a^\dagger E_b | j \rangle = C_{ab}\delta_{ij}$, $C = C^\dagger$
- $[[n,k,d]]$: k qubits in length n (rate k/n)

$$\text{distance } d = \min_{\text{Pauli ops}} \{ wt(E_k) \mid \langle i | E_k | j \rangle \neq C_k \delta_{ij} \}$$

$$\text{So } wt(E_k) \leq d-1 \Rightarrow \langle i | E_k | j \rangle = C_k \delta_{ij}$$

Can split $d-1$ wt across 2 ops: $E_a^\dagger E_b = E_k$

$$\left\lfloor \frac{d-1}{2} \right\rfloor = \min\{ wt(E_a), wt(E_b) \}$$

$$\Rightarrow \boxed{\text{can correct } \left\lfloor \frac{d-1}{2} \right\rfloor \text{ errors}}$$

"Dominant error is a thief who steals qubits"

Located errors : All errors E_a have support on t known qubits

then $wt(E_a) \leq t$, $wt(E_b) \leq t$ and $wt(E_a^\dagger E_b) \leq t$ for all located errors

$$\Rightarrow \text{If dist} = d, \quad d-1 = \min\{ wt(E_a), wt(E_b) \}$$

$$\Rightarrow \boxed{\text{can correct } d-1 \text{ located errors}}$$

Ph 452 Lecture 24

<u>Error detection</u> : For $[[n,k,d]]$ code,

$$\langle \bar{i} | E_a | \bar{j} \rangle = c_a \delta_{ij} \quad \forall\ E_a \text{ s.t. } wt(E_a) \le d-1$$

$$\Leftrightarrow \quad E_a |\bar{i}\rangle = c_a |\bar{i}\rangle + \underbrace{|\varphi_{ai}^{\perp}\rangle}_{\text{orthogonal to } \mathcal{C}}$$

Measure $\Pi_0 = \sum |c_a|^2 |\bar{i}\rangle\langle\bar{i}|$

$\Pi_1 = |\text{orthog}\rangle\langle\text{orthog}|$

Outcome 0 : Codespace unchanged

1 : Error of $wt \le d-1$ detected!

$\Rightarrow$ $\boxed{\text{can } \underline{\text{detect}} \text{ } d\text{-}1 \text{ errors}}$

Ph 452 Lecture 24

QEC Criteria

Necessary:

$$\mathcal{R} \circ \mathcal{E}(\rho_{code}) \propto \rho_{code} \Rightarrow \sum (R_k E_i) \rho_c (R_k E_i)^+ = c\, \rho_c$$

Let $\Pi_c = \sum |i\rangle\langle i|$.

$$\sum (R_k E_a \Pi_c)\, \rho\, (\Pi_c E_a^+ R_k^+) = c\, \Pi_c \rho\, \Pi_c$$

w/ unitary sum. → OSR ambiguity: $R_k E_a \Pi_c = u_{ka} \sqrt{c}\, \Pi_c$

$\Rightarrow$ $\Rightarrow \Pi_c E_a^+ R_k^+ = u_{ka}^* \sqrt{c}\, \Pi_c$

$$\Rightarrow \Pi_c E_a^+ R_k^+ R_k E_b \Pi_c = c\, u_{ka}^* u_{kb} \Pi_c$$

Sum over k, use $\sum R_k^+ R_k = I$:

$$\Pi_c E_a^+ E_b \Pi_c = C_{ab} \Pi_c, \qquad C_{ab} := \sum_k c\, u_{ka}^* u_{kb}$$

$$\Rightarrow \langle i | E_a^+ E_b | j \rangle = C_{ab} \delta_{ij}$$

Ph452 Lecture 24

Sufficient

$$\langle \bar{i} | E_a^\dagger E_b | \bar{j} \rangle = C_{ab}\, \delta_{ij}, \quad C = C^\dagger$$

Let $\sum_{ab} u_{ja}^* C_{ab} u_{kb} = d_k \delta_{jk}$

Let $F_k := \sum_a u_{ka} E_a$. Then $\langle \bar{i} | F_a^\dagger F_b | \bar{j} \rangle = d_a \delta_{ab} \delta_{ij}$.

$$R_k := \frac{1}{\sqrt{d_k}} \sum_i |\bar{i}\rangle\langle \bar{i}| F_k^\dagger \quad (R_k = 0 \text{ if } d_k = 0)$$

Then on $\rho_c = \sum_{ij} r_{ij} |\bar{i}\rangle\langle \bar{j}|$

$(\tilde{\mathcal{F}} = \mathcal{E})$

$$\mathcal{R} \circ \mathcal{E}(\rho_c) = \sum_{ijka} R_k F_a r_{ij} |\bar{i}\rangle\langle \bar{j}| F_a^\dagger R_k^\dagger$$

$$= \sum_{\substack{ijka \\ lm}} \frac{r_{ij}}{d_k} |\bar{l}\rangle \underbrace{\langle \bar{l}| F_k^\dagger F_a |\bar{i}\rangle}_{d_k \delta_{ak} \delta_{il}} \underbrace{\langle \bar{j}| F_a^\dagger F_k |\bar{m}\rangle}_{d_k \delta_{ak} \delta_{jm}} \langle \bar{m}|$$

$$= \sum_{ijk} d_k r_{ij} |\bar{i}\rangle\langle \bar{j}|$$

$$= \left(\sum_k d_k \right) \rho_c$$

$$\propto \rho_c$$

$F_k = \sum u_{ka} E_a \Rightarrow E_k = \sum u^*_{ak} F_a$

Ph 452 Lecture 24

Linearity of QEC:

Hmm, maybe can only correct linear comb. of F_k's, not E_k's?

If $\{E_k\}$ correctable, then $\{G_j = \sum_j \alpha_{jk} E_k\}$ also is!

Proof: Let R_k, F_k, U be as before. Then $G_\ell = \sum \alpha_{\ell p} F_p$

$$\sum_{ijk\ell} R_k G_\ell r_{ij} |\bar{i}\rangle\langle\bar{j}| G_\ell^\dagger R_k^\dagger$$

$$= \sum_{\substack{ijk\ell \\ mnpq}} \frac{r_{ij}}{d_k} \alpha^*_{\ell p} \alpha_{\ell q} |\bar{m}\rangle \underbrace{\langle\bar{m}| F_k^\dagger F_p |\bar{i}\rangle}_{d_k \delta_{kp} \delta_{im}} \underbrace{\langle\bar{j}| F_q^\dagger F_k |\bar{n}\rangle}_{d_k \delta_{qk} \delta_{jn}} \langle\bar{n}|$$

$$= \left(\sum_{k\ell} d_k \alpha^*_{\ell k} \alpha_{\ell k}\right) \sum_{ij} r_{ij} |\bar{i}\rangle\langle\bar{j}|$$

$$\propto \rho_c$$

$\Rightarrow$ If can correct for depolarizing channel on any t qubits, can correct <u>any</u> error on $\leq t$ qubits.

Ph452 Lecture 24

Quantum Hamming Bound

Let $[[n, k, 2t+1]]$ be a nondegenerate code.

Each error space orthogonal, dim $= 2^k$.

errors: $\binom{n}{j}$ locations for j errors

3 pauli errors / location
+ 1 identity "error"

$\rightarrow \sum_{j=0}^{t} \binom{n}{j} 3^j$ total # errors

All error spaces must fit in n-qubits:

~~for CHB let $3^j \to 1$~~

$$\boxed{\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leq 2^n}$$

Perfect codes: saturate QHB.

For $t=1$, $k=1$, can check by hand need $n \geq 5$

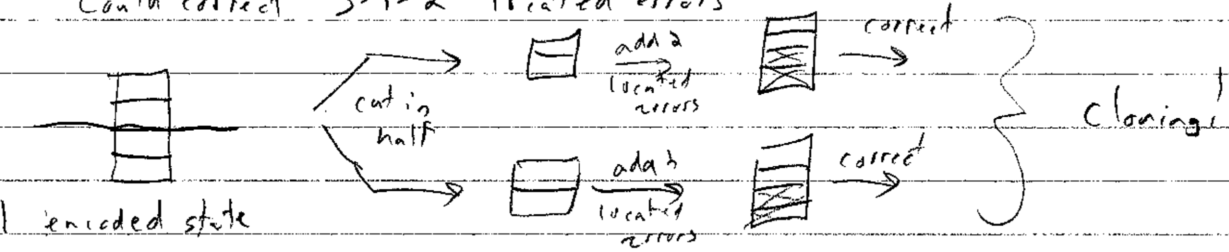
(I know of no degen code violating QHB, tho.)

Ph 432 Lecture 24

No-cloning bound

Is there a $[\![4,1,3]\!]$ degenerate code?

Could correct $3-1=2$ located errors



Generally, $[\![n, k \geq 1, d]\!]$ must obey

$$\boxed{n > 2(d-1)}$$

Note: $|\phi^+\rangle = |00\rangle + |11\rangle / \sqrt{2}$ is a $[\![2,0,2]\!]$ code
$\left(wt(E_k) = 2-1 = 1 \Rightarrow \langle i | E_k | i \rangle = C_k \delta_{ii} \right)$

Quantum Singleton Bound ("Maximum distance separable")

$$\boxed{n - k \geq 2(d-1)}$$

Gilbert-Varshamov "Bound"

An $[\![n, k, 2t+1]\!]$ code does exist whenever

$$\boxed{\frac{k}{n} \geq 1 - H_2\left(\frac{t}{n}\right)}$$

$H_2(p) = -p\log_2 p - (1-p)\log(1-p)$ "Shanon Entropy"