(10) Distance of $T(S) = \min \{ wt(A) : A \in N(S) - S \}$

Pf: Distance of $T(S) = \min \{ wt(F) : PFP \neq cP \}$

Since F = linear combination of Paulis in $\hat{P}_n$, consider $E \in \hat{P}_n$ first.

Case 1: $E \in S$, then $PEP = P$

Case 2: $E \notin N(S)$, then $\forall |\eta\rangle \in \mathbb{C}^{2^n}$

(Q_i: anti com with F)

$$PEP|\eta\rangle = PEQ_iP|\eta\rangle$$
$$= -PQ_iEP|\eta\rangle$$
$$= -PEP|\eta\rangle$$

$\therefore PEP|\eta\rangle = 0 \quad \therefore \quad PEP = 0 = c \cdot P$.

Case 3: $E \in N(S) - S$.

- Let $F = \sum_{E_i \in S} a_i E_i + \sum_{E_j \in N(S)-S} b_j E_j + \sum_{E_k \notin N(S)} h_k E_k$. attains min in dist of $T(S)$.
- We have $PFP = \sum_{E_i \in S} a_i P + \sum_{E_j \in N(S)-S} b_j P E_j P$
- Cannot have $b_j = 0 \ \forall j$ else $PFP = c \cdot P$ contradiction

$\therefore wt(F) \geq \min_{E_j \in N(S)-S} wt(E_j)$

- Meanwhile $\forall E_j \in N(S)-S$, $PE_jP \neq cP$

$\therefore$ Dist $T(S) = \min \{ wt(A) : A \in N(S) - S \}$

eg. $n=4$, $m=2$. $g_1 = XXXX$
$g_2 = ZZZZ$

Encodes 2-qubits.

Let $\bar{Z}_1 = ZZII$, $\bar{Z}_2 = ZIZI$

Let $\bar{X}_1 = XIXI$, $\bar{X}_2 = IIXX$

(Ex: find all possible $\bar{X}_1$
verify the # choices
then take $\bar{X}_1 = XIXI$
find all possible $\bar{X}_2$
verify the # choices).

$|\bar{0}\bar{0}\rangle \propto \frac{1}{16}(IIII+ZZII)(IIII+ZIZI)(IIII+XXXX)(IIII+ZZZZ)|0000\rangle$

$|\bar{0}\bar{0}\bar{0}\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ (trick: more Z's to the right).

$|\bar{0}\bar{1}\rangle = \bar{X}_2|\bar{0}\bar{0}\rangle = \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle)$

$|\bar{1}\bar{0}\rangle = \bar{X}_1|\bar{0}\bar{0}\rangle = \frac{1}{\sqrt{2}}(|0101\rangle + |1010\rangle)$

$|\bar{1}\bar{1}\rangle = \bar{X}_1\bar{X}_2|\bar{0}\bar{0}\rangle = \frac{1}{\sqrt{2}}(|0110\rangle + |1001\rangle)$

$S = \{IIII, XXXX, ZZZZ, YYYY\}$.

$N(S)/S = \{\bar{I}\bar{I}, \bar{I}\bar{X}, \bar{I}\bar{Z}, \bar{I}\bar{Y}, \bar{X}\bar{I}, \bar{X}\bar{X}, \bar{X}\bar{Y}, \bar{X}\bar{Z},$
$\bar{Z}\bar{I}, \bar{Z}\bar{X}, \bar{Z}\bar{Z}, \bar{Z}\bar{Y}, \bar{Y}\bar{I}, \bar{Y}\bar{X}, \bar{Y}\bar{Y}, \bar{Y}\bar{Z}\}$.

Ex: find the 4 coset reps for $\hat{P}_4/N(S)$.

Distance = 2 since all wt 1 Pauli anti com with g_1 or g_2.

• CSS codes (Calderbank-Shor-Steane)

Note that if $Q_1, Q_2, \ldots, Q_m$ generate S
then $Q_1Q_2, Q_2, \ldots, Q_m$ also generate S.

A stabilizer code $T(S)$ is a CSS code
if $\exists$ set of stabilizer generators each is either tensor product of I, X or I, Z

eg. Shor 9-bit code (6 Z-generators, 2 X-generators)

eg. 4-bit code (1 Z-generator, 1 X-generator).

These 2 generators have the same form

eg. Steane 7-bit code:

Stabilizer generators:

$Q_1 = I\ I\ I\ X\ X\ X\ X$
$Q_2 = I\ X\ X\ I\ I\ X\ X$
$Q_3 = X\ I\ X\ I\ X\ I\ X$

parity check matrix for 7-bit Hamming code

$Q_4 = 1\ 1\ 1\ Z\ Z\ Z\ Z$
$Q_5 = 1\ Z\ Z\ 1\ 1\ Z\ Z$
$Q_6 = Z\ 1\ Z\ 1\ Z\ 1\ Z$

The same, so these locate where an X-error occurs

Note that we need $HH^T = 0$ for the Hamming code for these generators to commute.

if a Z-error occurs on the ith qubit, and $s_1s_2s_3$ is the binary rep of i then meas outcome: $(-1)^{s_1}\ (-1)^{s_2}\ (-1)^{s_3}$

This is a wonderful code for fault-tolerance — it has nice encoded operations.

eg. 5-bit code is NOT CSS.

Pf: Ex.

Intuition: CSS codes correct X & Z errors separately.

Erasure error: $N(\rho) = |e\rangle\langle e|$ where $|e\rangle$ is orthogonal to the input space.

ie input is "erased" and you know it.

For n qubits, "m erasure errors" for $m \le n$ means m qubits are subject to the erasure error, the rest go through the noiseless channel, and we do not know up front which m qubits will be erased, but we can tell afterwards.

Formally: $N_{n,m} = \sum_{R = m\text{-subset of } [n]} (N^{\otimes m})_R \; (I^{\otimes(n-m)})_{\bar{R}} \; P_R$

$\bar{R}$: complement of R

Prop: a distance d code can correct up to $d-1$ erasure errors.

Pf: ① After the noise process, determine which subset R is erased, $|R| \le d-1$

② Replace each erased qubit by $|0\rangle$.

③ Refine error set $\mathcal{E}_R$ = all possible Pauli errors on R & no error on $\bar{R}$

④ $\forall E_i, E_j \in \mathcal{E}$, $P E_i^\dagger E_j P = c_{ij} P$

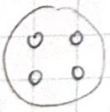
$E_i^\dagger E_j$: wt $\le |R| \le d-1$; P: code distance $= d$.

$\therefore$ QECC condition met for $\mathcal{E}_R$.

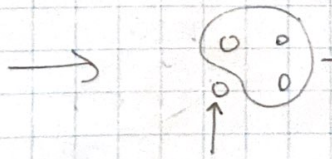
$\therefore \exists$ decoder that return the input.

↑ this depends on R !!

eg. 4-qubit code corrects up to 1 erasure error.
5 2



Any 3 qubits suffice to decode the 2 encoded qubits.



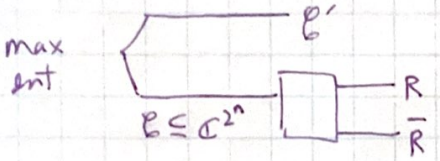
remaining qubit has no info on the encoded qubits.

Prop: QECC corrects erasure errors on the set of qubit R

($\Leftrightarrow$) $\forall |\psi\rangle \in \mathcal{C}$, $\mathrm{Tr}_{\bar{R}} |\psi\rangle\langle\psi|$ indep of $|\psi\rangle$

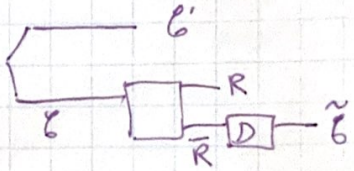
$\Leftrightarrow$ $\forall F$ trivial on $\bar{R}$, $\forall |\psi\rangle \in \mathcal{C}$, $\langle\psi|F|\psi\rangle$ indep of $|\psi\rangle$

Decoupling Lemma (Hayden):



If $\mathcal{E}'\bar{R}$ in product state

$\exists D$ on $\bar{R}$ s.t.



* If $\mathcal{E}'\bar{R}$ approx in product state

$\exists D$ on $\bar{R}$ s.t. $\mathcal{E}'\tilde{\mathcal{E}}$ approx in max ent state

ie D approx reverses $-\square\!\!\subset$.

$\mathcal{E}'\tilde{\mathcal{E}}$ max entangled.

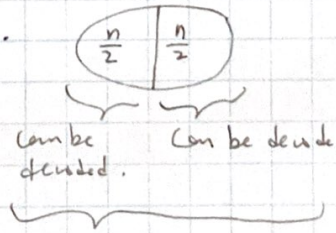
ie $\mathcal{E} \to \tilde{\mathcal{E}}$ identity channel.

ie $-\square\!\!\subset$ reversed.

Remark: Q secret sharing schemes are erasure codes.

Cor: If block length $= n$, dist $d < \frac{n}{2}+1$

Pf: If not, $d-1 \geq \frac{n}{2}$.



2 copies of the input, contradiction.

eg. $n=5$, $\frac{n}{2}+1 = 3.5$.

$n=4$, $\frac{n}{2}+1 = 3$.

∴ Our examples of 5-qubit code & 4-qubit code both have max distance

Reading: error detection code, bounds.