9. Combating noise: quantum error correcting codes

(NC 10.1-10.3, 10.5, M 5, KLM 10)

(a) Classical noise model

(b) 3-bit repetition code

(c) Quantum noise model

(d) Quantum 3-bit repetition code for X errors

(e) Shor 9-bit code for arbitrary Pauli error

(g) Discretization and sufficient conditions for QECC

(h) Stabilizer formalism -- quantum parity checks !

(i) Shor 9-bit code reloaded

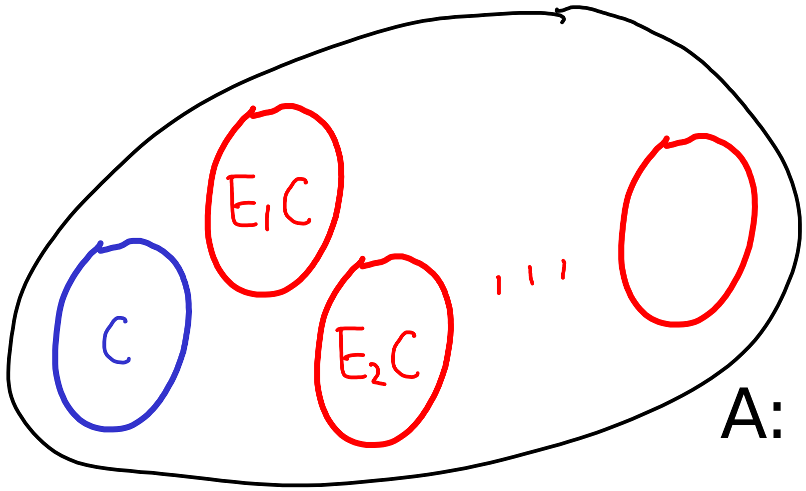
(j) Sufficient conditions for QECC for stabilizer codes

(l) 7-bit Steane code

(m) Erasure errors, q secret sharing, AdS/CFT corr

We saw how the 9-bit Shor code corrects up to one Pauli error and saw an example of discretization of error.

Idea:



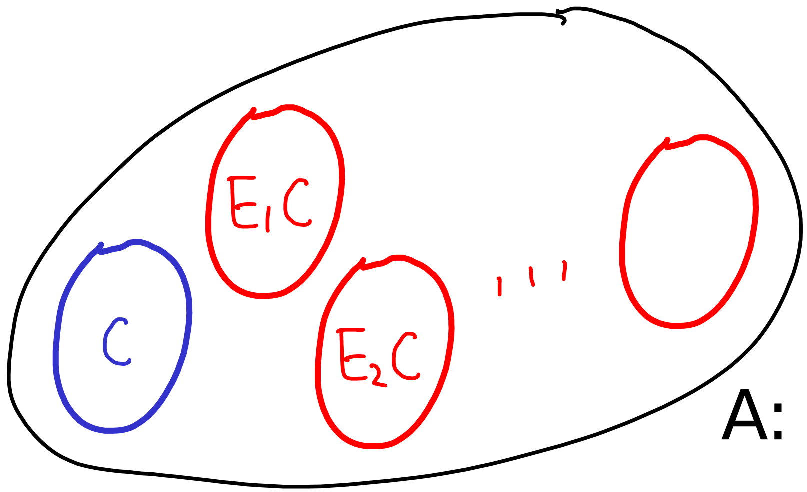
A: ambient space

C: codespace

$E_0 = I$, E_1, E_2, $\cdots$ unitary errors to identify and revert

We saw how the 9-bit Shor code corrects up to one Pauli error and saw an example of discretization of error.

Idea:



A: ambient space

C: codespace

$E_0 = I$, E_1, E_2, $\cdots$ unitary errors to identify and revert

E_i : determined by noise processes and block length

C chosen so that Ei takes C to orthogonal spaces Ei C, so, we can identify which Ei occurs and revert it.

* What about errors with non-unitary Kraus operators, e.g., amplitude damping or erasures?

* If we identify the error, can we revert them?

* How well discretization work?

* How to design, describe, and verify QECC?

Necessary and sufficient condition for QECC

Let P be the projector onto the codespace C $\subseteq$ A and E_i be a list of operators acting on A. Then,

$\forall i,j \quad P E_i^\dagger E_j P = m_{ij} P$ where $m_{ij} = (i,j)$-entry of some matrix $m \geq 0$

iff

what we offer in the code

Necessary and sufficient condition for QECC

Let P be the projector onto the codespace $C \subseteq A$ and E_i be a list of operators acting on A. Then,

$\forall i,j \quad P E_i^\dagger E_j P = m_{ij} P$ where $m_{ij} = (i,j)$-entry of some matrix $m \geq 0$

iff

$\forall \mathcal{E}$ CP with Kraus operators $A_k \in \operatorname{span}\{E_i\}$, $\sum_k A_k^\dagger A_k \leq I$

$\exists R$ TCP $\forall \rho$ s.t. $P\rho P = \rho$, $R(\mathcal{E}(\rho)) = \frac{\operatorname{tr}\mathcal{E}(\rho)}{\operatorname{tr}\rho} \cdot \rho$

ie $\mathcal{E}$ can be reversed on C! ie C corrects $\mathcal{E}$!

what error we can correct

Necessary and sufficient condition for QECC

Let P be the projector onto the codespace $C \subseteq A$ and E_i be a list of operators acting on A. Then,

$\forall i,j \quad P E_i^\dagger E_j P = m_{ij} P$ where $m_{ij} = (i,j)$-entry of some matrix $m \geq 0$

iff

$\forall\, \mathcal{E}$ CP with Kraus operators $A_k \in \operatorname{span}\{E_i\}$, $\sum_k A_k^\dagger A_k \leq I$

$\exists R$ TCP $\forall \rho$ s.t. $P\rho P = \rho$, $R(\mathcal{E}(\rho)) = \frac{\operatorname{tr} \mathcal{E}(\rho)}{\operatorname{tr} \rho} \cdot \rho$

ie $\mathcal{E}$ can be reversed on C! ie C corrects $\mathcal{E}$!

NB. Ei's: what we identify, Ak's: what we correct.
Neither needs to be unitary.

Something simpler suffices for us ...

Sufficient condition for QECC

Let P be the projector onto the codespace C $\subseteq$ A and E_i be a list of unitary operators acting on A.

If $\forall\, i,j \quad P E_i^\dagger E_j P = P\, \delta_{ij}\, m_i$ where $m_i \geq 0$

then

$\forall\, \mathcal{E}$ CP with Kraus operators $A_k \in \operatorname{span}\{E_i\}$

$\exists\, R$ TCP s.t. $\forall \rho$ s.t. $P\rho P = \rho$, $\operatorname{tr}\rho = 1$, $R(\mathcal{E}(\rho)) = \rho \operatorname{tr} \mathcal{E}(\rho)$

Something simpler suffices for us ...

Sufficient condition for QECC

Let P be the projector onto the codespace $C \subseteq A$ and E_i be a list of unitary operators acting on A.

If $\forall\, i,j \quad P E_i^\dagger E_j P = P\, \delta_{ij}\, m_i \quad$ where $m_i \geq 0$

then

$\forall\, \mathcal{E}$ CP with Kraus operators $A_k \in \mathrm{span}\{E_i\}$

$\exists\, R$ TCP s.t. $\forall \rho$ s.t. $P \rho P = \rho$, $\mathrm{tr}\,\rho = 1$, $R(\mathcal{E}(\rho)) = \rho\, \mathrm{tr}\, \mathcal{E}(\rho)$

NB. With this sufficient condition, QECCs designed for unitary errors Ei's (in particular Pauli errors) correct arbitrary Ak's in their span (general discretization).

Interpreting the sufficient condition:

$\forall\, i,j \quad P E_i^\dagger E_j P = P\, \delta_{ij}\, m_i \quad$ where $m_i \geq 0$

(1) Orthogonality:

For i≠j, Ei, Ej take the code space C to ortho spaces.

Interpreting the sufficient condition:

$\forall\, i,j \quad P E_i^{\dagger} E_j P = P\, \delta_{ij}\, m_i \quad$ where $m_i \geq 0$

(1) Orthogonality:

For i≠j, Ei, Ej take the code space C to ortho spaces.

Let $|\psi_L\rangle, |\phi_L\rangle \in C$. Consider $E_i|\psi_L\rangle$, $E_j|\phi_L\rangle$.

Then $\langle\psi_L| E_i^{\dagger} E_j |\phi_L\rangle = \langle\psi_L| P E_i^{\dagger} E_j P |\phi_L\rangle = 0$

since $P|\psi_L\rangle = |\psi_L\rangle$ etc $\qquad \delta_{ij}$

Interpreting the sufficient condition:

$$\forall\, i,j \quad P E_i^\dagger E_j P = P\, \delta_{ij}\, m_i \quad \text{where } m_i \geq 0$$

(1) Orthogonality:

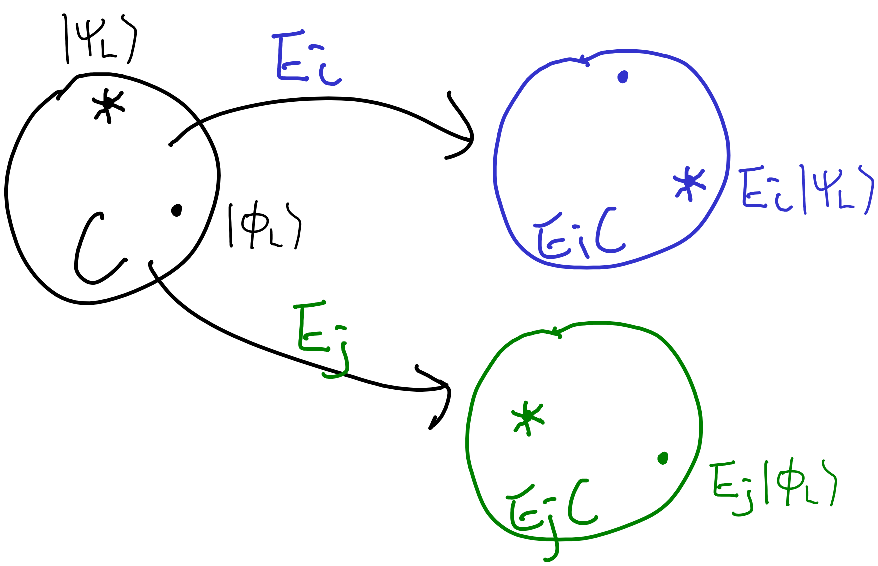
For $i \neq j$, E_i, E_j take the code space C to ortho spaces.

Let $|\psi_L\rangle, |\phi_L\rangle \in C$. Consider $E_i|\psi_L\rangle$, $E_j|\phi_L\rangle$.

Then $\langle\psi_L|E_i^\dagger E_j|\phi_L\rangle = \langle\psi_L|P E_i^\dagger E_j P|\phi_L\rangle = 0$

since $P|\psi_L\rangle = |\psi_L\rangle$ etc

δ_{ij}



Interpreting the sufficient condition:

$$\forall\, i,j \quad P E_i^\dagger E_j P = P\, \delta_{ij}\, m_i \qquad \text{where } m_i \geq 0$$

(2) Non-deformation (even for non-unitary Ei's):
For each i, Ei preserves inner product on C.

Interpreting the sufficient condition:

$\forall i,j \quad P E_i^\dagger E_j P = P \, \delta_{ij} \, m_i \quad$ where $m_i \geq 0$

(2) Non-deformation (even for non-unitary Ei's):
For each i, Ei preserves inner product on C.

Let $|\psi_L\rangle, |\phi_L\rangle \in C$. Consider $E_i |\psi_L\rangle$, $E_i |\phi_L\rangle$.

Then $\langle \psi_L | E_i^\dagger E_i | \phi_L \rangle =$

Interpreting the sufficient condition:

$\forall\, i,j \quad P E_i^{\dagger} E_j P = P\, \delta_{ij}\, m_i \quad$ where $m_i \geq 0$

(2) Non-deformation (even for non-unitary Ei's):
For each i, Ei preserves inner product on C.

Let $|\psi_L\rangle, |\phi_L\rangle \in C$. Consider $E_i|\psi_L\rangle$, $E_i|\phi_L\rangle$.

Then $\langle\psi_L|E_i^{\dagger} E_i|\phi_L\rangle = \langle\psi_L|P E_i^{\dagger} E_i P|\phi_L\rangle$

Interpreting the sufficient condition:

$$\forall\, i,j \quad P E_i^\dagger E_j P = P\, \delta_{ij}\, m_i \quad \text{where } m_i \geq 0$$

(2) Non-deformation (even for non-unitary Ei's):
For each i, Ei preserves inner product on C.

Let $|\psi_L\rangle, |\phi_L\rangle \in C$. Consider $E_i|\psi_L\rangle$, $E_i|\phi_L\rangle$.

Then $\langle\psi_L|E_i^\dagger E_i|\phi_L\rangle = \langle\psi_L|P E_i^\dagger E_i P|\phi_L\rangle$

$$= \langle\psi_L|\, m_i P\, |\phi_L\rangle = m_i \langle\psi_L|\phi_L\rangle$$

independent of the states $|\psi_L\rangle, |\phi_L\rangle$

Interpreting the sufficient condition:

$$\forall\, i,j \quad P E_i^\dagger E_j P = P\, \delta_{ij}\, m_i \quad \text{where } m_i \geq 0$$

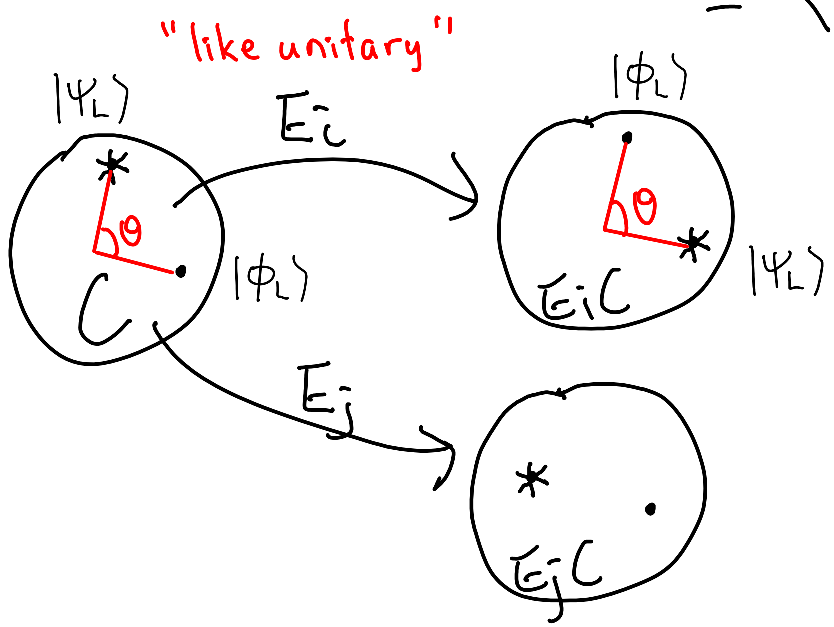
(2) Non-deformation (even for non-unitary Ei's):
For each i, Ei preserves inner product on C.

Let $|\psi_L\rangle, |\phi_L\rangle \in C$. Consider $E_i|\psi_L\rangle$, $E_i|\phi_L\rangle$.

Then $\langle\psi_L|E_i^\dagger E_i|\phi_L\rangle = \langle\psi_L|P E_i^\dagger E_i P|\phi_L\rangle$

$= \langle\psi_L|\, m_i P\, |\phi_L\rangle = m_i \langle\psi_L|\phi_L\rangle$

independent of the states



Interpreting the sufficient condition:

$$\forall i,j \quad P E_i^\dagger E_j P = P \, \delta_{ij} \, m_i \quad \text{where } m_i \geq 0$$

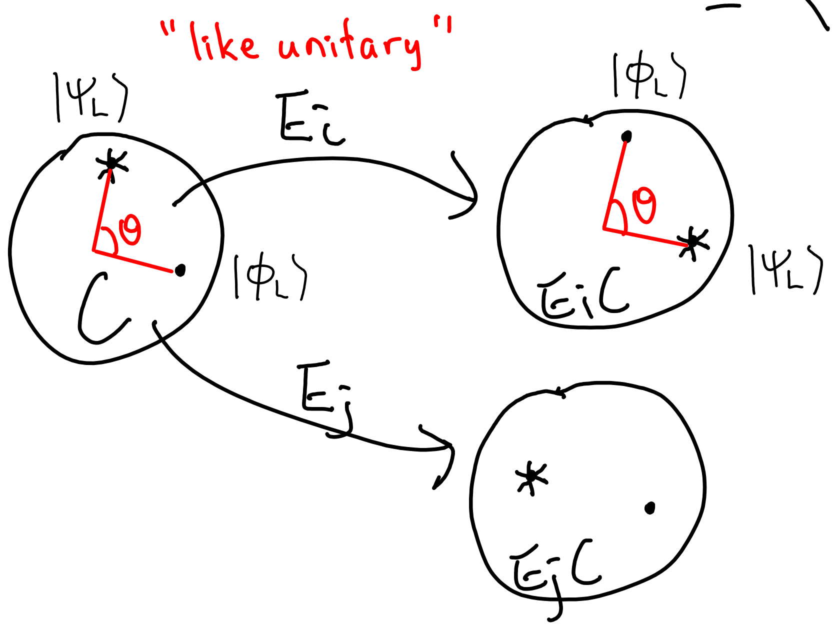
(2) Non-deformation (even for non-unitary Ei's):
For each i, Ei preserves inner product on C.

Let $|\psi_L\rangle, |\phi_L\rangle \in C$. Consider $E_i|\psi_L\rangle$, $E_i|\phi_L\rangle$.

Then $\langle\psi_L|E_i^\dagger E_i|\phi_L\rangle = \langle\psi_L|P E_i^\dagger E_i P|\phi_L\rangle$

$= \langle\psi_L| m_i P |\phi_L\rangle = m_i \langle\psi_L|\phi_L\rangle$

independent of the states



In fact $P E_i^\dagger E_i P = m_i P$

$\Rightarrow \quad E_i P = \sqrt{m_i}\, U_i P$

So we can revert using $U_i^\dagger$.

Claim: If $\forall\, i,j \quad P E_i^\dagger E_j P = P\, \delta_{ij}\, m_i \quad$ where $m_i \geq 0$

then $\forall\, \mathcal{E}$ CP with Kraus operators $A_k \in \operatorname{span}\{E_i\}$

$\exists R$ TCP s.t. $\forall \rho$ s.t. $P\rho P = \rho$, $\operatorname{tr}\rho = 1$, $R(\mathcal{E}(\rho)) = \rho \operatorname{tr} \mathcal{E}(\rho)$

Proof:

If Ei's are unitary, projector onto $E_i C = E_i P E_i^\dagger =: P_i$

Claim: If $\forall\, i,j \quad P E_i^\dagger E_j P = P \,\delta_{ij}\, m_i$ where $m_i \geq 0$

then $\forall\, \mathcal{E}$ CP with Kraus operators $A_k \in \mathrm{span}\{E_i\}$

$\exists\, R$ TCP s.t. $\forall \rho$ s.t. $P\rho P = \rho$, $\mathrm{tr}\,\rho = 1$, $R(\mathcal{E}(\rho)) = \rho\, \mathrm{tr}\, \mathcal{E}(\rho)$

Proof:

If Ei's are unitary, projector onto $E_i C = E_i P E_i^\dagger =: P_i$

Reason: $\forall\, |\psi_L\rangle \in C$,

$P_i\, E_i |\psi_L\rangle =$

$E_i |\psi_L\rangle$

Claim: If $\forall i,j \quad P E_i^\dagger E_j P = P \delta_{ij} m_i$ where $m_i \geq 0$

then $\forall \mathcal{E}$ CP with Kraus operators $A_k \in \text{span}\{E_i\}$

$\exists R$ TCP s.t. $\forall \rho$ s.t. $P\rho P = \rho$, $\text{tr}\,\rho = 1$, $R(\mathcal{E}(\rho)) = \rho \, \text{tr}\, \mathcal{E}(\rho)$

Proof:

If Ei's are unitary, projector onto $E_i C = E_i P E_i^\dagger =: P_i$

Reason: $\forall |\psi_L\rangle \in C$,

$$P_i E_i |\psi_L\rangle = E_i P E_i^\dagger E_i |\psi_L\rangle$$

Claim: If $\forall\, i,j \quad P E_i^\dagger E_j P = P\, \delta_{ij}\, m_i$ where $m_i \geq 0$

then $\forall\, \mathcal{E}$ CP with Kraus operators $A_k \in \operatorname{span}\{E_i\}$

$\exists R$ TCP s.t. $\forall \rho$ s.t. $P\rho P = \rho$, $\operatorname{tr}\rho = 1$, $R(\mathcal{E}(\rho)) = \rho \operatorname{tr} \mathcal{E}(\rho)$

Proof:

If Ei's are unitary, projector onto $E_i C = E_i P E_i^\dagger =: P_i$

Reason: $\forall\, |\psi_L\rangle \in C$,

$$P_i\, E_i|\psi_L\rangle = E_i P E_i^\dagger E_i |\psi_L\rangle$$

$$= E_i P |\psi_L\rangle = E_i |\psi_L\rangle$$

by the simplifying assumption Ei unitary

$\because |\psi_L\rangle \in C$

Claim: If $\forall i,j \ \ P E_i^\dagger E_j P = P \, \delta_{ij} \, m_i$ where $m_i \geq 0$

then $\forall \mathcal{E}$ CP with Kraus operators $A_k \in \mathrm{span}\{E_i\}$

$\exists R$ TCP s.t. $\forall \rho$ s.t. $P \rho P = \rho$, $\mathrm{tr}\,\rho = 1$, $R(\mathcal{E}(\rho)) = \rho \, \mathrm{tr}\, \mathcal{E}(\rho)$

Proof:

If Ei's are unitary, projector onto $E_i C = E_i P E_i^\dagger =: P_i$

if $i \neq j$, $P_i P_j = E_i P E_i^\dagger E_j P E_j^\dagger = 0$, so $\{P_i\}_{i=1}^{r}$ ortho.

range for E_i's

Claim: If $\forall i,j \ P E_i^\dagger E_j P = P \delta_{ij} m_i$ where $m_i \geq 0$

then $\forall \mathcal{E}$ CP with Kraus operators $A_k \in \text{span}\{E_i\}$

$\exists R$ TCP s.t. $\forall \rho$ s.t. $P\rho P = \rho$, $\operatorname{tr}\rho = 1$, $R(\mathcal{E}(\rho)) = \rho \operatorname{tr}\mathcal{E}(\rho)$

Proof:

If Ei's are unitary, projector onto $E_i C = E_i P E_i^\dagger =: P_i$

if $i \neq j$, $P_i P_j = E_i P E_i^\dagger E_j P E_j^\dagger = 0$, so $\{P_i\}_{i=1}^r$ ortho.

range for E_i's

Syndrome measurement $\mathcal{M}$ has projectors:

$P_1, P_2, \cdots, P_r$, $P_{r+1} = I - \sum_{i=1}^{r+1} P_i$, $\mathcal{M}(\sigma) = \sum_{i=1}^{r+1} P_i \sigma P_i \otimes |i\rangle\langle i|$

Claim: If $\forall\, i,j \quad P E_i^\dagger E_j P = P \, \delta_{ij}\, m_i$ where $m_i \geq 0$

then $\forall\, \mathcal{E}$ CP with Kraus operators $A_k \in \mathrm{span}\{E_i\}$

$\exists\, R$ TCP s.t. $\forall \rho$ s.t. $P\rho P = \rho$, $\mathrm{tr}\,\rho = 1$, $R(\mathcal{E}(\rho)) = \rho \, \mathrm{tr}\, \mathcal{E}(\rho)$

Proof:

If Ei's are unitary, projector onto $E_i C = E_i P E_i^\dagger =: P_i$

if $i \neq j$, $P_i P_j = E_i P E_i^\dagger E_j P E_j^\dagger = 0$, so $\{P_i\}_{i=1}^{r}$ ortho.

range for E_i's

Syndrome measurement $\mathcal{M}$ has projectors:

$P_1, P_2, \cdots, P_r, \quad P_{r+1} = I - \sum_{i=1}^{r+1} P_i, \qquad \mathcal{M}(\sigma) = \sum_{i=1}^{r+1} P_i \sigma P_i \otimes |i\rangle\langle i|$

Let $\tilde{R}(\sigma) = \sum_{i=1}^{r+1} V_i P_i \sigma P_i V_i^\dagger \otimes |i\rangle\langle i|, \quad V_i = E_i^\dagger, \; i = 1, \ldots, r$

$V_{r+1} = I$

i.e., measure which Ei, then revert.

Let $\tilde{R}(\sigma) = \sum_{i=1}^{r+1} V_i P_i \sigma P_i V_i^{+} \otimes |i\rangle\langle i|$, $V_i = E_i^{+}$, $i = 1, \ldots, r$

$V_{r+1} = I$

Checking $\tilde{R}$ is TCP:

Let $\tilde{R}(\sigma) = \sum_{i=1}^{r+1} V_i P_i \sigma P_i V_i^{\dagger} \otimes |i\rangle\langle i|$, $V_i = E_i^{\dagger}$, $i = 1, \ldots, r$

$V_{r+1} = I$

Checking $\tilde{R}$ is TCP:

1. $\tilde{R}$ has a Kraus representation, so linear and CP.

Let $\tilde{R}(\sigma) = \sum_{i=1}^{r+1} V_i P_i \sigma P_i V_i^{\dagger} \otimes |i\rangle\langle i|$, $\quad V_i = E_i^{\dagger}$, $i = 1, \ldots, r$

$V_{r+1} = I$

Checking $\tilde{R}$ is TCP:

1. $\tilde{R}$ has a Kraus representation, so linear and CP.

2. $\mathrm{tr}\, \tilde{R}(\sigma) = \mathrm{tr} \sum_{i=1}^{r+1} V_i P_i \sigma P_i V_i^{\dagger} \otimes |i\rangle\langle i|$

Let $\tilde{R}(\sigma) = \sum_{i=1}^{r+1} V_i P_i \sigma P_i V_i^\dagger \otimes |i\rangle\langle \bar{i}|$, $V_i = E_i^\dagger$, $i = 1, \dots, r$

$V_{r+1} = I$

Checking $\tilde{R}$ is TCP:

1. $\tilde{R}$ has a Kraus representation, so linear and CP.

2. $\operatorname{tr} \tilde{R}(\sigma) = \operatorname{tr} \sum_{i=1}^{r+1} V_i P_i \sigma P_i V_i^\dagger \otimes |i\rangle\langle \bar{i}|$

$$= \sum_{i=1}^{r+1} \left(\operatorname{tr} P_i V_i^\dagger V_i P_i \sigma \right) \cdot \langle \bar{i} | i \rangle$$

Let $\tilde{R}(\sigma) = \sum_{i=1}^{r+1} V_i P_i \sigma P_i V_i^\dagger \otimes |i\rangle\langle i|$, $V_i = E_i^\dagger$, $i = 1, \dots, r$

$V_{r+1} = I$

Checking $\tilde{R}$ is TCP:

1. $\tilde{R}$ has a Kraus representation, so linear and CP.

2. $\operatorname{tr} \tilde{R}(\sigma) = \operatorname{tr} \sum_{i=1}^{r+1} V_i P_i \sigma P_i V_i^\dagger \otimes |i\rangle\langle i|$

$$= \sum_{i=1}^{r+1} \left(\operatorname{tr} P_i V_i^\dagger V_i P_i \sigma \right) \cdot \langle i | i \rangle$$

$$= \sum_{i=1}^{r+1} \left(\operatorname{tr} P_i \sigma \right) \qquad (\because V_i^\dagger V_i = I, \ P_i P_i = P_i)$$

Let $\tilde{R}(\sigma) = \sum_{i=1}^{r+1} V_i P_i \sigma P_i V_i^{+} \otimes |i\rangle\langle i|$, $\quad V_i = E_i^{+}$, $i = 1, \dots, r$

$V_{r+1} = I$

Checking $\tilde{R}$ is TCP:

1. $\tilde{R}$ has a Kraus representation, so linear and CP.

2. $$\mathrm{tr}\,\tilde{R}(\sigma) = \mathrm{tr} \sum_{i=1}^{r+1} V_i P_i \sigma P_i V_i^{+} \otimes |i\rangle\langle i|$$

$$= \sum_{i=1}^{r+1} \left(\mathrm{tr}\, P_i V_i^{+} V_i P_i \sigma\right) \cdot \langle i|i\rangle$$

$$= \sum_{i=1}^{r+1} \left(\mathrm{tr}\, P_i \sigma\right) \qquad \left(\because V_i^{+} V_i = I,\ P_i P_i = P_i\right)$$

$$= \mathrm{tr} \sum_{i=1}^{r+1} P_i \sigma = \mathrm{tr}\, \sigma \qquad \left(\because \sum_{i=1}^{r+1} P_i = I\right)$$

So, $\tilde{R}$ trace preserving.

Claim: If $\forall i,j \; P E_i^\dagger E_j P = P \, \delta_{ij} \, m_i$ where $m_i \geq 0$

then $\forall \mathcal{E}$ CP with Kraus operators $A_k \in \operatorname{span}\{E_i\}$

$\exists R$ TCP s.t. $\forall \rho$ s.t. $P\rho P = \rho$, $\operatorname{tr}\rho = 1$, $R(\mathcal{E}(\rho)) = \rho \operatorname{tr} \mathcal{E}(\rho)$

$$\tilde{R}(\sigma) = \sum_{i=1}^{r+1} V_i P_i \sigma P_i V_i^\dagger \otimes |i\rangle\langle i| ,$$

$V_i = E_i^\dagger$, $i = 1, \ldots, r$

$V_{r+1} = I$

$$R(\sigma) = \operatorname{tr}_2 \tilde{R}(\sigma)$$

$\tilde{R}$ TCP $\Rightarrow$ R TCP.

Claim: If $\forall\, i,j \quad P E_i^\dagger E_j P = P\, \delta_{ij}\, m_i$ where $m_i \geq 0$

then $\forall\, \mathcal{E}$ CP with Kraus operators $A_k \in \operatorname{span}\{E_i\}$

$\exists\, R$ TCP s.t. $\forall \rho$ s.t. $P\rho P = \rho$, $\operatorname{tr}\rho = 1$, $R(\mathcal{E}(\rho)) = \rho \operatorname{tr} \mathcal{E}(\rho)$

$$\tilde{R}(\sigma) = \sum_{i=1}^{r+1} V_i P_i \sigma P_i V_i^\dagger \otimes |i\rangle\langle i|, \qquad A_k = \sum_{j=1}^{r} b_{jk} E_j$$

$$V_i = E_i^\dagger, \quad i = 1, \ldots, r$$

$$V_{r+1} = I$$

$$R(\sigma) = \operatorname{tr}_2 \tilde{R}(\sigma)$$

showing this next

$\tilde{R}$ TCP $\Rightarrow$ R TCP.

$\forall \rho$ s.t. $P \rho P = \rho$,

$$\tilde{R}(\mathcal{E}(\rho)) = \sum_{i=1}^{r+1} V_i P_i \sum_k A_k \rho A_k^\dagger P_i V_i^\dagger \otimes |i\rangle\langle \bar{i}|$$

$\forall \rho$ s.t. $P \rho P = \rho$,

$$\tilde{R}(\mathcal{E}(\rho)) = \sum_{i=1}^{r+1} V_i P_i \sum_k A_k \rho A_k^\dagger P_i V_i^\dagger \otimes |i\rangle\langle \bar{i}|$$

$A_k \in \mathrm{span}\{E_i\}$

$$= \sum_{i=1}^{r+1} V_i P_i \sum_k \sum_{j=1}^{r} b_{jk} E_j \, \rho \sum_{l=1}^{r} b_{lk}^* E_l^\dagger P_i V_i^\dagger \otimes |i\rangle\langle \bar{i}|$$

$\forall \rho$ s.t. $P \rho P = \rho$,

$$\tilde{R}(\mathcal{E}(\rho)) = \sum_{i=1}^{r+1} V_i P_i \sum_k A_k \rho A_k^\dagger P_i V_i^\dagger \otimes |i\rangle\langle \bar{i}|$$

$A_k \in \mathrm{span}\{E_i\}$ $\longrightarrow$
$$= \sum_{i=1}^{r+1} V_i P_i \sum_k \sum_{j=1}^{r} b_{jk} E_j \rho \sum_{l=1}^{r} b_{lk}^* E_l^\dagger P_i V_i^\dagger \otimes |i\rangle\langle \bar{i}|$$

$$= \sum_k \sum_{j=1}^{r} \sum_{l=1}^{r} b_{jk} b_{lk}^* \sum_{i=1}^{r+1} V_i P_i E_j \rho E_l^\dagger P_i V_i^\dagger \otimes |i\rangle\langle \bar{i}|$$

$$\forall \rho \text{ s.t. } P\rho P = \rho,$$

$$\tilde{R}(\mathcal{E}(\rho)) = \sum_{i=1}^{r+1} V_i P_i \sum_k A_k \rho A_k^\dagger P_i V_i^\dagger \otimes |i\rangle\langle i|$$

$A_k \in \text{span}\{E_i\} \longrightarrow$

$$= \sum_{i=1}^{r+1} V_i P_i \sum_k \sum_{j=1}^{r} b_{jk} E_j \rho \sum_{l=1}^{r} b_{lk}^* E_l^\dagger P_i V_i^\dagger \otimes |i\rangle\langle i|$$

$$= \sum_k \sum_{j=1}^{r} \sum_{l=1}^{r} b_{jk} b_{lk}^* \sum_{i=1}^{r+1} \underbrace{V_i P_i E_j \rho E_l^\dagger P_i V_i^\dagger}_{V_i E_i \underbrace{P E_i^\dagger E_j P}_{m_i P \delta_{ij}} \rho \underbrace{P E_l^\dagger E_i P}_{m_i P \delta_{il}} E_i^\dagger V_i^\dagger} \otimes |i\rangle\langle i|$$

(holds even for $i = r+1$)

$\forall \rho$ s.t. $P\rho P = \rho$,

$$\tilde{R}(\mathcal{E}(\rho)) = \sum_{i=1}^{r+1} V_i P_i \sum_k A_k \rho A_k^\dagger P_i V_i^\dagger \otimes |i\rangle\langle \bar{i}|$$

$A_k \in \mathrm{span}\{E_i\}$ $\longrightarrow$ $$= \sum_{i=1}^{r+1} V_i P_i \sum_k \sum_{j=1}^{r} b_{jk} E_j \rho \sum_{l=1}^{r} b_{lk}^* E_l^\dagger P_i V_i^\dagger \otimes |i\rangle\langle \bar{i}|$$

$$= \sum_k \sum_{j=1}^{r} \sum_{l=1}^{r} b_{jk} b_{lk}^* \sum_{i=1}^{r+1} \underbrace{V_i P_i E_j \rho E_l^\dagger P_i V_i^\dagger}_{V_i E_i P E_i^\dagger E_j P \rho P E_l^\dagger E_i P E_i^\dagger V_i^\dagger} \otimes |i\rangle\langle \bar{i}|$$

$$V_i E_i \underbrace{P E_i^\dagger E_j P}_{m_i P \delta_{ij}} \rho \underbrace{P E_l^\dagger E_i P}_{m_i P \delta_{il}} E_i^\dagger V_i^\dagger \quad \text{(holds even for } i = r+1\text{)}$$

discretization of error from A_k to E_i, m collapses sum of Ej's to 1 Ei !

$$= \sum_k \sum_{i=1}^{r} |b_{ik}|^2 V_i E_i m_i P \rho m_i P E_i^\dagger V_i^\dagger \otimes |i\rangle\langle \bar{i}|$$

$\forall \rho$ s.t. $P \rho P = \rho$,

$$\tilde{R}(\mathcal{E}(\rho)) = \sum_{i=1}^{r+1} V_i P_i \sum_k A_k \rho A_k^\dagger P_i V_i^\dagger \otimes |i\rangle\langle i|$$

$A_k \in \mathrm{span}\{E_i\}$

$$= \sum_{i=1}^{r+1} V_i P_i \sum_k \sum_{j=1}^{r} b_{jk} E_j \rho \sum_{l=1}^{r} b_{lk}^* E_l^\dagger P_i V_i^\dagger \otimes |i\rangle\langle i|$$

$$= \sum_k \sum_{j=1}^{r} \sum_{l=1}^{r} b_{jk} b_{lk}^* \sum_{i=1}^{r+1} \underbrace{V_i P_i E_j \rho E_l^\dagger P_i V_i^\dagger} \otimes |i\rangle\langle i|$$

$$V_i E_i \underbrace{P E_i^\dagger E_j P}_{m_i P \delta_{ij}} \rho \underbrace{P E_l^\dagger E_i P}_{m_i P \delta_{il}} E_i^\dagger V_i^\dagger$$

(holds even for $i = r+1$)

discretization of error from A_k to E_i, m collapses sum of Ej's to 1 Ei !

$$= \sum_k \sum_{i=1}^{r} |b_{ik}|^2 V_i E_i m_i P \rho m_i P E_i^\dagger V_i^\dagger \otimes |i\rangle\langle i|$$

$$= \rho \otimes \sum_k \sum_{i=1}^{r} |b_{ik}|^2 |i\rangle\langle i|$$

($m_i = 1$ if E_i unitary)

$\forall \rho$ s.t. $P \rho P = \rho$,

$$R(\mathcal{E}(\rho)) = \mathrm{tr}_2 \, \tilde{R}(\mathcal{E}(\rho))$$

$$= \mathrm{tr}_2 \, \rho \otimes \sum_k \sum_{i=1}^{r} |b_{ik}|^2 \, |i\rangle\langle i|$$

$\forall \rho$ s.t. $P \rho P = \rho$,

$$R(\mathcal{E}(\rho)) = \mathrm{tr}_2\, \tilde{R}(\mathcal{E}(\rho))$$

$$= \mathrm{tr}_2\, \rho \otimes \sum_k \sum_{i=1}^{r} |b_{ik}|^2\, |i\rangle\langle i|$$

$$= \rho \underbrace{\sum_k \sum_{i=1}^{r} |b_{ik}|^2}_{\frac{\mathrm{tr}\,\mathcal{E}(\rho)}{\mathrm{tr}(\rho)} = \mathrm{tr}\,\mathcal{E}(\rho)}$$

$\because$ R is trace preserving

1 by assumption

$\square$

Example how to use the QECC sufficient condition

Consider the channel that reset a qubit to $|0\rangle$ wp p.

$$N(\rho) = (1-p)\,\rho + p\left(A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger\right)$$

where $A_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $A_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

Example how to use the QECC sufficient condition

Consider the channel that reset a qubit to $|0\rangle$ wp p.

$$N(\rho) = (1-p)\,\rho + p\left(A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger\right)$$

where $A_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $A_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

Aside as an exercise: is the above probabilistic reset channel the same as an amplitude damping channel of some value of de-excitation gamma?

To find out, explicitly write down $N(\rho)$ as a 2x2 matrix and compare with the output of the amplitude damping channel from topic08.

Example how to use the QECC sufficient condition

Consider the channel that reset a qubit to $|0\rangle$ wp p.

$$N(\rho) = (1-p)\,\rho + p\left(A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger\right)$$

where $A_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $A_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

The worst case input/output fidelity for the channel,

$$\min_{|\psi\rangle} \operatorname{tr} N(|\psi\rangle\langle\psi|)\, |\psi\rangle\langle\psi|$$

prob to find the output in the space spanned by the input, generalizing fidelity between 2 pure states

$$F^2(|\psi_1\rangle, |\psi_2\rangle) = |\langle\psi_1|\psi_2\rangle|^2$$

$$= \operatorname{tr} |\psi_2\rangle\langle\psi_2|\, |\psi_1\rangle\langle\psi_1|$$

Example how to use the QECC sufficient condition

Consider the channel that reset a qubit to $|0\rangle$ wp p.

$$\mathcal{N}(\rho) = (1-p)\,\rho + p\left(A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger\right)$$

where $A_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $A_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

The worst case input/output fidelity for the channel,

$$\min_{|\psi\rangle} \operatorname{tr} \mathcal{N}(|\psi\rangle\langle\psi|)\, |\psi\rangle\langle\psi| = \operatorname{tr} \mathcal{N}(|1\rangle\langle 1|)\, |1\rangle\langle 1| = 1-p.$$

prob to find the output in the space spanned by the input, generalizing fidelity between 2 pure states

$$F^2(|\psi_1\rangle, |\psi_2\rangle) = |\langle\psi_1|\psi_2\rangle|^2$$

$$= \operatorname{tr} |\psi_2\rangle\langle\psi_2|\, |\psi_1\rangle\langle\psi_1|$$

Ex: show that min attained at $|1\rangle$.

Example how to use the QECC sufficient condition

If we use the 9-bit Shor code, noise process is $\mathcal{N}^{\otimes 9}$ for

$$\mathcal{N}(\rho) = (1-p)\,\rho + p\left(A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger \right)$$

Example how to use the QECC sufficient condition

If we use the 9-bit Shor code, noise process is $\mathcal{N}^{\otimes 9}$ for

$$\mathcal{N}(\rho) = (1-p)\,\rho + p\left(A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger\right)$$

$$\mathcal{N}^{\otimes 9}(\rho) = \mathcal{E}_1(\rho) + \mathcal{E}_2(\rho) \; \text{———} \; O(p^2)$$

joint state on 9 qubits

state on 1 qubit

Example how to use the QECC sufficient condition

If we use the 9-bit Shor code, noise process is $\mathcal{N}^{\otimes 9}$ for

$$\mathcal{N}(\rho) = (1-p)\rho + p\left(A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger\right)$$

$$\mathcal{N}^{\otimes 9}(\rho) = \mathcal{E}_1(\rho) + \mathcal{E}_2(\rho) \text{ —— } O(p^2)$$

$$(1-p)^9 \rho + (1-p)^8 p \left(A_0 \otimes I^{\otimes 8} \rho A_0^\dagger \otimes I^{\otimes 8} + A_1 \otimes I^{\otimes 8} \rho A_1^\dagger \otimes I^{\otimes 8} \right.$$
$$\left. + \text{ cyclic permutations} \right)$$

Example how to use the QECC sufficient condition

If we use the 9-bit Shor code, noise process is $\mathcal{N}^{\otimes 9}$ for

$$\mathcal{N}(\rho) = (1-p)\,\rho + p\left(A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger\right)$$

$$\mathcal{N}^{\otimes 9}(\rho) = \mathcal{E}_1(\rho) + \mathcal{E}_2(\rho) \text{ ——— } O(p^2)$$

$$(1-p)^9 \rho + (1-p)^8 p \left(A_0 \otimes I^{\otimes 8} \rho A_0^\dagger \otimes I^{\otimes 8} + A_1 \otimes I^{\otimes 8} \rho A_1^\dagger \otimes I^{\otimes 8} \right.$$
$$\left. + \text{ cyclic permutations} \right)$$

All 19 Kraus ops in $\mathcal{E}_1$ are in the span of $I, X_{1,\dots,9}, Z_{1,\dots,9}, Y_{1,\dots,9}$

From the theorem, $\exists R$ s.t. $R(\mathcal{E}_1(\rho)) = \rho \operatorname{tr} \mathcal{E}_1(\rho)$.

Example how to use the QECC sufficient condition

If we use the 9-bit Shor code, noise process is $\mathcal{N}^{\otimes 9}$ for

$$\mathcal{N}(\rho) = (1-p)\rho + p\left(A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger\right)$$

$$\mathcal{N}^{\otimes 9}(\rho) = \mathcal{E}_1(\rho) + \mathcal{E}_2(\rho) \text{ ------ } O(p^2)$$

$$\mathcal{E}_1(\rho) = (1-p)^9 \rho + (1-p)^8 p \left(A_0 \otimes I^{\otimes 8} \rho A_0^\dagger \otimes I^{\otimes 8} + A_1 \otimes I^{\otimes 8} \rho A_1^\dagger \otimes I^{\otimes 8} + \text{cyclic permutations} \right)$$

All 19 Kraus ops in $\mathcal{E}_1$ are in the span of $I, X_{1,\ldots,9}, Z_{1,\ldots,9}, Y_{1,\ldots,9}$

From the theorem, $\exists R$ s.t. $R(\mathcal{E}_1(\rho)) = \rho \operatorname{tr} \mathcal{E}_1(\rho)$.

So, $R(\mathcal{N}^{\otimes 9}(\rho)) = \rho \operatorname{tr} \mathcal{E}_1(\rho) + R \circ \mathcal{E}_2(\rho)$.

So, $\mathcal{R}(\mathcal{N}^{\otimes 9}(\rho)) = \rho \operatorname{tr} \mathcal{E}_1(\rho) + \mathcal{R} \circ \mathcal{E}_2(\rho)$.

$$\min_{|\psi_L\rangle} \operatorname{tr} \mathcal{R}(\mathcal{N}^{\otimes 9}(|\psi_L\rangle\langle\psi_L|))\, |\psi_L\rangle\langle\psi_L|$$

So, $\mathcal{R}(N^{\otimes 9}(\rho)) = \rho \operatorname{tr} \mathcal{E}_1(\rho) + \mathcal{R} \circ \mathcal{E}_2(\rho)$.

$$\min_{|\psi_L\rangle} \operatorname{tr} \mathcal{R}(N^{\otimes 9}(|\psi_L\rangle\langle\psi_L|))\, |\psi_L\rangle\langle\psi_L|$$

$$= \min_{|\psi_L\rangle} \operatorname{tr} \Big(|\psi_L\rangle\langle\psi_L| \operatorname{tr} \mathcal{E}_1(|\psi_L\rangle\langle\psi_L|) + \mathcal{R} \circ \mathcal{E}_2(|\psi_L\rangle\langle\psi_L|) \Big) |\psi_L\rangle\langle\psi_L|$$

So, $\mathcal{R}(\mathcal{N}^{\otimes 9}(\rho)) = \rho \operatorname{tr} \mathcal{E}_1(\rho) + \mathcal{R} \circ \mathcal{E}_2(\rho)$.

$$\min_{|\psi_L\rangle} \operatorname{tr} \mathcal{R}(\mathcal{N}^{\otimes 9}(|\psi_L\rangle\langle\psi_L|)) |\psi_L\rangle\langle\psi_L|$$

$$= \min_{|\psi_L\rangle} \operatorname{tr} \Big(|\psi_L\rangle\langle\psi_L| \operatorname{tr} \mathcal{E}_1(|\psi_L\rangle\langle\psi_L|) + \mathcal{R} \circ \mathcal{E}_2(|\psi_L\rangle\langle\psi_L|) \Big) |\psi_L\rangle\langle\psi_L|$$

$$= \min_{|\psi_L\rangle} \operatorname{tr} \mathcal{E}_1(|\psi_L\rangle\langle\psi_L|) + \operatorname{tr} \Big(\mathcal{R} \circ \mathcal{E}_2(|\psi_L\rangle\langle\psi_L|) \Big) |\psi_L\rangle\langle\psi_L|$$

So, $R(N^{\otimes 9}(\rho)) = \rho \operatorname{tr} \mathcal{E}_1(\rho) + R \circ \mathcal{E}_2(\rho)$.

$$\min_{|\psi_L\rangle} \operatorname{tr} R(N^{\otimes 9}(|\psi_L\rangle\langle\psi_L|))\, |\psi_L\rangle\langle\psi_L|$$

$$= \min_{|\psi_L\rangle} \operatorname{tr} \Big(|\psi_L\rangle\langle\psi_L| \operatorname{tr} \mathcal{E}_1(|\psi_L\rangle\langle\psi_L|) + R \circ \mathcal{E}_2(|\psi_L\rangle\langle\psi_L|) \Big) |\psi_L\rangle\langle\psi_L|$$

$$= \min_{|\psi_L\rangle} \underbrace{\operatorname{tr} \mathcal{E}_1(|\psi_L\rangle\langle\psi_L|)}_{(1-p)^9 + 9(1-p)^8 p} + \operatorname{tr} \Big(R \circ \mathcal{E}_2(|\psi_L\rangle\langle\psi_L|) \Big) |\psi_L\rangle\langle\psi_L|$$

$$\gtrsim 1 - O(p^2)$$

So the 9-bit code is effective in correcting up to one resetting error.

So, $R(N^{\otimes 9}(\rho)) = \rho \operatorname{tr} \mathcal{E}_1(\rho) + R \circ \mathcal{E}_2(\rho)$.

$$\min_{|\psi_L\rangle} \operatorname{tr} R(N^{\otimes 9}(|\psi_L\rangle\langle\psi_L|))\, |\psi_L\rangle\langle\psi_L|$$

$$= \min_{|\psi_L\rangle} \operatorname{tr} \Big(|\psi_L\rangle\langle\psi_L| \operatorname{tr} \mathcal{E}_1(|\psi_L\rangle\langle\psi_L|) + R \circ \mathcal{E}_2(|\psi_L\rangle\langle\psi_L|) \Big) |\psi_L\rangle\langle\psi_L|$$

$$= \min_{|\psi_L\rangle} \underbrace{\operatorname{tr} \mathcal{E}_1(|\psi_L\rangle\langle\psi_L|)}_{(1-p)^9 + 9(1-p)^8 p} + \underbrace{\operatorname{tr} \Big(R \circ \mathcal{E}_2(|\psi_L\rangle\langle\psi_L|) \Big) |\psi_L\rangle\langle\psi_L|}_{\geq 0}$$

$(\operatorname{tr} AB \geq 0 \text{ for } A, B \geq 0)$

$$\gtrsim 1 - O(p^2)$$

So the 9-bit code is effective in correcting up to one resetting error.

Summary:

A QECC corrects noise process $\mathcal{E}$
if $\mathcal{E}$ has Kraus operators in the span of some Ei's
each Ei unitary, and the Ei C's do not overlap.

<u>Summary</u>:

A QECC corrects noise process $\mathcal{E}$
if $\mathcal{E}$ has Kraus operators in the span of some Ei's
each Ei unitary, and the Ei C's do not overlap.

The proof is constructive:
Syndrome measurement has projectors $E_i P E_i^\dagger$'s
and if outcome is i, correction is $E_i^\dagger$.

Summary:

A QECC corrects noise process $\mathcal{E}$
if $\mathcal{E}$ has Kraus operators in the span of some Ei's
each Ei unitary, and the Ei C's do not overlap.

The proof is constructive:
Syndrome measurement has projectors $E_i P E_i^\dagger$'s
and if outcome is i, correction is $E_i^\dagger$.

Next:

Special QECCs with syndrome measurements based on "parities" generalized to the quantum setting.

9. Combating noise: quantum error correcting codes

(NC 10.1-10.3, 10.5, M 5, KLM 10)

(a) Classical noise model

(b) 3-bit repetition code

(c) Quantum noise model

(d) Quantum 3-bit repetition code for X errors

(e) Shor 9-bit code for arbitrary Pauli error

(g) Discretization and sufficient conditions for QECC

(h) Stabilizer formalism -- quantum parity checks !

(i) Shor 9-bit code reloaded

(j) Sufficient conditions for QECC for stabilizer codes

(l) 7-bit Steane code

(m) Erasure errors, q secret sharing, AdS/CFT corr

Quantum error correction sonnet -- Daniel Gottesman

We cannot clone, perforce; instead we split
coherence to protect it from that wrong
that would destroy our valued quantum bit
and make our computation take too long.

Correct a flip and phase -- that will suffice.
If in our code another error's bred,
we simply measure it, then God plays dice,
collapsing it to X or Y or zed.

We start with noisy seven, nine, or five
and end with perfect one. To better spot
those flaws we must avoid, we first must strive
to find which ones commute and which do not.

With group and eigenstate, we've learned to fix
your quantum errors with our quantum tricks.

The stabilizer formalism -- motivating example

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

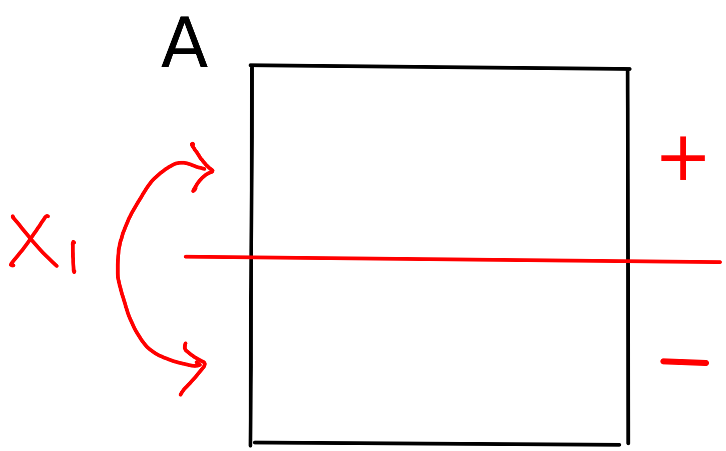
Unknown Pauli applied to the 1st qubit	Resulting state	Eigen value of ZZ	Eigen value of XX
I	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	+	+
Z	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	+	−
X	$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$	−	+
Y	$\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$	−	−

The pair of eigenvalues of ZZ, XX identify the unknown Pauli.

The stabilizer formalism -- motivating example

Consider: $|\Phi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \longrightarrow$ subspace C

$\mathbb{C}^{2\otimes 2} \longrightarrow$ ambient space A

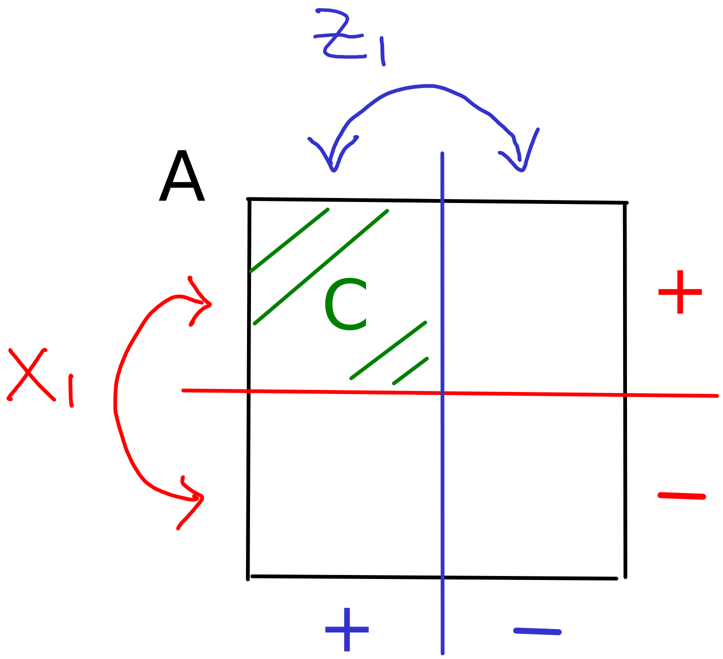


eigenspace of ZZ

The stabilizer formalism -- motivating example

Consider: $|\Phi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \longrightarrow$ subspace C

$\mathbb{C}^{2\otimes 2} \longrightarrow$ ambient space A



eigenspace of ZZ

eigenspace of XX

Y=iZX

Useful general picture ....

Reminder in linear algebra:

Let P, Q be two commuting projectors of equal dim.
The simultaneous +1 eigenspace of P and Q has projector PQ.

Reminder in linear algebra:

Let P, Q be two commuting projectors of equal dim.
The simultaneous +1 eigenspace of P and Q has projector PQ.

Proof: P, Q can be diagonalized in the same basis.

$$P = U \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix} U^\dagger, \qquad Q = U \begin{pmatrix} 0 & & \\ & I & \\ & & 0 \end{pmatrix} U^\dagger$$

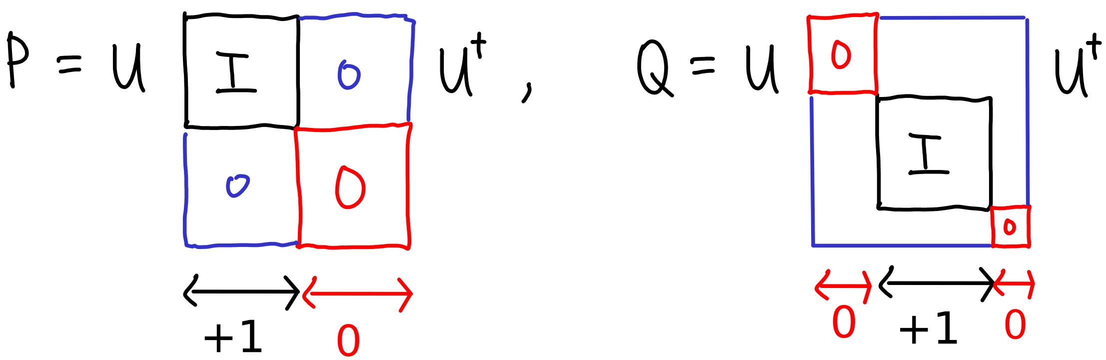
+1 0 | 0 +1 0

eigenspace of P | eigenspace of Q

Reminder in linear algebra:

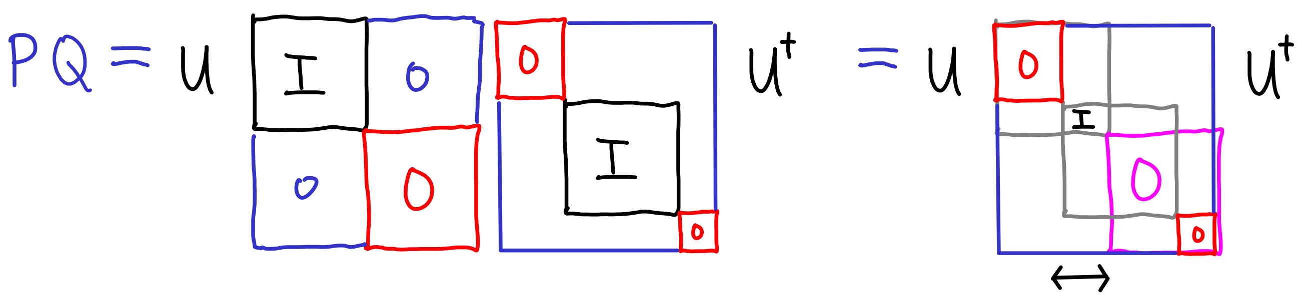
Let P, Q be two commuting projectors of equal dim.
The simultaneous +1 eigenspace of P and Q has projector PQ.

Proof: P, Q can be diagonalized in the same basis.



eigenspace of P

eigenspace of Q

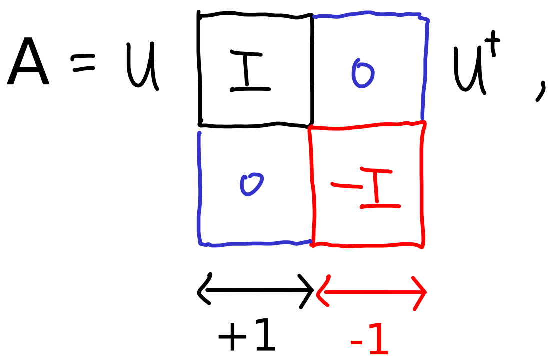


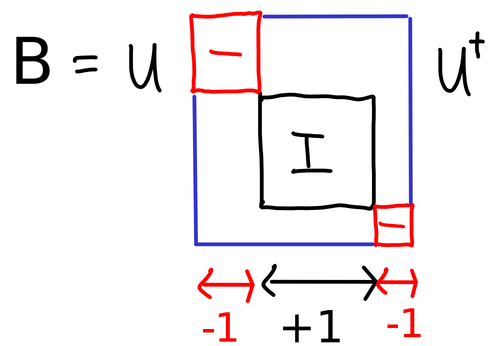
simultaneous +1
eigenspace of P & Q

<u>Reminder in linear algebra</u>:

Let A, B be two commuting operators of equal dim with eigenvalues +/-1. The simultaneous ++, +-, -+, --1 eigenspaces of A and B is a partition of the space.

Proof: A, B can be diagonalized in the same basis.



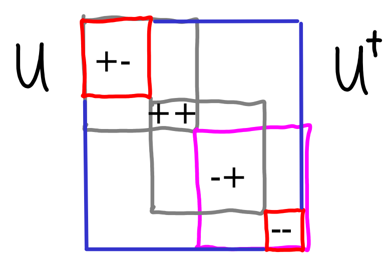


eigenspace of A

eigenspace of B

The ambience space is divided into simultaneous ++, +-, -+, -- eigenspaces of A & B.

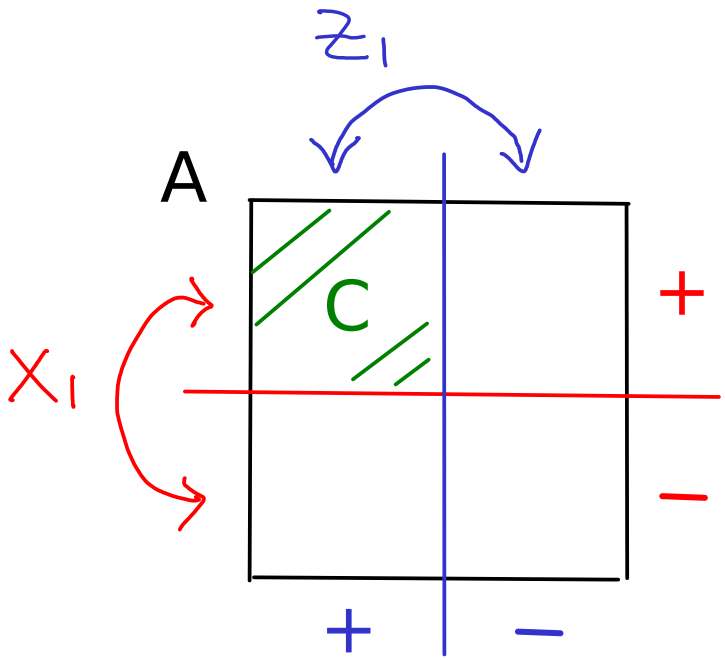
If in addition Tr(A) = Tr(B) = Tr(AB) = 0, each eigenspace has 1/4 of the total dimension.



The stabilizer formalism -- motivating example

Consider: $|\Phi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$ $\longrightarrow$ subspace C

$\mathbb{C}^{2\otimes 2}$ $\longrightarrow$ ambient space A



eigenspace of ZZ

eigenspace of XX

Y=iZX

Dim(A) = 4, dim(C) = dim(A)/2/2 = 1

XX ZZ

A quick note on "measuring ZZ, XX".

Projectors describing the measurement of ZZ:

(II+ZZ)/2,   (II-ZZ)/2

Projectors describing the measurement of XX:

(II+XX)/2,   (II-XX)/2

A quick note on "measuring ZZ, XX".

Projectors describing the measurement of ZZ:

(II+ZZ)/2,   (II-ZZ)/2

Projectors describing the measurement of XX:

(II+XX)/2,   (II-XX)/2

Projectors describing the simultaneous measurements of XX & ZZ:

(II+XX)/2 * (II+ZZ)/2,   (II-XX)/2 * (II+ZZ)/2
(II-XX)/2 * (II+ZZ)/2,   (II-XX)/2 * (II-ZZ)/2

Within each projector, ordering in the * doesn't matter since XX and ZZ commute.

A quick note on "measuring ZZ, XX".

Projectors describing the measurement of ZZ:

(II+ZZ)/2,   (II-ZZ)/2

Projectors describing the measurement of XX:

(II+XX)/2,   (II-XX)/2

Projectors describing the simultaneous measurements of XX & ZZ:

Exercise: check explicitly these are the projectors onto the 4 Bell states!

(II+XX)/2 * (II+ZZ)/2,   (II-XX)/2 * (II+ZZ)/2
(II-XX)/2 * (II+ZZ)/2,   (II-XX)/2 * (II-ZZ)/2

Within each projector, ordering in the * doesn't matter since XX and ZZ commute.

The example of the 4 Bell states and that measuring XX, ZZ reveals what happens to the Bell state generalizes to a general QECC ...

Example: 3-bit code for X errors:

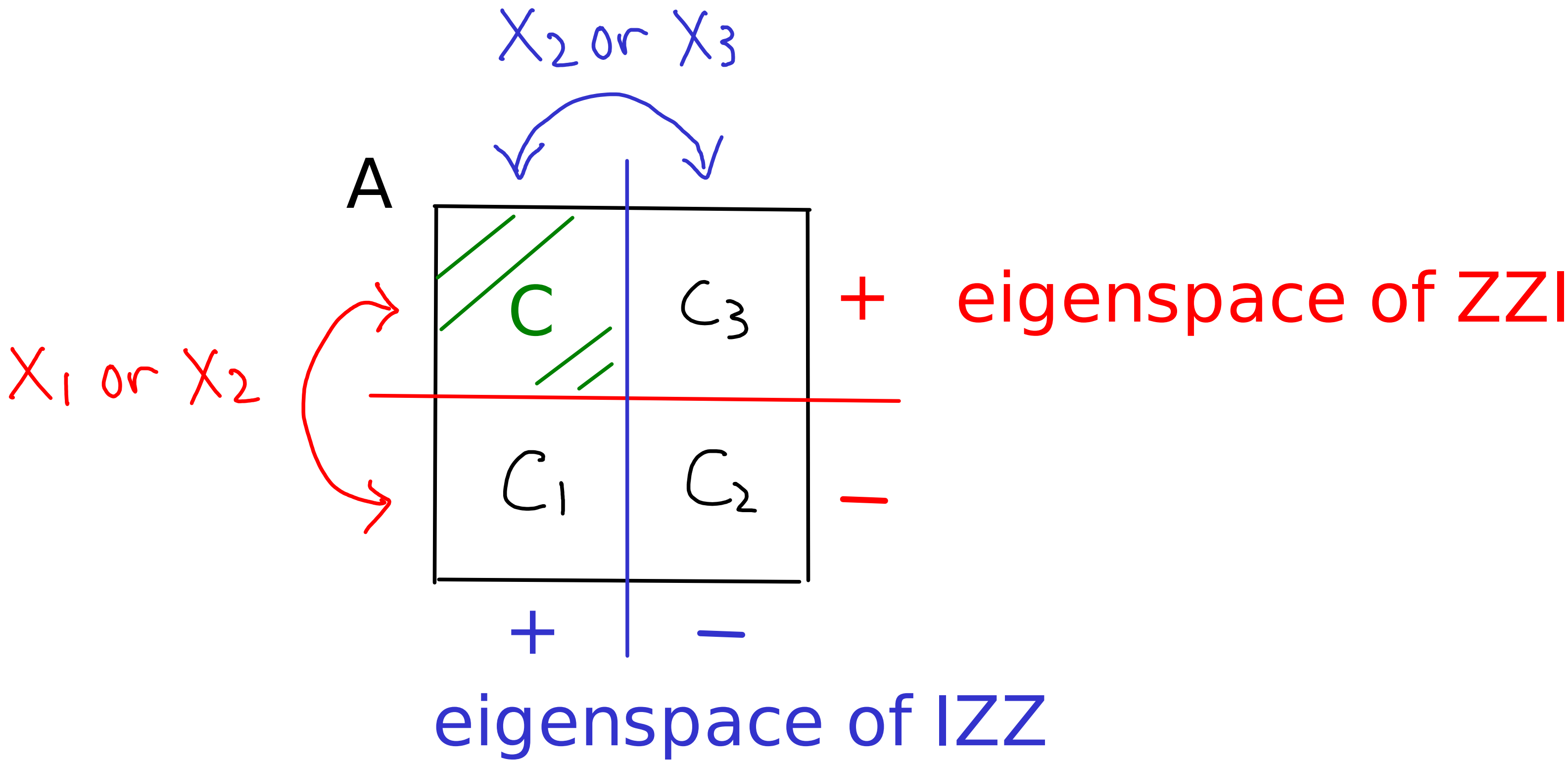
ambient space A: $\mathbb{C}^{2\otimes 3}$

subspace C: $a|000\rangle + b|111\rangle$

Example: 3-bit code for X errors:

ambient space A: $\mathbb{C}^{2^{\otimes 3}}$

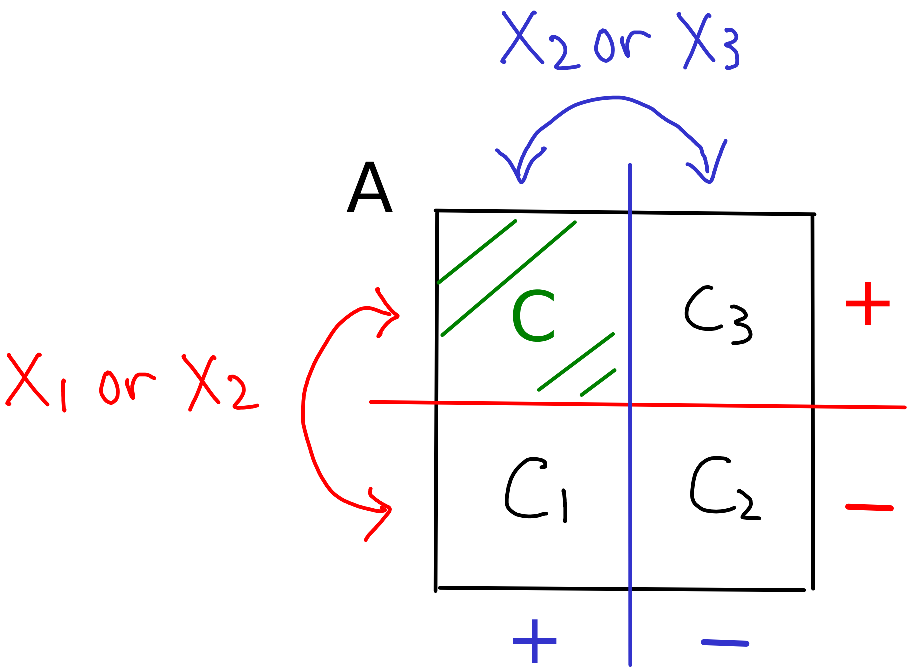
subspace C: $a|000\rangle + b|111\rangle$



Example: 3-bit code for X errors:

ambient space A: $\mathbb{C}^{2^{\otimes 3}}$

subspace C: $a|000\rangle + b|111\rangle$



eigenspace of ZZI

eigenspace of IZZ

Dim(A) = 8, dim(C) = dim(A)/2/2 = 2

ZZ1 IZZ

Example: 3-bit code for X errors:

Syndrome measurement for 3-bit code for X errors:

* eigenvalues of ZZI, with projectors

$$\Pi_{12+} = (III + ZZI)/2 = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I,$$
$$\Pi_{12-} = (III - ZZI)/2 = (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I.$$

* eigenvalues of IZZ, with projectors

$$\Pi_{23+} = (III + IZZ)/2 = I \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|),$$
$$\Pi_{23-} = (III - IZZ)/2 = I \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|).$$

Example: 3-bit code for X errors:

Syndrome measurement for 3-bit code for X errors:

* eigenvalues of ZZI, with projectors

$$\Pi_{12+} = (III + ZZI)/2 = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I,$$
$$\Pi_{12-} = (III - ZZI)/2 = (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I.$$

* eigenvalues of IZZ, with projectors

$$\Pi_{23+} = (III + IZZ)/2 = I \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|),$$
$$\Pi_{23-} = (III - IZZ)/2 = I \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|).$$

Measuring both ZZI and IZZ, there are 4 outcomes.

e.g., If the outcome of measuring ZZI is "+", state is spanned by $\{|00\rangle|0\rangle, |00\rangle|1\rangle, |11\rangle|0\rangle, |11\rangle|1\rangle\}$. If an additional measurement of IZZ yields -1, the span is reduced to $\{|00\rangle|1\rangle, |11\rangle|0\rangle\}$, i.e., C3.

Ex: check for other cases.

Measuring both ZZI and IZZ, there are 4 outcomes, corresponding to a measurement with projectors:

$\Pi_{12+}\Pi_{23+}$, $\Pi_{12+}\Pi_{23-}$, $\Pi_{12-}\Pi_{23+}$, $\Pi_{12-}\Pi_{23-}$

Measuring both ZZI and IZZ, there are 4 outcomes, corresponding to a measurement with projectors:

$\Pi_{12+}\Pi_{23+}$, $\Pi_{12+}\Pi_{23-}$, $\Pi_{12-}\Pi_{23+}$, $\Pi_{12-}\Pi_{23-}$

From direct calculation:

$$\Pi_{12+}\Pi_{23+} = |000\rangle\langle 000| + |111\rangle\langle 111|$$

$$\Pi_{12-}\Pi_{23+} = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$\Pi_{12-}\Pi_{23-} = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$\Pi_{12+}\Pi_{23-} = |001\rangle\langle 001| + |110\rangle\langle 110|$$

Measuring both ZZI and IZZ, there are 4 outcomes, corresponding to a measurement with projectors:

$\Pi_{12+}\Pi_{23+}$, $\Pi_{12+}\Pi_{23-}$, $\Pi_{12-}\Pi_{23+}$, $\Pi_{12-}\Pi_{23-}$

From direct calculation:

$\Pi_{12+}\Pi_{23+} = |000\rangle\langle 000| + |111\rangle\langle 111|$ projector onto C0

$\Pi_{12-}\Pi_{23+} = |100\rangle\langle 100| + |011\rangle\langle 011|$ C1

$\Pi_{12-}\Pi_{23-} = |010\rangle\langle 010| + |101\rangle\langle 101|$ C2

$\Pi_{12+}\Pi_{23-} = |001\rangle\langle 001| + |110\rangle\langle 110|$ C3

code word	after X1	after X2	after X3
$a\|000\rangle + b\|111\rangle$	$a\|100\rangle + b\|011\rangle$	$a\|010\rangle + b\|101\rangle$	$a\|001\rangle + b\|110\rangle$
C0	C1	C2	C3

Previous approach:

(1) specify $|0\rangle \to |0_L\rangle$

$|1\rangle \to |1_L\rangle$

(2) list $E_i\,(a|0_L\rangle + b|1_L\rangle)$

(3) derive syndrome measurement by inspecting (2)

Previous approach:

(1) specify $|0\rangle \to |0_L\rangle$

$|1\rangle \to |1_L\rangle$

(2) list $E_i(a|0_L\rangle + b|1_L\rangle)$

(3) derive syndrome measurement by inspecting (2)

Stabilizer code: NC 10.5

(1) Specify a list of Pauli's; codespace is simultaneous +1 eigenspace, syndrome is the list of eigenvalues

Previous approach:

(1) specify $|0\rangle \to |0_L\rangle$

$|1\rangle \to |1_L\rangle$

(2) list $E_i(a|0_L\rangle + b|1_L\rangle)$

(3) derive syndrome measurement by inspecting (2)

Stabilizer code: NC 10.5

(1) Specify a list of Pauli's; codespace is simultaneous +1 eigenspace, syndrome is the list of eigenvalues

(2) check QECC condition (or just tabulate syndromes)

Previous approach:

(1) specify $|0\rangle \to |0_L\rangle$
$|1\rangle \to |1_L\rangle$

(2) list $E_i(a|0_L\rangle + b|1_L\rangle)$

(3) derive syndrome measurement by inspecting (2)

Stabilizer code: NC 10.5

(1) Specify a list of Pauli's; codespace is simultaneous +1 eigenspace, syndrome is the list of eigenvalues

(2) check QECC condition (or just tabulate syndromes)

(3) specify X_L and Z_L (for encoding/decoding and fault tolerance)

Previous approach:

(1) specify $|0\rangle \rightarrow |0_L\rangle$

$|1\rangle \rightarrow |1_L\rangle$

(2) list $E_i(a|0_L\rangle + b|1_L\rangle)$

(3) derive syndrome measurement by inspecting (2)

Stabilizer code: NC 10.5

(1) Specify a list of Pauli's; codespace is simultaneous +1 eigenspace, syndrome is the list of eigenvalues

(2) check QECC condition (or just tabulate syndromes)

(3) specify X_L and Z_L (for encoding/decoding and fault tolerance)

(4) specify encoded gates

Previous approach:

(1) specify $|0\rangle \to |0_L\rangle$

$|1\rangle \to |1_L\rangle$

(2) list $E_i(a|0_L\rangle + b|1_L\rangle)$

(3) derive syndrome measurement by inspecting (2)

Typically, writing down the code state takes exponential time in the blocklength.

Stabilizer code: NC 10.5

(1) Specify a list of Pauli's; codespace is simultaneous +1 eigenspace, syndrome is the list of eigenvalues

(2) check QECC condition (or just tabulate syndromes)

(3) specify X_L and Z_L (for encoding/decoding and fault tolerance)

(4) specify encoded gates

Polynomial-time analysis.

Definition: a stabilizer code C of blocklength n is a simultaneous +1 eigenspace of a list of commuting, independent, Pauli matrices on n qubits.

A list of Pauli matrices P1, P2, ... Pr is independent if none if them is a product of a subset of the others.

e.g., ZZI, IZZ are independent.
e.g., ZZI, IZZ, ZIZ are not independent.

Definition: Pauli group on n qubits P_n

Consider $\mathbb{C}^{2\otimes n}$. Let X_t, Z_t be the X, Z Pauli operator acting on the t-th qubit (I on the rest).

The Pauli group is defined to be the group generated multiplicatively by X_t, Z_t, for t=1,2,...,n, and scalar i.

Definition: Pauli group on n qubits P_n

Consider $\mathbb{C}^{2^{\otimes n}}$. Let X_t, Z_t be the X, Z Pauli operator acting on the t-th qubit (I on the rest).

The Pauli group is defined to be the group generated multiplicatively by $X_t, Z_t,$ for t=1,2,...,n, and scalar i.

Let Y = iXZ = $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$.

Let YZX = iXZ(ZX) = i * I.

So, Y can act on any qubit;
and an element of the Pauli group may have any power of i multiplied to it.

Definition: Pauli group on n qubits P_n

Consider $\mathbb{C}^{2^{\otimes n}}$. Let X_t, Z_t be the X, Z Pauli operator acting on the t-th qubit (I on the rest).

The Pauli group is defined to be the group generated multiplicatively by X_t, Z_t, for t=1,2,...,n, and scalar i.

Let Y = iXZ = $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$. Let YZX = iXZ(ZX) = i * I.

e.g., n=2. Generators: XI, IX, ZI, IZ

Group elements generated multiplicatively:

$$\left\{ \begin{matrix} II, & XI, IX, XX, & ZI, IZ, ZZ, & \\ YI, XZ, YZ, & ZX, IY, ZY, & & YX, XY, YY \end{matrix} \right\} \times \{1, -1, i, -i\}$$

NB. Focus on the quotient group without the scalar.

Definition: a stabilizer code C of blocklength n is a simultaneous +1 eigenspace of a list of commuting, independent, Pauli matrices on n qubits.

Remarks:

1. The list generates a group (subgroup of the Pauli group) under matrix multiplication, called the "stabilizer group" S of the code C. .

Definition: a stabilizer code C of blocklength n is a simultaneous +1 eigenspace of a list of commuting, independent, Pauli matrices on n qubits.

Remarks:

1. The list generates a group (subgroup of the Pauli group) under matrix multiplication, called the "stabilizer group" S of the code C. .

2. The code is a +1 eigenspace of any element in this group. (So, each element M is a "stabilizer of C" : M fixes every vector in C.)

Proof: let $M_1, M_2, \cdots M_r$ be matrices from the list,

$M = M_1 M_2 \cdots M_r$ be their product.

$$\forall |\psi\rangle \in C, \; M|\psi\rangle = M_r \cdots M_2 M_1 |\psi\rangle$$

$$= M_r \cdots M_2 |\psi\rangle = M_r \cdots |\psi\rangle = |\psi\rangle .$$

Definition: a stabilizer code C of blocklength n is a simultaneous +1 eigenspace of a list of commuting, independent, Pauli matrices on n qubits.

Remarks:

3. The initial list of commuting matrices is called the set of "generators" for the stabilizer group.

e.g., ZZI, IZZ generates a group of 4 elements:

$$ZZI^0\, IZZ^0 = III, \qquad ZZI^1\, IZZ^0 = ZZI,$$
$$ZZI^0\, IZZ^1 = IZZ, \qquad ZZI^1\, IZZ^1 = ZIZ.$$

Definition: a stabilizer code C of blocklength n is a simultaneous +1 eigenspace of a list of commuting, independent, Pauli matrices on n qubits.

Remarks:

3. The initial list of commuting matrices is called the set of "generators" for the stabilizer group.

e.g., ZZI, IZZ generates a group of 4 elements:

$ZZI^0\, IZZ^0 = III$, $\quad ZZI^1\, IZZ^0 = ZZI$,
$ZZI^0\, IZZ^1 = IZZ$, $\quad ZZI^1\, IZZ^1 = ZIZ$.

4. By (a) commutivity, (b) each Pauli squares to I, each stabilizer can be specified by whether each generator is a factor or not, so, the stabilizer group has 2^m elements for a list of m generators. e.g., m = 2 above.

9. Combating noise: quantum error correcting codes

(NC 10.1-10.3, 10.5, M 5, KLM 10)

(a) Classical noise model

(b) 3-bit repetition code

(c) Quantum noise model

(d) Quantum 3-bit repetition code for X errors

(e) Shor 9-bit code for arbitrary Pauli error

(g) Discretization and sufficient conditions for QECC

(h) Stabilizer formalism -- quantum parity checks !

(i) Shor 9-bit code reloaded

(j) Sufficient conditions for QECC for stabilizer codes

(l) 7-bit Steane code

(m) Erasure errors, q secret sharing, AdS/CFT corr

9-bit code: $|0_L\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |111\rangle\right)^{\otimes 3}, \quad |1_L\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle - |111\rangle\right)^{\otimes 3}$

It is a stabilizer code of blocklength 9, with 8 generators (commuting Pauli matrices) for its stabilizer.

	I	X_1	X_2	X_3	⋯	Y_9 ← Error
ZZI III III	+	-	-	+		+
IZZ III III	+	+	-	-		+
III ZZI III	+	+	+	+		+
III IZZ III	+	+	+	+		+
III III ZZI	+	+	+	+		+
III III IZZ	+	+	+	+		-
XXX XXX III	+	+	+	+		+
III XXX XXX	+	+	+	+		-

sufficient syndrome info for recovery

9-bit code: $|0_L\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |111\rangle\right)^{\otimes 3}$, $|1_L\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle - |111\rangle\right)^{\otimes 3}$

Claim: XXXXXXXXX = Z_L
ZZZZZZZZZ = X_L

9-bit code: $|0_L\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |111\rangle\right)^{\otimes 3}, \quad |1_L\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle - |111\rangle\right)^{\otimes 3}$

Claim: $XXXXXXXXX = Z_L$

$ZZZZZZZZZ = X_L$

Checking:

$$\begin{tikzcd}
(|000\rangle+|111\rangle) \arrow[loop right, "XXX"] \arrow[d, shift right, "ZZZ"'] & \\
(|000\rangle-|111\rangle) \arrow[u, shift right] \arrow[r, shift left, "XXX"] & -(|000\rangle-|111\rangle) \arrow[l, shift left]
\end{tikzcd}$$

9-bit code: $|0_L\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |111\rangle\right)^{\otimes 3}$, $|1_L\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle - |111\rangle\right)^{\otimes 3}$

Claim: $XXXXXXXXX = Z_L$
$ZZZZZZZZZ = X_L$

Checking:

$$(|000\rangle + |111\rangle) \circlearrowleft XXX$$

$$ZZZ \; \downarrow\uparrow$$

$$(|000\rangle - |111\rangle) \overset{XXX}{\rightleftarrows} -(|000\rangle - |111\rangle)$$

thus:

$$|0_L\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |111\rangle\right)^{\otimes 3} \circlearrowleft (XXX)^{\otimes 3}$$

$$(ZZZ)^{\otimes 3} \; \downarrow\uparrow$$

$$|1_L\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle - |111\rangle\right)^{\otimes 3} \overset{(XXX)^{\otimes 3}}{\rightleftarrows} -\left(|000\rangle - |111\rangle\right)^{\otimes 3} = -|1_L\rangle$$

More remarks:

5. Different sets may generate the same group. e.g., {ZZI, IZZ} and {ZZI, ZIZ} generate the same group, and lead to the 1st and 2nd circuits for the 3-qubit X error correcting code.

More remarks:

5. Different sets may generate the same group.
e.g., {ZZI, IZZ} and {ZZI, ZIZ} generate the same group, and lead to the 1st and 2nd circuits for the 3-qubit X error correcting code.

6. Chicken and egg situation, both works.
Write down the code C, then find the stabilizer group (parity checks).
Write down the stabilizer generators, then find the code stabilized by them.

More remarks:

5. Different sets may generate the same group.
e.g., {ZZI, IZZ} and {ZZI, ZIZ} generate the same group, and lead to the 1st and 2nd circuits for the 3-qubit X error correcting code.

6. Chicken and egg situation, both works.
Write down the code C, then find the stabilizer group (parity checks).
Write down the stabilizer generators, then find the code stabilized by them.

7. Any two Pauli matrices commute or anticommute.

8. We design QECCs to correct Pauli errors (the Ei's).
We drop the "dagger" from the hermitian matrices.

More remarks:

e.g., XX, ZZ generates the group II, XX, ZZ, YY.
The code has 1 dimension, spanned by $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$.

e.g., 9-bit code has 8 generators, code has $\frac{2^9}{2^8} = 2$ dims.

More remarks:

e.g., XX, ZZ generates the group II, XX, ZZ, YY.
The code has 1 dimension, spanned by $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

e.g., 9-bit code has 8 generators, code has $\frac{2^9}{2^8} = 2$ dims.

Theorem: a stabilizer code with block length n and (n-k) stabilizer generators has $\frac{2^n}{2^{n-k}} = 2^k$ dims.

(Pf: exercise, based on "Reminder in linear algebra, p65-68.)

Summary for stabilizer code formalism:

Definition: a stabilizer code C of blocklength n is a simultaneous +1 eigenspace of a list of commuting, independent, Pauli matrices on n qubits.

If the list has n-k Pauli matrices, they generate (multi-plicatively) a stabilizer group S with 2^{n-k} elements.

Every element M in S is a "stabilizer of C" :
M fixes every vector in C. C has 2^{k} dim.

The n-k matrices are called "generators" for the stabilizer.