Quantum error correction, Operator Algebra, Representation Theory

Chi-Kwong Li
Department of Mathematics, The College of William and Mary;
Institute for Quantum Computing, University of Waterloo

Joint work with Cordelia Li, Diane Pelejo, Sage Stanish.

Introduction

- M_n (H_n): the set of $n \times n$ complex (Hermitian) matrices.

Introduction

- M_n (H_n): the set of $n \times n$ complex (Hermitian) matrices.
- Quantum states are represented as density matrices,
  i.e., positive semidefinite matrices in H_n in with trace one.

Introduction

- M_n (H_n): the set of $n \times n$ complex (Hermitian) matrices.
- Quantum states are represented as density matrices,
  i.e., positive semidefinite matrices in H_n in with trace one.
- Denote by D_n the set of density matrices in M_n.

Introduction

- M_n (H_n): the set of $n \times n$ complex (Hermitian) matrices.
- Quantum states are represented as density matrices,
  i.e., positive semidefinite matrices in H_n in with trace one.
- Denote by D_n the set of density matrices in M_n.
- A quantum channel (operation) $\mathcal{E} : M_n \to M_n$ is a trace preserving completely positive map admitting an operator sum representation

$$\rho \to \boxed{\begin{array}{c}\text{Quantum}\\ \text{Channel } \mathcal{E}\end{array}} \to \mathcal{E}(\rho), \qquad \mathcal{E}(\rho) = E_1 \rho E_1^\dagger + \cdots + E_r \rho E_r^\dagger,$$

for some $E_1, \ldots, E_r \in M_n$ such that $E_1^\dagger E_1 + \cdots + E_r^\dagger E_r = I_n$.

Introduction

- M_n (H_n): the set of $n \times n$ complex (Hermitian) matrices.
- Quantum states are represented as density matrices,
  i.e., positive semidefinite matrices in H_n in with trace one.
- Denote by D_n the set of density matrices in M_n.
- A quantum channel (operation) $\mathcal{E} : M_n \to M_n$ is a trace preserving completely positive map admitting an operator sum representation

$$\rho \to \boxed{\text{Quantum Channel } \mathcal{E}} \to \mathcal{E}(\rho), \qquad \mathcal{E}(\rho) = E_1 \rho E_1^\dagger + \cdots + E_r \rho E_r^\dagger,$$

for some $E_1, \ldots, E_r \in M_n$ such that $E_1^\dagger E_1 + \cdots + E_r^\dagger E_r = I_n$.

- In the context of quantum error correction, $E_1, \ldots, E_r$ are the error operators associated with the channel.

Basic Problem

How to recover useful/important information (data bits) after it passes through a noisy quantum channel $\mathcal{E}$ with "known" (by Tomography) error operators.

Basic Problem

How to recover useful/important information (data bits) after it passes through a noisy quantum channel $\mathcal{E}$ with "known" (by Tomography) error operators.

Correction scheme Encode the data bits $\tilde{\rho} \in D_k$ as $\rho \in D_n$ for a larger n, and send it through the channel $\mathcal{E}$ to get $\mathcal{E}(\rho)$. Then do one of the following.

Basic Problem

How to recover useful/important information (data bits) after it passes through a noisy quantum channel $\mathcal{E}$ with "known" (by Tomography) error operators.

Correction scheme Encode the data bits $\tilde{\rho} \in D_k$ as $\rho \in D_n$ for a larger n, and send it through the channel $\mathcal{E}$ to get $\mathcal{E}(\rho)$. Then do one of the following.

- Apply a syndrome measurement to $\mathcal{E}(\rho)$ using additional qubits;

Basic Problem

How to recover useful/important information (data bits) after it passes through a noisy quantum channel $\mathcal{E}$ with "known" (by Tomography) error operators.

Correction scheme Encode the data bits $\tilde{\rho} \in D_k$ as $\rho \in D_n$ for a larger n, and send it through the channel $\mathcal{E}$ to get $\mathcal{E}(\rho)$. Then do one of the following.

- Apply a syndrome measurement to $\mathcal{E}(\rho)$ using additional qubits; then construct a recovery channel $\mathcal{R}$ so that $\mathcal{R} \circ \mathcal{E}(\rho) = \rho$.

Basic Problem

How to recover useful/important information (data bits) after it passes through a noisy quantum channel $\mathcal{E}$ with "known" (by Tomography) error operators.

Correction scheme Encode the data bits $\tilde{\rho} \in D_k$ as $\rho \in D_n$ for a larger n, and send it through the channel $\mathcal{E}$ to get $\mathcal{E}(\rho)$. Then do one of the following.

- Apply a syndrome measurement to $\mathcal{E}(\rho)$ using additional qubits; then construct a recovery channel $\mathcal{R}$ so that $\mathcal{R} \circ \mathcal{E}(\rho) = \rho$.

$$\boxed{\tilde{\rho} \to \rho \to \mathcal{E}(\rho) \to \mathcal{E}(\rho) \otimes \sigma \to (\mathcal{E}(\rho), \tilde{\sigma}) \to \mathcal{R} \circ \mathcal{E}(\rho) = \rho \to \tilde{\rho}.}$$

$$\tilde{P} \to P_1P_2P_2 \to Q_1Q_2Q_3 \to (Q_1Q_2Q_3) \otimes (R_1R_2) \to ((Q_1Q_2Q_3), (M_1M_2)) \to (P_1P_2P_3) \to \tilde{P}.$$

Quantum Error Correction

Basic Problem

How to recover useful/important information (data bits) after it passes through a noisy quantum channel $\mathcal{E}$ with "known" (by Tomography) error operators.

Correction scheme Encode the data bits $\tilde{\rho} \in D_k$ as $\rho \in D_n$ for a larger n, and send it through the channel $\mathcal{E}$ to get $\mathcal{E}(\rho)$. Then do one of the following.

- Apply a syndrome measurement to $\mathcal{E}(\rho)$ using additional qubits; then construct a recovery channel $\mathcal{R}$ so that $\mathcal{R} \circ \mathcal{E}(\rho) = \rho$.

$$\boxed{\tilde{\rho} \to \rho \to \mathcal{E}(\rho) \to \mathcal{E}(\rho) \otimes \sigma \to (\mathcal{E}(\rho), \tilde{\sigma}) \to \mathcal{R} \circ \mathcal{E}(\rho) = \rho \to \tilde{\rho}.}$$

$$\tilde{P} \to P_1 P_2 P_2 \to Q_1 Q_2 Q_3 \to (Q_1 Q_2 Q_3) \otimes (R_1 R_2) \to ((Q_1 Q_2 Q_3), (M_1 M_2)) \to (P_1 P_2 P_3) \to \tilde{P}.$$

- Use operator algebra techniques to determine an error avoiding subspace to construct a recovery channel $\mathcal{R}$.

$$\boxed{\tilde{\rho} \to \rho \to \mathcal{E}(\rho) \to \mathcal{R} \circ \mathcal{E}(\rho) = \hat{\rho} \to \tilde{\rho}.}$$

$$\tilde{P} \to P_1 P_2 P_2 \to Q_1 Q_2 Q_3 \to \tilde{P} \otimes (R_1 R_2)) \to \tilde{P}.$$

Quantum Error Correction

Basic Problem

How to recover useful/important information (data bits) after it passes through a noisy quantum channel $\mathcal{E}$ with "known" (by Tomography) error operators.

Correction scheme Encode the data bits $\tilde{\rho} \in D_k$ as $\rho \in D_n$ for a larger n, and send it through the channel $\mathcal{E}$ to get $\mathcal{E}(\rho)$. Then do one of the following.

- Apply a syndrome measurement to $\mathcal{E}(\rho)$ using additional qubits; then construct a recovery channel $\mathcal{R}$ so that $\mathcal{R} \circ \mathcal{E}(\rho) = \rho$.

$$\boxed{\tilde{\rho} \to \rho \to \mathcal{E}(\rho) \to \mathcal{E}(\rho) \otimes \sigma \to (\mathcal{E}(\rho), \tilde{\sigma}) \to \mathcal{R} \circ \mathcal{E}(\rho) = \rho \to \tilde{\rho}.}$$

$$\tilde{P} \to P_1 P_2 P_2 \to Q_1 Q_2 Q_3 \to (Q_1 Q_2 Q_3) \otimes (R_1 R_2) \to ((Q_1 Q_2 Q_3), (M_1 M_2)) \to (P_1 P_2 P_3) \to \tilde{P}.$$

- Use operator algebra techniques to determine an error avoiding subspace to construct a recovery channel $\mathcal{R}$.

$$\boxed{\tilde{\rho} \to \rho \to \mathcal{E}(\rho) \to \mathcal{R} \circ \mathcal{E}(\rho) = \hat{\rho} \to \tilde{\rho}.}$$

$$\tilde{P} \to P_1 P_2 P_2 \to Q_1 Q_2 Q_3 \to \tilde{P} \otimes (R_1 R_2)) \to \tilde{P}.$$

Ideally, $\quad \tilde{P} \to P_1 P_2 P_2 \to Q_1 Q_2 Q_3 \to P_1 P_2 P_3 \to \tilde{P}.$

Example: Bit-flip channel

Consider the bit-flip error $\tilde{\rho} \mapsto X\tilde{\rho}X^\dagger$ with $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ that will exchange the two classical states $|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $|1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

Example: Bit-flip channel

Consider the bit-flip error $\tilde{\rho} \mapsto X\tilde{\rho}X^\dagger$ with $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ that will exchange the two classical states $|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $|1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

We can encode one qubit $\tilde{\rho} \in M_2$ into a 3-qubit system $\rho \in M_{2^3}$, i.e., we will use two qubits to protect one qubits.

Example: Bit-flip channel

Consider the bit-flip error $\tilde{\rho} \mapsto X\tilde{\rho}X^\dagger$ with $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ that will exchange the two classical states $|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $|1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

We can encode one qubit $\tilde{\rho} \in M_2$ into a 3-qubit system $\rho \in M_{2^3}$, i.e., we will use two qubits to protect one qubits. The channel on three qubits has the form:

$$\rho \mapsto p_0\rho + p_1 E_1 \rho E_1^\dagger + p_2 E_2 \rho E_2^\dagger + p_3 E_3 \rho E_3^\dagger,$$

where $p_0, p_1, p_2, p_3 \geq 0$ summing up to 1,

$$E_1 = X \otimes I_2 \otimes I_2, E_2 = I_2 \otimes X \otimes I_2, E_3 = I_2 \otimes I_2 \otimes X.$$

Example: Bit-flip channel

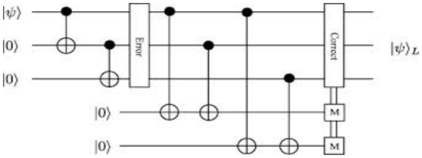
Consider the bit-flip error $\tilde{\rho} \mapsto X\tilde{\rho}X^\dagger$ with $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ that will exchange the two classical states $|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $|1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

We can encode one qubit $\tilde{\rho} \in M_2$ into a 3-qubit system $\rho \in M_{2^3}$, i.e., we will use two qubits to protect one qubits. The channel on three qubits has the form:

$$\rho \mapsto p_0\rho + p_1 E_1 \rho E_1^\dagger + p_2 E_2 \rho E_2^\dagger + p_3 E_3 \rho E_3^\dagger,$$

where $p_0, p_1, p_2, p_3 \geq 0$ summing up to 1,

$$E_1 = X \otimes I_2 \otimes I_2, E_2 = I_2 \otimes X \otimes I_2, E_3 = I_2 \otimes I_2 \otimes X.$$



QECC with syndrome measurement.

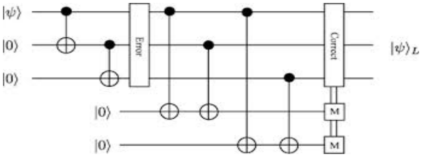
Consider the bit-flip error $\tilde{\rho} \mapsto X\tilde{\rho}X^\dagger$ with $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ that will exchange the two classical states $|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $|1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

We can encode one qubit $\tilde{\rho} \in M_2$ into a 3-qubit system $\rho \in M_{2^3}$, i.e., we will use two qubits to protect one qubits. The channel on three qubits has the form:

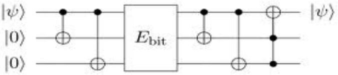
$$\rho \mapsto p_0\rho + p_1 E_1 \rho E_1^\dagger + p_2 E_2 \rho E_2^\dagger + p_3 E_3 \rho E_3^\dagger,$$

where $p_0, p_1, p_2, p_3 \geq 0$ summing up to 1,

$$E_1 = X \otimes I_2 \otimes I_2, E_2 = I_2 \otimes X \otimes I_2, E_3 = I_2 \otimes I_2 \otimes X.$$



QECC with syndrome measurement.



QECC without syndrome measurement.

Operator algebra

Question

How to find a recovery channel without syndrome measurement?

Operator algebra

Question

How to find a recovery channel without syndrome measurement?
Equivalently, how to find the error avoiding subspace?

Operator algebra

Question

How to find a recovery channel without syndrome measurement?
Equivalently, how to find the error avoiding subspace?

- Let $\mathcal{A}$ be the algebra generated by $\{E_1, \ldots, E_r, E_1^\dagger, \ldots, E_r^\dagger\}$.

Operator algebra

Question

How to find a recovery channel without syndrome measurement?
Equivalently, how to find the error avoiding subspace?

- Let $\mathcal{A}$ be the algebra generated by $\{E_1, \ldots, E_r, E_1^\dagger, \ldots, E_r^\dagger\}$.
- By the Wedderburn Theorem, there is a unitary U such that

$$U^\dagger \mathcal{A} U = I_{f_1} \otimes M_{g_1} \oplus \cdots \oplus I_{f_k} \otimes M_{g_k}.$$

Operator algebra

Question

How to find a recovery channel without syndrome measurement?
Equivalently, how to find the error avoiding subspace?

- Let $\mathcal{A}$ be the algebra generated by $\{E_1, \ldots, E_r, E_1^\dagger, \ldots, E_r^\dagger\}$.
- By the Wedderburn Theorem, there is a unitary U such that

$$U^\dagger \mathcal{A} U = I_{f_1} \otimes M_{g_1} \oplus \cdots \oplus I_{f_k} \otimes M_{g_k}.$$

- Assume $f_1 \geq \cdots \geq f_k$, and set $(f_1, g_1) = (f, g)$. Then

$$U^\dagger \mathcal{A} U \subseteq (I_f \otimes M_g) \oplus M_{n-fg}.$$

Operator algebra

Question

How to find a recovery channel without syndrome measurement?
Equivalently, how to find the error avoiding subspace?

- Let $\mathcal{A}$ be the algebra generated by $\{E_1, \ldots, E_r, E_1^\dagger, \ldots, E_r^\dagger\}$.
- By the Wedderburn Theorem, there is a unitary U such that

$$U^\dagger \mathcal{A} U = I_{f_1} \otimes M_{g_1} \oplus \cdots \oplus I_{f_k} \otimes M_{g_k}.$$

- Assume $f_1 \geq \cdots \geq f_k$, and set $(f_1, g_1) = (f, g)$. Then

$$U^\dagger \mathcal{A} U \subseteq (I_f \otimes M_g) \oplus M_{n-fg}.$$

Thus $U^\dagger E_j U = \begin{pmatrix} I_{f_1} \otimes F_j & \\ & G_j \end{pmatrix}$ for $j = 1, \ldots, r$.

Operator algebra

Question

How to find a recovery channel without syndrome measurement?
Equivalently, how to find the error avoiding subspace?

- Let $\mathcal{A}$ be the algebra generated by $\{E_1, \ldots, E_r, E_1^\dagger, \ldots, E_r^\dagger\}$.
- By the Wedderburn Theorem, there is a unitary U such that
$$U^\dagger \mathcal{A} U = I_{f_1} \otimes M_{g_1} \oplus \cdots \oplus I_{f_k} \otimes M_{g_k}.$$
- Assume $f_1 \geq \cdots \geq f_k$, and set $(f_1, g_1) = (f, g)$. Then
$$U^\dagger \mathcal{A} U \subseteq (I_f \otimes M_g) \oplus M_{n-fg}.$$
Thus $U^\dagger E_j U = \begin{pmatrix} I_{f_1} \otimes F_j & \\ & G_j \end{pmatrix}$ for $j = 1, \ldots, r$.
- If we encode $\tilde{\rho} \in M_f$ as $\rho = U \begin{pmatrix} \tilde{\rho} \otimes \sigma & \\ & 0_{n-fg} \end{pmatrix} U^\dagger$,

  then $\mathcal{E}(\rho) = U \begin{pmatrix} \tilde{\rho} \otimes \hat{\sigma} & \\ & 0_{n-fg} \end{pmatrix} U^\dagger$ so that $\tilde{\rho}$ is recoverable.

Question

The unitary matrix U is useful in the encoding and decoding processes. How to find a "good" unitary U to implement the QEC scheme?

Representation Theory and Group Theory

Question

The unitary matrix U is useful in the encoding and decoding processes. How to find a "good" unitary U to implement the QEC scheme?

- Representation theory can help determine a matrix U.

Representation Theory and Group Theory

Question

The unitary matrix U is useful in the encoding and decoding processes. How to find a "good" unitary U to implement the QEC scheme?

- Representation theory can help determine a matrix U.
- But we need to find a unitary U which can be implemented easily (depending on the hardware).

Representation Theory and Group Theory

Question

The unitary matrix U is useful in the encoding and decoding processes. How to find a "good" unitary U to implement the QEC scheme?

- Representation theory can help determine a matrix U.
- But we need to find a unitary U which can be implemented easily (depending on the hardware).
- In particular, U should admit a decomposition

$$U = U_1 \cdots U_m$$

so that each U_i is a unitary gate (quantum gate) available in the quantum computer lab.

Representation Theory and Group Theory

Question

The unitary matrix U is useful in the encoding and decoding processes. How to find a “good” unitary U to implement the QEC scheme?

- Representation theory can help determine a matrix U.
- But we need to find a unitary U which can be implemented easily (depending on the hardware).
- In particular, U should admit a decomposition

$$U = U_1 \cdots U_m$$

  so that each U_i is a unitary gate (quantum gate) available in the quantum computer lab.
- For example, we need to use the standard gates or basic gates available at the IBM online quantum computers: qiskit.

Fully correlated channels

- Consider channels with error operators of the form $W^{\otimes n}$, where $W \in SU(2)$.

Fully correlated channels

- Consider channels with error operators of the form $W^{\otimes n}$, where $W \in SU(2)$.
- So, the action of an error operator has the form

$$\sigma_1 \otimes \cdots \otimes \sigma_n \to (W\sigma_1 W^\dagger) \otimes \cdots \otimes (W\sigma_n W^\dagger).$$

Fully correlated channels

- Consider channels with error operators of the form $W^{\otimes n}$, where $W \in SU(2)$.
- So, the action of an error operator has the form

$$\sigma_1 \otimes \cdots \otimes \sigma_n \to (W\sigma_1 W^\dagger) \otimes \cdots \otimes (W\sigma_n W^\dagger).$$

- The quantum channel may be represented by

$$\mathcal{E}(\rho) = \int W^{\otimes n}\rho(W^{\otimes n})^\dagger d\mu(W).$$

Fully correlated channels

- Consider channels with error operators of the form $W^{\otimes n}$, where $W \in SU(2)$.
- So, the action of an error operator has the form

$$\sigma_1 \otimes \cdots \otimes \sigma_n \to (W\sigma_1 W^\dagger) \otimes \cdots \otimes (W\sigma_n W^\dagger).$$

- The quantum channel may be represented by

$$\mathcal{E}(\rho) = \int W^{\otimes n} \rho (W^{\otimes n})^\dagger d\mu(W).$$

- It is possible that only a finite number unitary W may occur, say, $W \in \{I_2, \sigma_x, \sigma_y, \sigma_z\}$, where $\sigma_x, \sigma_y, \sigma_z$ are the Pauli matrices:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Frobenius formula

- One can use representation theory to decompose the algebra $\mathcal{A}$ generated by $\{W^{\otimes n} : W \in SU(2)\}$ as

$$I_{f_0} \otimes M_{g_0} \oplus \cdots \oplus I_{f_k} \otimes M_{g_k}$$

with $k = [n/2]$ (in terms of the Clebsch-Gordan coefficients).

Frobenius formula

- One can use representation theory to decompose the algebra $\mathcal{A}$ generated by $\{W^{\otimes n} : W \in SU(2)\}$ as

$$I_{f_0} \otimes M_{g_0} \oplus \cdots \oplus I_{f_k} \otimes M_{g_k}$$

with $k = [n/2]$ (in terms of the Clebsch-Gordan coefficients).

- For $j = 0, \ldots, k$,

$$f_j = \binom{n}{j} - \binom{n}{j-1} \qquad \text{and} \qquad g_j = n + 1 - 2j.$$

Frobenius formula

- One can use representation theory to decompose the algebra $\mathcal{A}$ generated by $\{W^{\otimes n} : W \in SU(2)\}$ as

$$I_{f_0} \otimes M_{g_0} \oplus \cdots \oplus I_{f_k} \otimes M_{g_k}$$

with $k = [n/2]$ (in terms of the Clebsch-Gordan coefficients).

- For $j = 0, \ldots, k$,

$$f_j = \binom{n}{j} - \binom{n}{j-1} \qquad \text{and} \qquad g_j = n + 1 - 2j.$$

- We have $2^n = f_0 * g_0 + \cdots + f_k * g_k$.

Frobenius formula

- One can use representation theory to decompose the algebra $\mathcal{A}$ generated by $\{W^{\otimes n} : W \in SU(2)\}$ as

$$I_{f_0} \otimes M_{g_0} \oplus \cdots \oplus I_{f_k} \otimes M_{g_k}$$

  with $k = [n/2]$ (in terms of the Clebsch-Gordan coefficients).

- For $j = 0, \ldots, k$,

$$f_j = \binom{n}{j} - \binom{n}{j-1} \qquad \text{and} \qquad g_j = n + 1 - 2j.$$

- We have $2^n = f_0 * g_0 + \cdots + f_k * g_k$.
- Let $n = p + q + r$, where p ($[\log_s(f_j)]$) data qubits will be protected by q ($[\log_2(g_j)]$) arbitrary qubits, and $r = n - p - q$ pure qubits. Then

Frobenius formula

- One can use representation theory to decompose the algebra $\mathcal{A}$ generated by $\{W^{\otimes n} : W \in SU(2)\}$ as

$$I_{f_0} \otimes M_{g_0} \oplus \cdots \oplus I_{f_k} \otimes M_{g_k}$$

with $k = [n/2]$ (in terms of the Clebsch-Gordan coefficients).

- For $j = 0, \ldots, k$,

$$f_j = \binom{n}{j} - \binom{n}{j-1} \qquad \text{and} \qquad g_j = n + 1 - 2j.$$

- We have $2^n = f_0 * g_0 + \cdots + f_k * g_k$.
- Let $n = p + q + r$, where p ($[\log_s(f_j)]$) data qubits will be protected by q ($[\log_2(g_j)]$) arbitrary qubits, and $r = n - p - q$ pure qubits. Then

$n = 2$: $2^2 = 1 * 3 + 1 * 1$, no error correction.

$n = 3$: $2^3 = 1 * 4 + 2 * 2$, $(p, q, r) = (1, 1, 1)$.

$n = 4$: $2^4 = 1 * 5 + 3 * 3 + 2 * 1$, $(p, q, r) = (1, 1, 2)$ or $(1, 0, 3)$.

$n = 5$: $2^5 = 1 * 6 + 4 * 4 + 5 * 2$, $(p, q, r) = (2, 2, 1)$ or $(2, 1, 2)$.

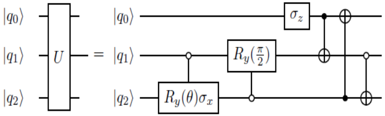
For $n = 3$, the following two unitary matrices satisfy $U^\dagger \mathcal{A} U = I_2 \otimes M_2 \oplus M_4$

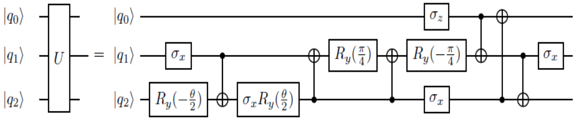
$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \sqrt{\frac{2}{3}} & 0 & 0 & 0 & 0 & \sqrt{\frac{1}{3}} & 0 & 0 \\ -\sqrt{\frac{1}{6}} & 0 & \sqrt{\frac{1}{2}} & 0 & 0 & \sqrt{\frac{1}{3}} & 0 & 0 \\ 0 & \sqrt{\frac{1}{6}} & 0 & \sqrt{\frac{1}{2}} & 0 & 0 & \sqrt{\frac{1}{3}} & 0 \\ -\sqrt{\frac{1}{6}} & 0 & -\sqrt{\frac{1}{2}} & 0 & 0 & \sqrt{\frac{1}{3}} & 0 & 0 \\ 0 & \sqrt{\frac{1}{6}} & 0 & -\sqrt{\frac{1}{2}} & 0 & 0 & \sqrt{\frac{1}{3}} & 0 \\ 0 & -\sqrt{\frac{2}{3}} & 0 & 0 & 0 & 0 & \sqrt{\frac{1}{3}} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ \sqrt{\frac{2}{3}} & 0 & 0 & 0 & \sqrt{\frac{1}{3}} & 0 & 0 & 0 \\ -\sqrt{\frac{1}{6}} & 0 & \sqrt{\frac{1}{2}} & 0 & \sqrt{\frac{1}{3}} & 0 & 0 & 0 \\ 0 & \sqrt{\frac{1}{6}} & 0 & \sqrt{\frac{1}{2}} & 0 & -\sqrt{\frac{1}{3}} & 0 & 0 \\ -\sqrt{\frac{1}{6}} & 0 & -\sqrt{\frac{1}{2}} & 0 & \sqrt{\frac{1}{3}} & 0 & 0 & 0 \\ 0 & \sqrt{\frac{1}{6}} & 0 & -\sqrt{\frac{1}{2}} & 0 & -\sqrt{\frac{1}{3}} & 0 & 0 \\ 0 & -\sqrt{\frac{2}{3}} & 0 & 0 & 0 & -\sqrt{\frac{1}{3}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

For $n = 3$, the following two unitary matrices satisfy $U^\dagger \mathcal{A} U = I_2 \otimes M_2 \oplus M_4$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \sqrt{\frac{2}{3}} & 0 & 0 & 0 & 0 & \sqrt{\frac{1}{3}} & 0 & 0 \\ -\sqrt{\frac{1}{6}} & 0 & \sqrt{\frac{1}{2}} & 0 & 0 & \sqrt{\frac{1}{3}} & 0 & 0 \\ 0 & \sqrt{\frac{1}{6}} & 0 & \sqrt{\frac{1}{2}} & 0 & 0 & \sqrt{\frac{1}{3}} & 0 \\ -\sqrt{\frac{1}{6}} & 0 & -\sqrt{\frac{1}{2}} & 0 & 0 & \sqrt{\frac{1}{3}} & 0 & 0 \\ 0 & \sqrt{\frac{1}{6}} & 0 & -\sqrt{\frac{1}{2}} & 0 & 0 & \sqrt{\frac{1}{3}} & 0 \\ 0 & -\sqrt{\frac{2}{3}} & 0 & 0 & 0 & 0 & \sqrt{\frac{1}{3}} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ \sqrt{\frac{2}{3}} & 0 & 0 & 0 & \sqrt{\frac{1}{3}} & 0 & 0 & 0 \\ -\sqrt{\frac{1}{6}} & 0 & \sqrt{\frac{1}{2}} & 0 & \sqrt{\frac{1}{3}} & 0 & 0 & 0 \\ 0 & \sqrt{\frac{1}{6}} & 0 & \sqrt{\frac{1}{2}} & 0 & -\sqrt{\frac{1}{3}} & 0 & 0 \\ -\sqrt{\frac{1}{6}} & 0 & -\sqrt{\frac{1}{2}} & 0 & \sqrt{\frac{1}{3}} & 0 & 0 & 0 \\ 0 & \sqrt{\frac{1}{6}} & 0 & -\sqrt{\frac{1}{2}} & 0 & -\sqrt{\frac{1}{3}} & 0 & 0 \\ 0 & -\sqrt{\frac{2}{3}} & 0 & 0 & 0 & -\sqrt{\frac{1}{3}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

We are only able to decompose the second one into 5 standard gates $U_1, \ldots, U_5$ or 14 basic gates $V_1, \ldots, V_{14}$ with 6 CNOT gates.





A recursive scheme

- For $n = 3$, we can use 1 abitary and 1 pure state to protect 1 data qubit.

A recursive scheme

- For $n = 3$, we can use 1 abitary and 1 pure state to protect 1 data qubit.
- Recall that:

$$n = 4\text{:}\ 2^4 = 1 * 5 + 3 * 3 + 2 * 1, \qquad (p, q, r) = (1, 1, 2) \text{ or } (1, 0, 3).$$
$$n = 5\text{:}\ 2^5 = 1 * 6 + 4 * 4 + 5 * 2, \qquad (p, q, r) = (2, 2, 1) \text{ or } (2, 1, 2).$$

A recursive scheme

- For $n = 3$, we can use 1 abitary and 1 pure state to protect 1 data qubit.
- Recall that:

$$n = 4\text{: } 2^4 = 1 * 5 + 3 * 3 + 2 * 1, \qquad (p, q, r) = (1, 1, 2) \text{ or } (1, 0, 3).$$
$$n = 5\text{: } 2^5 = 1 * 6 + 4 * 4 + 5 * 2, \qquad (p, q, r) = (2, 2, 1) \text{ or } (2, 1, 2).$$

- For $n = 4$, we can protect at most 1 data bit.

A recursive scheme

- For $n = 3$, we can use 1 abitary and 1 pure state to protect 1 data qubit.
- Recall that:

$$n = 4\text{: } 2^4 = 1 * 5 + 3 * 3 + 2 * 1, \qquad (p, q, r) = (1, 1, 2) \text{ or } (1, 0, 3).$$
$$n = 5\text{: } 2^5 = 1 * 6 + 4 * 4 + 5 * 2, \qquad (p, q, r) = (2, 2, 1) \text{ or } (2, 1, 2).$$

- For $n = 4$, we can protect at most 1 data bit.
- For $n = 5$, we can use 2 arbitary and 1 pure state to protect 2 data qubits.

A recursive scheme

- For $n = 3$, we can use 1 abitary and 1 pure state to protect 1 data qubit.
- Recall that:

$$n = 4\colon\ 2^4 = 1 * 5 + 3 * 3 + 2 * 1, \qquad (p, q, r) = (1, 1, 2) \text{ or } (1, 0, 3).$$

$$n = 5\colon\ 2^5 = 1 * 6 + 4 * 4 + 5 * 2, \qquad (p, q, r) = (2, 2, 1) \text{ or } (2, 1, 2).$$

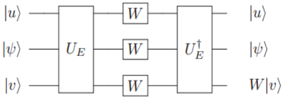
- For $n = 4$, we can protect at most 1 data bit.
- For $n = 5$, we can use 2 arbitary and 1 pure state to protect 2 data qubits.
- We can do it using the 3-qubit circuit twice:

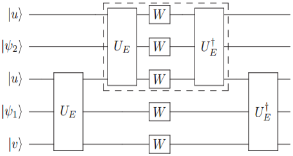
A recursive scheme

- For $n = 3$, we can use 1 abitary and 1 pure state to protect 1 data qubit.
- Recall that:

$$n = 4:\ 2^4 = 1 * 5 + 3 * 3 + 2 * 1, \qquad (p, q, r) = (1, 1, 2) \text{ or } (1, 0, 3).$$
$$n = 5:\ 2^5 = 1 * 6 + 4 * 4 + 5 * 2, \qquad (p, q, r) = (2, 2, 1) \text{ or } (2, 1, 2).$$

- For $n = 4$, we can protect at most 1 data bit.
- For $n = 5$, we can use 2 arbitary and 1 pure state to protect 2 data qubits.
- We can do it using the 3-qubit circuit twice:



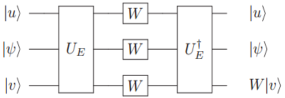


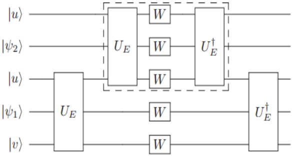
A recursive scheme

- For $n = 3$, we can use 1 abitary and 1 pure state to protect 1 data qubit.
- Recall that:

$$n = 4\text{: } 2^4 = 1 * 5 + 3 * 3 + 2 * 1, \qquad (p, q, r) = (1, 1, 2) \text{ or } (1, 0, 3).$$
$$n = 5\text{: } 2^5 = 1 * 6 + 4 * 4 + 5 * 2, \qquad (p, q, r) = (2, 2, 1) \text{ or } (2, 1, 2).$$

- For $n = 4$, we can protect at most 1 data bit.
- For $n = 5$, we can use 2 arbitary and 1 pure state to protect 2 data qubits.
- We can do it using the 3-qubit circuit twice:





- We can extend the recursive scheme to protect k data qubits using 1 arbitrary states and k pure state.

Finding a better scheme

- For $n = 6$, our recursive scheme does not work.

Finding a better scheme

- For $n = 6$, our recursive scheme does not work.
- On the other hand, $$2^6 = 1 * 7 + 5 * 5 + 9 * 3 + 5 * 1.$$

  so that $$(p, q, r) \in \{(2, 2, 2), (3, 1, 2), (2, 0, 4)\}.$$

Finding a better scheme

- For $n = 6$, our recursive scheme does not work.
- On the other hand, $$2^6 = 1 * 7 + 5 * 5 + 9 * 3 + 5 * 1.$$ so that $$(p, q, r) \in \{(2, 2, 2), (3, 1, 2), (2, 0, 4)\}.$$
- We can use 1 arbitary states, 2 pure state to protect 3 data qubits.

Finding a better scheme

- For $n = 6$, our recursive scheme does not work.
- On the other hand, $2^6 = 1 * 7 + 5 * 5 + 9 * 3 + 5 * 1.$

  so that $(p, q, r) \in \{(2, 2, 2), (3, 1, 2), (2, 0, 4)\}.$
- We can use 1 arbitary states, 2 pure state to protect 3 data qubits.
- How to construct such an circuit?

Finding a better scheme

- For $n = 6$, our recursive scheme does not work.
- On the other hand, $$2^6 = 1 * 7 + 5 * 5 + 9 * 3 + 5 * 1.$$

  so that $$(p, q, r) \in \{(2, 2, 2), (3, 1, 2), (2, 0, 4)\}.$$
- We can use 1 arbitary states, 2 pure state to protect 3 data qubits.
- How to construct such an circuit?
- We need to find a unitary $U \in M_{64}$ such that

$$U^\dagger \mathcal{A} U \subseteq I_8 \otimes M_3 \oplus M_{40}$$

and encode $\tilde{\rho} \in M_8$ as

$$\rho = P(\tilde{\rho} \otimes \sigma \oplus O_{48})P^t \subseteq M_8 \otimes M_3 \oplus M_{40}$$

with $\sigma \in M_2$ so that $U^\dagger(\mathcal{E}(\rho))U = \tilde{\rho} \otimes \hat{\sigma}$, where $\hat{\sigma} \in M_8$.

Finding a better scheme

- For $n = 6$, our recursive scheme does not work.
- On the other hand, $2^6 = 1 * 7 + 5 * 5 + 9 * 3 + 5 * 1$.

  so that $(p, q, r) \in \{(2, 2, 2), (3, 1, 2), (2, 0, 4)\}$.

- We can use 1 arbitary states, 2 pure state to protect 3 data qubits.
- How to construct such an circuit?
- We need to find a unitary $U \in M_{64}$ such that

$$U^\dagger \mathcal{A} U \subseteq I_8 \otimes M_3 \oplus M_{40}$$

  and encode $\tilde{\rho} \in M_8$ as

$$\rho = P(\tilde{\rho} \otimes \sigma \oplus O_{48})P^t \subseteq M_8 \otimes M_3 \oplus M_{40}$$

  with $\sigma \in M_2$ so that $U^\dagger(\mathcal{E}(\rho))U = \tilde{\rho} \otimes \hat{\sigma}$, where $\hat{\sigma} \in M_8$.

- The matrix U and P should admit decomposition as simple unitary gates.

Finding a better scheme

- For $n = 6$, our recursive scheme does not work.
- On the other hand, $\quad 2^6 = 1 * 7 + 5 * 5 + 9 * 3 + 5 * 1.$

  so that $\quad (p, q, r) \in \{(2, 2, 2), (3, 1, 2), (2, 0, 4)\}.$
- We can use 1 arbitary states, 2 pure state to protect 3 data qubits.
- How to construct such an circuit?
- We need to find a unitary $U \in M_{64}$ such that

$$U^\dagger \mathcal{A} U \subseteq I_8 \otimes M_3 \oplus M_{40}$$

  and encode $\tilde{\rho} \in M_8$ as

$$\rho = P(\tilde{\rho} \otimes \sigma \oplus O_{48})P^t \subseteq M_8 \otimes M_3 \oplus M_{40}$$

  with $\sigma \in M_2$ so that $U^\dagger(\mathcal{E}(\rho))U = \tilde{\rho} \otimes \hat{\sigma}$, where $\hat{\sigma} \in M_8$.
- The matrix U and P should admit decomposition as simple unitary gates.
- The recursive scheme is useful before we can find a practical and efficient scheme.

Extension to qudits

Consider quantum channels on n-qudits (d-dimensional) with error operators of the form $W^{\otimes n}$, where $W \in SU(d)$.

Extension to qudits

Consider quantum channels on n-qudits (d-dimensional) with error operators of the form $W^{\otimes n}$, where $W \in SU(d)$.

Theorem [GLNPS, 2014]

For the n-qudit channels described above, we can use $n = dk + 1$ physical qudits protect k logical qubits.

Extension to qudits

Consider quantum channels on n-qudits (d-dimensional) with error operators of the form $W^{\otimes n}$, where $W \in SU(d)$.

Theorem [GLNPS, 2014]

For the n-qudit channels described above, we can use $n = dk + 1$ physical qudits protect k logical qubits. So, the "error correction rate" is

$$k/(dk+1) \to 1/d \text{ as } n = dk + 1 \to \infty.$$

Extension to qudits

Consider quantum channels on n-qudits (d-dimensional) with error operators of the form $W^{\otimes n}$, where $W \in SU(d)$.

Theorem [GLNPS, 2014]

For the n-qudit channels described above, we can use $n = dk + 1$ physical qudits protect k logical qubits. So, the "error correction rate" is

$$k/(dk+1) \to 1/d \text{ as } n = dk + 1 \to \infty.$$

Remark One can actually find a QECC of higher dimension correcting $f(n)$ qudits such that $f(n)/n \to 1$ as $n \to \infty$.

Extension to qudits

Consider quantum channels on n-qudits (d-dimensional) with error operators of the form $W^{\otimes n}$, where $W \in SU(d)$.

Theorem [GLNPS, 2014]

For the n-qudit channels described above, we can use $n = dk + 1$ physical qudits protect k logical qubits. So, the "error correction rate" is

$$k/(dk+1) \to 1/d \text{ as } n = dk + 1 \to \infty.$$

Remark One can actually find a QECC of higher dimension correcting $f(n)$ qudits such that $f(n)/n \to 1$ as $n \to \infty$.

Question Can we find a better scheme?

Extension to qudits

Consider quantum channels on n-qudits (d-dimensional) with error operators of the form $W^{\otimes n}$, where $W \in SU(d)$.

Theorem [GLNPS, 2014]

For the n-qudit channels described above, we can use $n = dk + 1$ physical qudits protect k logical qubits. So, the "error correction rate" is

$$k/(dk+1) \to 1/d \text{ as } n = dk + 1 \to \infty.$$

Remark One can actually find a QECC of higher dimension correcting $f(n)$ qudits such that $f(n)/n \to 1$ as $n \to \infty$.

Question Can we find a better scheme?

C.K. Li, M. Nakahara, Y.T. Poon, N.S. Sze, H. Tomita, Recursive Encoding and Decoding of Noiseless Subsystem and Decoherence Free Subspace, Physical Review A 84, 044301 (2011).

U. Gungordu, C.K. Li, M. Nakahara, Y.T. Poon and N.K. Sze, Recursive encoding and decoding of the noiseless subsystem for qudits, Physical Review A, 89, 042301 (2014).

Any comments, suggestions, answers?

Any comments, suggestions, answers?

Thank you for your attention!