Introduction to Quantum Error Correction

David Kribs

Department of Mathematics and Statistics

University of Guelph

BIRS Workshop, February 2007

Outline

We will touch on the work of...

D. Bacon, M.-D. Choi, C. Bennett, I. Chuang, D. DiVincenzo, L.-M. Duan, D. Gottesman, G.-C. Guo, J. Kempe, M. Knill, K. Kraus, D.K., R. Laflamme, D. Lidar, M. Nielsen, D. Poulin, M. Rasetti, P. Shor, J. Smolin, L. Viola, K. Whaley, W. Wootters, P. Zanardi

Noise Models

Evolution $\mathcal{E}$ of an open quantum system S in contact with an external environment E, with corresponding (finite dimensional) Hilbert space $\mathcal{H} = \mathcal{H}_S \otimes \mathcal{H}_E$, is determined by a unitary $U \in \mathcal{L}(\mathcal{H})$ and density operator $\rho_E \in \mathcal{L}(\mathcal{H}_E)$ as follows: $\forall \sigma_S \in \mathcal{L}(\mathcal{H})$,

$$\begin{aligned} \sigma_S &\mapsto \sigma_S \otimes \rho_E \in \mathcal{L}(\mathcal{H}) \\ &\mapsto U(\sigma_S \otimes \rho_E)U^\dagger := \mathcal{U}(\sigma_S \otimes \rho_E) \in \mathcal{L}(\mathcal{H}) \\ &\mapsto \mathrm{Tr}_E \left(\mathcal{U}(\sigma_S \otimes \rho_E)\right) := \mathcal{E}(\rho_S) \in \mathcal{L}(\mathcal{H}_S). \end{aligned}$$

Definition. A *quantum channel* (or *operation*) on $\mathcal{H}$ is a completely positive and trace preserving (CPTP) map $\mathcal{E} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$.

Examples (1) $U \in \mathcal{L}(\mathcal{H})$ unitary;

$$\mathcal{E}(\sigma) = U\sigma U^\dagger \quad \forall \sigma \in \mathcal{L}(\mathcal{H}).$$

(2) Pauli operators:

$$X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \quad Y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right), \quad Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right).$$

The "depolarizing channel" defined on $\mathcal{L}(\mathbb{C}^2)$ is given by

$$\mathcal{E}(\sigma) = \frac{1}{4}\big(\sigma + X\sigma X^\dagger + Y\sigma Y^\dagger + Z\sigma Z^\dagger\big) = \frac{\mathrm{Tr}(\sigma)}{2}\, I_2.$$

Theorem. Let $\mathcal{E} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ be a quantum channel. Then there are operators $\{E_a\}$ on $\mathcal{H}$ such that

$$\mathcal{E}(\sigma) = \sum_a E_a \sigma E_a^\dagger \quad \forall \sigma \in \mathcal{B}(\mathcal{H}) \qquad -(CP)$$

$$\sum_a E_a^\dagger E_a = I. \qquad -(TP)$$

$\Rightarrow$ We write $\mathcal{E} = \{E_a\}$. The E_a are the *Kraus (Choi?) operators*, or *errors*, or *noise operators*, or *operation elements*, etc.

Example: Classical Noise

Probability distribution $\vec{p} = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \end{bmatrix}$; $p_j \geq 0,\ \sum_j p_j = 1.$

Stochastic matrix $M = [r_{ij}]$; $r_{ij} \geq 0,\ \sum_i r_{ij} = 1\ \forall j.$

$$\Rightarrow\ \vec{q} = M\vec{p}$$

As a channel: $\forall i, j$ let $E_{ij} = \sqrt{r_{ij}}\,|i\rangle\langle j|$, then

$$\Rightarrow \rho = \mathrm{diag}\,(p_j) \quad \mapsto \quad \sum_{i,j} E_{ij}\rho E_{ij}^{\dagger}.$$

QEC Standard Framework

Basic Setting.

$\Rightarrow \mathbb{C}^2 = \text{span}\{|0\rangle, |1\rangle\}$ Hilbert space for a two level quantum system. Quantum bits (qubits) are given by unit vectors

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

$\Rightarrow |\psi\rangle$ is a superposition of $|0\rangle$ and $|1\rangle$ if $\alpha \neq 0 \neq \beta$.

$\Rightarrow$ n-qubit Hilbert space $\mathcal{H} = \mathbb{C}^{2^n} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$ has an orthonormal basis given by

$$\Big\{ |i_1 \cdots i_n\rangle = |i_1\rangle \otimes \ldots \otimes |i_n\rangle \;\Big|\; i_j = 0, 1 \Big\}.$$

$\Rightarrow$ We can define operators $\{X_k, Y_k, Z_k : 1 \leq k \leq n\}$, on n-qubit space $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ by, for instance,

$$X_1 = X \otimes I_2 \otimes I_2 \otimes \ldots$$

$$X_2 = I_2 \otimes X \otimes I_2 \otimes \ldots.$$

The n-qubit **Pauli group** $\mathcal{P}_n$ is the unitary subgroup of $\mathcal{L}(\mathcal{H})$ generated by n-tensor products of elements from the single qubit Pauli group,

$$\mathcal{P}_1 = \Big\{ \pm I_2, \pm iI_2, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ \Big\}.$$

$\Rightarrow$ Elements of $\mathcal{P}_n$ either commute or anti-commute.

$\Rightarrow$ Codes (in the standard framework) are given by subspaces $\mathcal{C} \subseteq \mathcal{H}$. The subspace can encode $[\log(\dim \mathcal{C})]$ logical qubits.

Definition. A code $\mathcal{C}$ is *correctable* for an error model $\mathcal{E}$ on $\mathcal{H}$ if there is a CPTP map $\mathcal{R} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ such that

$$\big(\mathcal{R} \circ \mathcal{E}\big)(\sigma) = \sigma \quad \forall \sigma \in \mathcal{L}(\mathcal{C}) \subseteq \mathcal{L}(\mathcal{H}).$$

Theorem. The following are equivalent:

(1) $\mathcal{C}$ is correctable for $\mathcal{E} = \{E_a\}$.

(2) There are scalars $\Lambda = (\lambda_{ab})$ such that

$$P_{\mathcal{C}} E_a^\dagger E_b P_{\mathcal{C}} = \lambda_{ab} P_{\mathcal{C}} \quad \forall a, b.$$

Example

Let $\mathcal{C} = \mathrm{span}\{|00\rangle, |11\rangle\} \subseteq \mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$ and

$$\mathcal{E} = \left\{ \frac{1}{\sqrt{2}} \mathbb{1}_4, \frac{1}{\sqrt{2}} X_1 \right\} \quad \text{where} \quad X_1 = X \otimes \mathbb{1}_2.$$

Let $\mathcal{C}_1 = X_1 \mathcal{C} = \mathrm{span}\{|10\rangle, |01\rangle\}$.

Then $\mathcal{R} = \{I_4^\dagger P_{\mathcal{C}}, X_1^\dagger P_{\mathcal{C}_1}\} = \{P_{\mathcal{C}}, X_1 P_{\mathcal{C}_1}\}$ corrects $\mathcal{E}$ on $\mathcal{C}$.

Passive QEC: Decoherence-Free Subspaces.

In PQEC, symmetries within the noise of quantum channels are used to encode states in “quiet” subspaces or subsystems of the system Hilbert space prior to evolution.

Simplistic view of PQEC:

QEC frameworks typically consist of triples $(\mathcal{R}, \mathcal{E}, \mathcal{C})$, where $\mathcal{C}$ is a code, $\mathcal{E}$ is an error model, and $\mathcal{R}$ is a recovery operation.

$\Rightarrow$ PQEC can be thought of the case with $\mathcal{R} = \mathrm{id}$.

Definition. A subspace $\mathcal{C} \subseteq \mathcal{H}$ is *decoherence-free* for $\mathcal{E} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ if

$$\mathcal{E}(\sigma) = \sigma \qquad \forall \sigma = P_{\mathcal{C}} \sigma P_{\mathcal{C}}.$$

$\Rightarrow$ Fundamental examples are given by joint eigenspaces for the noise operators of $\mathcal{E} = \{E_a\}$.

E.g. On n-qubit space, with $1 \leq k < n$, the subspace

$$\mathcal{C} = \mathrm{span}\left\{ |00\cdots 0\, i_{k+1} \cdots i_n\rangle \;\middle|\; i_j = 0 \,\mathrm{or}\, 1 \right\}$$

is a joint eigenvalue-1 space (a "stabilizer space") for $Z_1, Z_2, \ldots, Z_k$ of dimension 2^{n-k}.

Stabilizer Formalism.

The stabilizer formalism provides the most useful framework for constructing codes (for Pauli error models) in Active QEC (i.e., $\mathcal{R} \neq id$).

Starting Point: Codes are obtained by first considering joint eigenvalue-1 eigenspaces (stabilizer subspaces) $\mathcal{V}_G$ for abelian subgroups G of $\mathcal{P}_n$.

E.g. $G =< Z_1, \ldots, Z_k >$ for some $1 \leq k < n$, and the code subspace above.

Theorem. If G is an abelian subgroup of $\mathcal{P}_n$, with minimal generating set of k elements such that $-I \notin G$, then $\mathcal{V}_G$ is a 2^{n-k}-dimensional subspace (and hence encodes $n-k$ logical qubits).

$\Rightarrow$ The stablizer code $\mathcal{V}_G$ is correctable for any noise model with error operators taken from G, but more is true...

$\Rightarrow$ Let $N(G) = Z(G)$ be the normalizer (and centralizer) of G inside $\mathcal{P}_n$.

Theorem. Let G be an abelian subgroup of $\mathcal{P}_n$, such that $-I \notin G$, with stabilizer subspace $\mathcal{V}_G$. Suppose $\{E_a\}$ is a set of operators in $\mathcal{P}_n$ such that

$$E_a^\dagger E_b \notin N(G) \setminus G \quad \forall a, b.$$

Then $\{E_a\}$ is a correctable set of errors for the code $\mathcal{V}_G$.

Example. The 9-qubit code is a 2-dimensional (single qubit) subspace of 9-qubit space that corrects any collection of single qubit errors. The code $\mathcal{V}_G$ is the stablizer for the group G with generators:

$$
\begin{array}{c|ccccccccc}
g_1 & Z & Z & I & I & I & I & I & I & I \\
g_2 & I & Z & Z & I & I & I & I & I & I \\
g_3 & I & I & I & Z & Z & I & I & I & I \\
g_4 & I & I & I & I & Z & Z & I & I & I \\
g_5 & I & I & I & I & I & I & Z & Z & I \\
g_6 & I & I & I & I & I & I & I & Z & Z \\
g_7 & X & X & X & X & X & X & I & I & I \\
g_8 & I & I & I & X & X & X & X & X & X
\end{array}
$$

E.g. Consider the single qubit errors X_1 and Y_4. The product $X_1 Y_4 = XIIYIIIII$ anti-commutes with g_1, and thus does not belong to $Z(G)$.

$\Rightarrow$ In vector form, the 9-qubit code is given by

$$\mathcal{V}_G = \mathrm{span}\{|0_L\rangle, |1_L\rangle\}$$

where

$$|0_L\rangle := \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

$$|1_L\rangle := \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}.$$

QEC Subsystem Framework

(a.k.a. Operator QEC)

Basic Setting.

A quantum system A is a *subsystem* of $\mathcal{H}$ if there is another system B such that $A \otimes B$ is a subspace of $\mathcal{H}$;

$$\mathcal{H} = (A \otimes B) \oplus (A \otimes B)^{\perp}.$$

Note. The case $\dim B = 1$ yields subspaces.

Definition. A subsystem A is *correctable* for an error model $\mathcal{E}$ on $\mathcal{H}$ if there is a CPTP map $\mathcal{R} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ such that

$$\forall \sigma^A \forall \sigma^B \ \exists \tau^B \ : \ \big(\mathcal{R} \circ \mathcal{E}\big)(\sigma^A \otimes \sigma^B) = \sigma^A \otimes \tau^B .$$

Note. If A is correctable for $\mathcal{E}$, and if we fix a state $|\beta\rangle \in B$, then $A \otimes |\beta\rangle$ is a correctable *subspace* code for $\mathcal{E}$.

Theorem. The following are equivalent:

(1) A is correctable for $\mathcal{E} = \{E_a\}$.

(2) There are operators F_{ab} on B such that

$$P_{A\otimes B}\ E_a^\dagger E_b\ P_{A\otimes B} = I_A \otimes F_{ab} \quad \forall a, b.$$

$\Rightarrow$ The proof is constructive.

Passive QEC: Noiseless Subsystems.

Definition. A subsystem A is a *noiseless subsystem* for $\mathcal{E}$ if ($\dim A > 1$ and)

$$\forall \sigma^A \, \forall \sigma^B \; \exists \tau^B : \mathcal{E}(\sigma^A \otimes \sigma^B) = \sigma^A \otimes \tau^B .$$

Equivalently,

$$(\mathrm{Tr}_B \circ \mathcal{E})(\sigma) = \mathrm{Tr}_B(\sigma) \quad \forall \sigma = \sigma^A \otimes \sigma^B .$$

Note. This definition can be regarded as the $\mathcal{R} = \mathrm{id}$ case in Subsystem QEC.

Theorem. Let $\mathcal{E} = \{E_a\}$ be a quantum channel on $\mathcal{H}$, and suppose $\mathcal{H} = (A \otimes B) \oplus \mathcal{K}$. Then the following two conditions are equivalent:

(1) A is a NS (or DFS when $\dim B = 1$) for $\mathcal{E}$.

(2) There are operators F_a such that

$$P_{A\otimes B}\ E_a\ P_{A\otimes B} = I_A \otimes F_a \quad \forall a.$$

Consider the unital case: $\mathcal{E}(I) = \sum_a E_a E_a^\dagger = I$.

$\Rightarrow$ If $\sigma \in \{E_a\}'$, then $\mathcal{E}(\sigma) = \sum_a E_a \sigma E_a^\dagger = \sigma \mathcal{E}(I) = \sigma$.

Theorem. If $\mathcal{E}$ is a unital channel, then

$$\{E_a\}' = \mathrm{Fix}\,(\mathcal{E}) := \{\sigma : \mathcal{E}(\sigma) = \sigma\}.$$

$\Rightarrow$ $\exists m_k, n_k \geq 1$ such that $\mathrm{Fix}\,(\mathcal{E}) \cong \bigoplus_k (I_{m_k} \otimes \mathcal{M}_{n_k})$.

$\Rightarrow$ Let $\mathcal{H} = \bigoplus_k A_k \otimes B_k$ be the spatial decomposition. Then each A_k (such that $\dim A_k > 1$) is a NS/DFS for $\mathcal{E}$.

$\Rightarrow$ In fact, every NS/DFS for a unital channel $\mathcal{E}$ can be obtained in this way.

Example. $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathcal{E} = \{Z_1, Z_2\}$ given by,

$$\mathcal{E}(\sigma) = \frac{1}{2}(Z_1 \sigma Z_1^\dagger + Z_2 \sigma Z_2^\dagger).$$

$\Rightarrow$ Then the "noise commutant" satisfies:

$$\{Z_1, Z_2\}' = \mathrm{Fix}\,(\mathcal{E}) = \left\{ \begin{pmatrix} a & & & 0 \\ & b & & \\ & & c & \\ 0 & & & d \end{pmatrix} \right\}.$$

$\Rightarrow$ $\mathcal{E}$ has no NS/DFS.

Example. $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathcal{E} = \{UZ_1, UZ_2\}$ given by,

$$\mathcal{E}(\sigma) = \frac{1}{2} U (Z_1 \sigma Z_1^\dagger + Z_2 \sigma Z_2^\dagger) U^\dagger,$$

where $U = \mathbb{1}_4 - 2|11\rangle\langle 11|$.

$\Rightarrow$ Here $\{UZ_1, UZ_2\}' = \mathrm{Fix}\,(\mathcal{E}) = \left\{ \begin{pmatrix} a & 0 & 0 & b \\ 0 & e & 0 & 0 \\ 0 & 0 & f & 0 \\ c & 0 & 0 & d \end{pmatrix} \right\}.$

Thus, $\mathrm{Fix}\,(\mathcal{E}) \cong \mathcal{M}_2 \oplus \mathbb{C} \oplus \mathbb{C}$, and $\mathcal{E}$ has a single qubit DFS.

Specifically, $\mathcal{E}(\sigma) = \sigma$ for all σ of the form

$$\sigma = a|00\rangle\langle 00| + b|00\rangle\langle 11| + c|11\rangle\langle 00| + d|11\rangle\langle 11|.$$

Stabilizer Subsystem Codes.

There is a natural extension of the stabilizer formalism to the case of subsystem codes.

Starting Point: Codes are obtained by considering the commutant structure G' of arbitrary (not necessarily abelian) subgroups G of $\mathcal{P}_n$.

Idea: Suppose

$$\mathrm{Alg}\,(G) = \bigoplus_k I_{m_k} \otimes \mathcal{M}_{n_k},$$

and so

$$G' = \bigoplus_k \mathcal{M}_{m_k} \otimes I_{n_k}.$$

Let

$$\mathcal{H} = \bigoplus_k A_k \otimes B_k$$

be the associated spatial decomposition and put

$$P_k := P_{A_k \otimes B_k} = I_{A_k \otimes B_k}.$$

$\Rightarrow$ Let $\{g_i\} \subseteq G$, and suppose $g_i = \bigoplus_k I_{A_k} \otimes b_{k,i}$. Then $\forall i, j$ and $\forall k$,

$$\begin{aligned} P_k g_i^\dagger g_j P_k &= (P_k g_i^\dagger P_k)(P_k g_j P_k) \\ &= I_{A_k} \otimes b_{k,i}^\dagger b_{k,j}. \end{aligned}$$

Hence, A_k is correctable for $\{g_i\}$.

Example. Let $G =< Z\,I,\;\; X\,X >$. Then G' encodes a single qubit stabilizer subsystem, since

$$G' = \left\{ \begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & d & c \\ 0 & 0 & b & a \end{pmatrix} : a, b, c, d \in \mathbb{C} \right\} \cong I_2 \otimes \mathcal{M}_2.$$

$\Rightarrow$ Conjugation by the controlled-NOT unitary explicitly yields the form $G' \cong I_2 \otimes \mathcal{M}_2$.