Introduction to Quantum Error Correction

Students: H. Ananthakrishnan, E. Barajas, A. Bhutiani, S. Cheng, S. Choudhary, S. Dulam, C. Eddington, J. Go P. Jasso, V. Joshi, D. Kamaraj, S. Karuturi, A. Mansingh, L. Miao, A. Pashupati, M. Perera, A. Prakash, K. Prasad, C. Schneider, A. Sivaraman, S. Somani, K. Uppal, D. Wang, R. Wang, D. Xianto, L. Yang, Y. Yardi

Primary Facilitator: Dheeran E. Wiggins *Co-Facilitator:* Dr. Micah E. Fogel

Groups and Hilbert Spaces

Definition (Group). *A group is a pair $(G, \cdot)$ where G is a set and $\cdot : G^2 \to G$ is a binary operation such that (i) for all $g_1, g_2, g_3 \in G$, we have $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$, (ii) there exists an $e \in G$ such that for all $g \in G$, $e \cdot g = g = g \cdot e$, and (iii) for all $g \in G$, there exists a $g^{-1} \in G$ so that $g \cdot g^{-1} = e = g^{-1} \cdot g$.*

Definition (Homomorphism). *A function $\phi : G \to G'$ between groups is a homomorphism if it preserves the respective operation functions of G and G'.*

Definition (Isomorphism). *A homomorphism ϕ is an isomorphism if it has an inverse ϕ^{-1}.*

Definition (Centralizer). *The centralizer $C_G(S)$ of a set $S \subseteq G$ is defined as*

$$C_G(S) = \{g \in G : gs = sg \text{ for all } s \in S\}.$$

Definition (Normalizer). *The normalizer $\mathcal{N}_G(S)$ of a subset $S \subseteq G$ is*

$$\mathcal{N}_G(S) = \{g \in G : gSg^{-1} = S\},$$

where

$$gSg^{-1} = \{gsg^{-1} : s \in S\}.$$

Definition (Vector Space). *A vector space over $\mathbb{C}$ is a pair $((\mathcal{H}, +), \cdot)$, where $(\mathcal{H}, +)$ is a group under addition and $\cdot : \mathbb{C} \times \mathcal{H} \to \mathcal{H}$ is an "action" by the complex numbers which satisfies compatibility, identity, and distributivity of the action over addition for both the "vectors" in $\mathcal{H}$ and the "scalars."*

Definition (Direct Sum). *The direct sum $\mathcal{H}_1 \oplus \mathcal{H}_2$ takes two vector spaces and returns a third, larger space of tuples in $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively, and thus, is closed under both operations' componentwise addition and scalar multiplication from $\mathbb{C}$. In general, the direct sum of spaces indexed by $i \in I$ is all tuples in $\mathcal{H}_i$ with finitely many nonzero entries.*

Definition (Finite-Dimensional Hilbert Space). *A complex, finite-dimensional Hilbert space $\mathcal{H}$ is a complex, finite-dimensional inner product space $(\mathcal{H}, (\cdot, \cdot))$.*

Knill-Laflamme Subspace Condition

Definition (Superoperator). *A superoperator is a bounded linear map $\Phi : \mathbb{B}(\mathcal{H}^A) \to \mathbb{B}(\mathcal{H}^B)$, where $\mathbb{B}(\mathcal{H})$ represents the space of bounded linear operators on $\mathcal{H}$. Since $\mathbb{B}(\mathcal{H})$ itself forms a Hilbert space, these maps describe the transformations between spaces of operators.*

Definition (Quantum Channel). *A quantum channel is a type of superoperator, represented as a bounded linear map $\mathcal{E} : \mathbb{B}(\mathcal{H}^A) \to \mathbb{B}(\mathcal{H}^B)$ that satisfies the following properties: (i) Completely Positive: The map $\mathcal{E}$ is completely positive, meaning that for any auxiliary Hilbert space $\mathcal{H}^C$, the extended map $\mathcal{I}^C \otimes \mathcal{E}$ is positive, where $\mathcal{I}^C$ is the identity map on $\mathbb{B}(\mathcal{H}^C)$, and (ii) Trace Preserving: The map $\mathcal{E}$ is trace preserving, meaning that for any state ρ, $\operatorname{tr}(\rho) = \operatorname{tr}(\mathcal{E}(\rho))$.*

Theorem (Choi-Jamiołkowski Isomorphism). *A vector isomorphism Δ can be drawn between from superoperators in the set $\mathbb{B}(\mathbb{B}(\mathcal{H}^A) : \mathbb{B}(\mathcal{H}^B))$ to bounded operators in the set $\mathbb{B}(\mathcal{H}^A \otimes \mathcal{H}^B)$. This isomorphism sends every superoperator Φ to its Choi matrix J_Φ. The inverse map Δ^{-1} sends every Choi matrix to a superoperator $\Phi : \rho \mapsto \operatorname{tr}_A((\rho^t \otimes I^B)(J))$.*

Theorem (Kraus Representation). *A superoperator $\Phi : \mathbb{B}(\mathcal{H}^A) \to \mathbb{B}(\mathcal{H}^B)$ is completely positive if and only if there exist Kraus operators $\{E_i : \mathcal{H}^A \to \mathcal{H}^B\}_{i=1}^r$ such that:*

$$\Phi(X) = \sum_i E_i X E_i^\dagger, \quad \text{for all } X \in \mathbb{B}(\mathcal{H}^A).$$

Definition (Correctable Error). *An error $\mathcal{E}$ which can be corrected by a recovery operation $\mathcal{R}$ via $(\mathcal{R} \circ \mathcal{E})(\rho) \propto \rho$ is called "correctable" as long as both are quantum channels and there exists a $\mathbb{C}$-linear subspace $\mathcal{C} \subseteq \mathcal{H}$ called the code space such that $\rho \in \mathbb{B}(\mathcal{C})$.*

Theorem (Knill-Laflamme). *Let $\mathcal{E} : \mathbb{B}(\mathcal{H}) \to \mathbb{B}(\mathcal{H})$ be a quantum error channel with Kraus operators $\{E_i\}_{i=1}^r$, and let $P : \mathcal{H} \twoheadrightarrow \mathcal{C}$ be the orthogonal projection onto the code space $\mathcal{C} \subseteq \mathcal{H}$. Then, $\mathcal{E}$ is correctable if and only if*

$$PE_a^\dagger E_b P = \lambda_{ab} P,$$

where $[\lambda_{ab}] \in \mathbb{M}_r(\mathbb{C})$ is self-adjoint (Hermitian).

In other words, a quantum error $\mathcal{E}$'s "correctability" is entirely determined by its Kraus operators and the projection. When the Knill-Laflamme condition is satisfied, a correctable error can be inputted into the recovery channel $\mathcal{R}$ to return the code space $\mathcal{C}$ to its previous state, as $\mathcal{R}(\mathcal{E}(\rho)) \propto \rho$ (which becomes $\mathcal{R}(\mathcal{E}(\rho)) = \rho$ when the partial trace is applied).

The Stabilizer Formalism and n-qubit Pauli Group

Definition (Pauli Group). *The Pauli group is a multiplicative 2×2 matrix group defined by $\mathcal{P} = \langle X, Y, Z \rangle$, where*

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The Pauli group naturally acts on a 1-qubit system (with state space $\mathbb{C}^2$) via multiplication. Since an n-qubit system has state space $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$, the analog of the Pauli group for this space should somehow "live in" $\mathcal{P}_n \otimes \mathcal{P}_n \otimes \cdots \otimes \mathcal{P}_n$ to act on this state space.

Definition (n-qubit Pauli Group). *The n-qubit Pauli group is the set*

$$\mathcal{P}_n = \left\{ \gamma \bigotimes_{i=1}^n \sigma_i : \sigma_i \in \mathcal{P} \text{ and } \gamma \in \{\pm 1, \pm i\} \right\}.$$

Definition (Stabilizer Subgroup). *Let there be a subgroup $\mathcal{S} \leq \mathcal{P}_n$ that is abelian and such that $-I \notin \mathcal{S}$. Without loss of generality, assume $\mathcal{S} = \langle Z_1, \ldots, Z_s \rangle$ for $s \leq n$, where Z_j denotes a 1-local action of Z on the jth qubit. We call $\mathcal{S}$ a stabilizer subgroup.*

Definition (Stabilizer Code Space). *Given a stabilizer $\mathcal{S}$, define the associated code space by $\mathcal{C}(\mathcal{S}) = \operatorname{span}\{v \in (\mathbb{C}^2)^{\otimes n} : Z_j v = v \text{ for all } 1 \leq j \leq s\}$. These are all vectors which are invariant under the action of the stabilizer $\mathcal{S}$.*

Theorem (Stabilizer Formalism). *An error $\mathcal{E}$ with Kraus operators $\{E_i\}_{i=1}^r$ is correctable on the code space $\mathcal{C}(\mathcal{S})$ if and only if*

$$E_a^\dagger E_b \in \operatorname{span}\{\mathcal{P}_n \backslash \mathcal{N}_{\mathcal{P}_n}(\mathcal{S}) \cup \mathcal{S}\}.$$

Operator Quantum Error Correction

In general, motivated by the form of the so-called *noise commutant* $\mathcal{A}'$, we may form a Hilbert space decomposition

$$\mathcal{H} \simeq \bigoplus_J \mathcal{H}_J^A \otimes \mathcal{H}_J^B.$$

Pulling apart the sectors of the decomposition, we may simplify and fix a code space $\mathcal{H}^A \otimes \mathcal{H}^B$, yielding a new fixed partition

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

We call $\mathcal{H}^A$ a *noiseless subsystem*, thus stashing any information in the A-system of the code space. Then, letting $\mathcal{S} = \langle Z_1, Z_2, \ldots, Z_s \rangle$ be an n-fold Pauli stabilizer, we may form the gauge group

$$\mathcal{G} = \langle i, Z_1, \ldots, Z_s, X_{s+1}, Z_{s+1}, \ldots, X_{s+r}, Z_{s+r} \rangle,$$

writing that there exist s *stabilizer* qubits, r *gauge* qubits, and $n - s - r$ *logical* qubits.

Theorem (Poulin's Stabilizer Formalism). *Given an error channel $\mathcal{E}$ on $\mathcal{H}$, as above, a recovery channel $\mathcal{R}$ exists if and only if for all $1 \leq a, b \leq r$, the error Kraus operators satisfy*

$$E_a^\dagger E_b \in \operatorname{span}\{\mathcal{P}_n \setminus \mathcal{N}_{\mathcal{P}_n}(\mathcal{S}) \cup \mathcal{G}\}.$$

References

[1] R. Araiza and F. Leditzky. Basics of finite-dimensional quantum information theory, 2022.

[2] R. Duan. Super-activation of zero-error capacity of noisy quantum channels, 2009.

[3] D. S. Dummit and R. M. Foote. *Abstract Algebra*. Wiley, 3 edition, 2003.

[4] S. H. Friedberg, A. J. Insel, and L. E. Spence. *Linear Algebra*. Pearson, 5 edition, 2021.

[5] D. Gottesman. Stabilizer codes and quantum error correction, 1997.

[6] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *Physical Review Letters*, 84(11), 2000.

[7] D. Kribs, R. Laflamme, D. Poulin, and M. Lesosky. Operator quantum error correction, 2006.

[8] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 10 edition, 2016.

[9] D. Poulin. Stabilizer formalism for operator quantum error correction. *Phys. Rev. Lett.*, 95:230504, Dec 2005.

This expositional poster was compiled and presented by the listed students at the Intersession 2025 Expo at the Illinois Mathematics and Science Academy.