CORRECTABLE PAULI ERRORS IN STABILIZER CODES

NAVIN KASHYAP

Let $\mathcal{S} \le \mathcal{P}_n$ be a stabilizer group, i.e., a subgroup of $\mathcal{P}_n$ that does not contain $-I_N$. Define $\mathcal{S}^\Phi := \langle \mathcal{S} \cup \{i \cdot I_N\}\rangle$. In words, $\mathcal{S}^\Phi$ is the group consisting of operators in $\mathcal{S}$ with all possible phase factors i^ℓ attached: $\mathcal{S}^\Phi = \left\{ i^\ell M : M \in \mathcal{S}, \ell \in \{0,1,2,3\} \right\}$.

Theorem 1. *Let $S \le \mathcal{P}_n$ be a stabilizer group, with $\mathcal{Q}_\mathcal{S}$ the associated quantum stabilizer code. A collection of Pauli error operators $\mathcal{E} \subseteq \mathcal{P}_n$ is correctable by $\mathcal{Q}_\mathcal{S}$ if and only if*

$$E_k^\dagger E_\ell \notin C(\mathcal{S}) \setminus \mathcal{S}^\Phi \quad \textit{for all } E_k, E_\ell \in \mathcal{E}. \tag{1}$$

Proof. The idea is to show that a set of error operators $\mathcal{E} \subseteq \mathcal{P}_n$ satisfies the Knill-Laflamme condition

$$\langle \varphi | E_k^\dagger E_\ell | \psi \rangle = C_{k,l} \langle \varphi | \psi \rangle \quad \text{for all } E_k, E_\ell \in \mathcal{E} \text{ and all } |\varphi\rangle, |\psi\rangle \in \mathcal{Q}_\mathcal{S}. \tag{KL}$$

if and only if (1) holds.

(1) $\implies$ (KL): Let $E_k, E_\ell \in \mathcal{E}$ be such that $E_k^\dagger E_\ell \notin C(\mathcal{S}) \setminus \mathcal{S}^\Phi$. Then, either $E_k^\dagger E_\ell \notin C(\mathcal{S})$ (let's call this Case 1) or $E_k^\dagger E_\ell \in \mathcal{S}^\Phi$ (call this Case 2). Let us consider Case 1 first. In this case, there is some $M \in \mathcal{S}$ with which $E_k^\dagger E_\ell$ does not commute, i.e., $(E_k^\dagger E_\ell) \cdot M = -M \cdot (E_k^\dagger E_\ell)$. Then, for any $|\varphi\rangle, |\psi\rangle \in \mathcal{Q}_\mathcal{S}$, we have

$$\langle \varphi | E_k^\dagger E_\ell | \psi \rangle \;=\; \langle \varphi | E_k^\dagger E_\ell \cdot \underbrace{M |\psi\rangle}_{=|\psi\rangle} \;=\; -\langle \varphi | M \cdot E_k^\dagger E_\ell | \psi \rangle \;=\; -\langle \varphi | E_k^\dagger E_\ell | \psi \rangle .$$

Hence, $\langle \varphi | E_k^\dagger E_\ell | \psi \rangle = 0$. Therefore, for any $E_k, E_\ell \in \mathcal{E}$ such that $E_k^\dagger E_\ell \notin C(\mathcal{S})$, the condition in (KL) holds with $C_{k,l} = 0$.

Now, consider Case 2: $E_k^\dagger E_\ell \in \mathcal{S}^\Phi$. In this case, $E_k^\dagger E_\ell = i^{e(k,\ell)} M$ for some $M \in \mathcal{S}$ and some $e(k,\ell) \in \{0,1,2,3\}$. Then, for any $|\varphi\rangle, |\psi\rangle \in \mathcal{Q}_\mathcal{S}$, we have

$$\langle \varphi | E_k^\dagger E_\ell | \psi \rangle \;=\; i^{e(k,\ell)} \langle \varphi | M | \psi \rangle \;=\; i^{e(k,\ell)} \langle \varphi | \psi \rangle .$$

Thus, in this case, the condition in (KL) holds with $C_{k,\ell} = i^{e(k,\ell)}$.

So, in both cases, the Knill-Laflamme condition (KL) holds.

(KL) $\implies$ (1): Suppose, to the contrary, that (KL) holds but not (1). This means that there exists $E_k, E_\ell \in \mathcal{E}$ for which $\langle \varphi | E_k^\dagger E_\ell | \psi \rangle = C_{k,l} \langle \varphi | \psi \rangle$ for all $|\varphi\rangle, |\psi\rangle \in \mathcal{Q}_\mathcal{S}$, but $E_k^\dagger E_\ell \in C(\mathcal{S}) \setminus \mathcal{S}^\Phi$. In particular, $E := E_k^\dagger E_\ell$ is not in S^Φ, but it commutes with all $M \in \mathcal{S}$. This implies (by simultaneous diagonalizability) that there is a common eigenbasis for E and all $M \in \mathcal{S}$. As a consequence, there is a basis $|\varphi_1\rangle, \ldots, |\varphi_m\rangle$ of $\mathcal{Q}_\mathcal{S}$ such that all the $|\varphi_j\rangle$'s are also eigenvectors of E.

We claim that the eigenvalues associated with the eigenvectors $|\varphi_j\rangle$ of E are the same for all j. Indeed, suppose $E|\varphi_j\rangle = \lambda_j |\varphi_j\rangle$. Then, $\langle \varphi_j | E_k^\dagger E_\ell | \varphi_j \rangle = \langle \varphi_j | E | \varphi_j \rangle = \lambda_j$. But by (KL), $\langle \varphi_j | E_k^\dagger E_\ell | \varphi_j \rangle$ cannot have a dependence on $|\varphi_j\rangle$. Hence, $\lambda_j = \lambda$ for all j. Note that, since E is in the Pauli group $\mathcal{P}_n$, it is of the form $\pm M_1 \otimes \cdots \otimes M_n$ or $\pm i \cdot M_1 \otimes \cdots \otimes M_n$, with $M_j \in \{I, X, Y, Z\}$ for all j. When E is of the first form, then the eigenvalue λ must be ± 1, and when E is of the second form, then λ must be $\pm i$.

Now, define $E' := \lambda^{-1} E$, and note that (regardless of whether $\lambda = \pm 1$ or $\lambda = \pm i$) E' is of the form $\pm M_1 \otimes \cdots \otimes M_n$. In particular, $(E')^2 = I_N$. Moreover, since E is not in $\mathcal{S}^\Phi$, neither is E'. From this, it follows that we cannot obtain $-I_N$ by taking products of operators in $\mathcal{S} \cup \{E'\}$. Therefore, if we set $\mathcal{S}' := \langle \mathcal{S} \cup \{E'\}\rangle$ to be the subgroup of $\mathcal{P}_n$ generated by the operators in $\mathcal{S}$ along with E', then $-I_N \notin \mathcal{S}'$. Thus, $\mathcal{S}'$ is also a stabilizer group in $\mathcal{P}_n$.

Since $E' \notin \mathcal{S}^\Phi$, we have $|\mathcal{S}'| > |\mathcal{S}|$, and hence, $\dim \mathcal{Q}_{\mathcal{S}'} = 2^n/|\mathcal{S}'| < 2^n/|\mathcal{S}| = \dim \mathcal{Q}_{\mathcal{S}}$. On the other hand, for each j, we have

$$E' \left|\varphi_j\right\rangle \;=\; \lambda^{-1} \cdot E \left|\varphi_j\right\rangle \;=\; \lambda^{-1} \cdot \lambda \left|\varphi_j\right\rangle \;=\; \left|\varphi_j\right\rangle.$$

Thus, $\left|\varphi_j\right\rangle \in \mathcal{Q}_{\mathcal{S}'}$ for all j, which implies that $\mathcal{Q}_{\mathcal{S}} \subseteq \mathcal{Q}_{\mathcal{S}'}$, which contradicts the fact that $\dim \mathcal{Q}_{\mathcal{S}'} < \dim \mathcal{Q}_{\mathcal{S}}$. So, our initial assumption, namely, that (KL) holds but not (1), cannot be valid. □

MINIMUM DISTANCE

Definition 1. *The symplectic weight of a Pauli operator $M = i^\ell \cdot M_1 \otimes \cdots \otimes M_n$, with $M_j \in \{I, X, Y, Z\}$ for all j, is defined as*

$$\mathrm{wt_s}(M) \;:=\; |\{j : M_j \neq I\}|$$

We then have the following notion of minimum distance of a stabilizer code.

Definition 2. *For a quantum stabilizer code $\mathcal{Q}_{\mathcal{S}}$ with $\dim \mathcal{Q}_{\mathcal{S}} > 1$, associated with the stabilizer group $\mathcal{S}$, the minimum distance is defined as*

$$d_{\min}(\mathcal{Q}_{\mathcal{S}}) \;:=\; \min\bigl\{\mathrm{wt_s}(M) : M \in C(\mathcal{S}) \setminus \mathcal{S}^\Phi\bigr\}.$$

With this, an $[[n,k,d]]_2$ quantum stabilizer code is a 2^k-dimensional subspace of $\mathbb{C}^{2^n}$ having minimum distance d.

Example 1. *For $\mathcal{S} = \langle IZZ, ZIZ\rangle$, we have $d_{\min}(\mathcal{Q}_{\mathcal{S}}) = 1$, since IIZ is an operator of symplectic weight 1 in $C(\mathcal{S}) \setminus \mathcal{S}^\Phi$. Thus, $\mathcal{Q}_{\mathcal{S}}$ is a $[[3,1,1]]_2$ quantum stabilizer code.*

The utility of this notion of minimum distance derives from the following proposition.

Proposition 2. *An $[[n,k,d]]_2$ stabilizer code, with $k \geq 1$, can correct all errors in the set $\mathcal{E} = \{M \in \mathcal{P}_n : \mathrm{wt_s}(M) < d/2\}$.*

Proof. For any $E_1, E_2 \in \mathcal{E}$, we have $\mathrm{wt_s}(E_1^\dagger E_2) \leq \mathrm{wt_s}(E_1) + \mathrm{wt_s}(E_2) < d$. Hence, $E_1^\dagger E_2$ cannot be in $C(\mathcal{S}) \setminus \mathcal{S}^\Phi$, and the result follows from Theorem 1. □

The definition given above for the minimum distance of $\mathcal{Q}_{\mathcal{S}}$ cannot be directly extended to the case when $\dim \mathcal{Q}_{\mathcal{S}} = 1$, i.e., when $\mathcal{Q}_{\mathcal{S}}$ carries no logical qubits. Indeed, recall that we have $\dim \mathcal{Q}_{\mathcal{S}} = 1$ if and only if $C(\mathcal{S}) = \mathcal{S}^\Phi$, i.e., $C(\mathcal{S}) \setminus \mathcal{S}^\Phi = \emptyset$. Nonetheless, a somewhat meaningful definition of minimum distance can be given even in this case.

Definition 3. *For a quantum stabilizer code $\mathcal{Q}_{\mathcal{S}}$ with $\dim \mathcal{Q}_{\mathcal{S}} = 1$, associated with the stabilizer group $\mathcal{S}$, the minimum distance is defined as*

$$d_{\min}(\mathcal{Q}_{\mathcal{S}}) \;:=\; \min\bigl\{\mathrm{wt_s}(M) : M \in \mathcal{S}, M \neq I_N\bigr\}.$$

Equivalently, $d_{\min}(\mathcal{Q}_{\mathcal{S}}) \;:=\; \min\bigl\{\mathrm{wt_s}(M) : M \in \mathcal{S}^\Phi, M \neq \pm I_N, \pm i I_N\bigr\}$.

With this again, the set of Pauli operators $\mathcal{E} = \{M \in \mathcal{P}_n : \mathrm{wt_s}(M) < d_{\min}/2\}$ is correctable by $\mathcal{Q}_{\mathcal{S}}$. Indeed, if $E_1, E_2 \in \mathcal{E}$ are such that $E_2 = i^\ell E_1$, then $E_1^\dagger E_2 = \pm i^\ell I_N$. So, for $\left|\varphi\right\rangle, \left|\psi\right\rangle \in \mathcal{Q}_{\mathcal{S}}$, we have $\left\langle\varphi\right| E_1^\dagger E_2 \left|\psi\right\rangle = \pm i^\ell \left\langle\varphi|\psi\right\rangle$. On the other hand, if $E_1, E_2 \in \mathcal{E}$ are not scalar multiples of each other, then $E_1^\dagger E_2$ is not a multiple of I_N, and moreover, $\mathrm{wt_s}(E_1^\dagger E_2) < d$. Thus, $E_1^\dagger E_2 \notin \mathcal{S}^\Phi = C(\mathcal{S})$, which means that $E_1^\dagger E_2$ anti-commutes with some $M' \in \mathcal{S}$. We then have, for any $\left|\varphi\right\rangle, \left|\psi\right\rangle \in \mathcal{Q}_{\mathcal{S}}$,

$$\left\langle\varphi\right| E_1^\dagger E_2 \left|\psi\right\rangle \;=\; \left\langle\varphi\right| E_1^\dagger E_2 \cdot \underbrace{M' \left|\psi\right\rangle}_{=\left|\psi\right\rangle} \;=\; -\left\langle\varphi\right| M' \cdot E_1^\dagger E_2 \left|\psi\right\rangle \;=\; -\left\langle\varphi\right| E_1^\dagger E_2 \left|\psi\right\rangle.$$

Hence, $\left\langle\varphi\right| E_1^\dagger E_2 \left|\psi\right\rangle = 0$. We conclude that for any $E_1, E_2 \in \mathcal{E}$, the Knill-Laflamme condition holds, so that errors in $\mathcal{E}$ are correctable by $\mathcal{Q}_{\mathcal{S}}$.