Proof of LEMMA 4.1 (by Contradiction)

LEMMA 4.1 Given a $[n, k, d]$ stabilizer code C with stabilizer set $S = \{S_1, S_2, ..., S_i, ..., S_{n-k}\}$. Let P be a quantum operator, and $|\psi\rangle$ be the state of the codespace. If the operator P will not change the state of the data qubits, then P must commute with any stabilizer. That's, if $P|\psi\rangle = |\psi\rangle$, then $P \cdot S_i = S_i \cdot P$, for $\forall S_i \in S$.

Proof.
Suppose, for the sake of contradiction, that the statement

$$\text{If } P|\psi\rangle = |\psi\rangle, \text{ then } \exists S_i \in S \text{ such that } P \cdot S_i = -S_i \cdot P$$

is true.

Since $P \cdot S_i$ = $-S_i \cdot P$, we can deduce that

$$P \cdot S_i|\psi\rangle = -S_i \cdot P|\psi\rangle.$$

On the left-hand side, we have $P \cdot S_i|\psi\rangle$ = $|\psi\rangle$, because $S_i \in S$ implies that $S_i|\psi\rangle$ = $|\psi\rangle$, and $P|\psi\rangle$ = $|\psi\rangle$ by assumption.

However, on the right-hand side, we obtain $-|\psi\rangle$.

This leads to a contradiction, as we now have

$$|\psi\rangle = -|\psi\rangle.$$

Therefore, our assumption must be false, and thus **LEMMA 4.1** is proven.

Proof of THEOREM 4.2 (by Contradiction)

THEOREM 4.2 Let $\mathcal{VE}$ be a virtual error, $\mathcal{PE}_1$ be a set of physical errors that $\mathcal{VE} \notin \mathcal{PE}_1$ and $|\mathcal{PE}_1|$ is the maximum correction capacity of QEC code, and $S(\mathcal{VE} \cup \mathcal{PE}_1)$ be the syndrome of errors composed of $\mathcal{VE}$ and $\mathcal{PE}_1$. There exists another set of physical errors $\mathcal{PE}_2$ s.t. $|\mathcal{PE}_2|$ is less than or equal to the maximum correction capacity, such that its syndrome $S(\mathcal{PE}_2)$ is the same as $S(\mathcal{VE} \cup \mathcal{PE}_1)$. As such, based on LEMMA 4.1, we cannot find an operator P that makes $P|\psi\rangle = |\psi\rangle$ and distinguishes errors $\mathcal{VE} \cup \mathcal{PE}_1$ and $\mathcal{PE}_2$.

Proof.

Suppose, for the sake of contradiction, that there exists an operator P such that $P|\psi\rangle = |\psi\rangle$ and that P can distinguish the errors $E_1 = \mathcal{VE} \cup \mathcal{PE}_1$ and $E_2 = \mathcal{PE}_2$, which cannot be distinguished by all original stabilizers $S = \{S_1, S_2, \ldots, S_{n-k}\}$, in the sense that their syndromes for operation P satisfy

$$S(E_1) \neq S(E_2).$$

Because the errors E_1 and E_2 yield the same syndromes with respect to original stabilizers, we have, for every $S_i \in S$,

$$S_i E_1|\psi\rangle = \lambda_S E_1|\psi\rangle \quad \text{and} \quad S_i E_2|\psi\rangle = \lambda_S E_2|\psi\rangle,$$

where $\lambda_S \in \{+1, -1\}$, and $|\psi\rangle$ is an invalid state in the codespace.

If the operator P can distinguish between E_1 and E_2, it must act with opposite eigenvalues on the two erroneous states, i.e.,

$$PE_1|\psi\rangle = \lambda_P E_1|\psi\rangle \quad \text{and} \quad PE_2|\psi\rangle = -\lambda_P E_2|\psi\rangle,$$

where $\lambda_P \in \{+1, -1\}$.

Now, consider the quantity $\langle\psi|E_2 P S_i E_1|\psi\rangle$. On the one hand, using the assumptions on S_i and P, we have

$$\begin{aligned}
\langle\psi|E_2 P S_i E_1|\psi\rangle &= \langle\psi|E_2(-\lambda_P) S_i E_1|\psi\rangle \quad (\text{since } PE_2|\psi\rangle = -\lambda_P E_2|\psi\rangle) \\
&= \langle\psi|E_2(-\lambda_P)\lambda_S E_1|\psi\rangle \quad (\text{since } S_i E_1|\psi\rangle = \lambda_S E_1|\psi\rangle) \\
&= -\lambda_P \lambda_S \langle\psi|E_2 E_1|\psi\rangle.
\end{aligned}$$

On the other hand, since by Lemma 4.1 the operator P commutes with every stabilizer generator S_i (i.e., $P \cdot S_i = S_i \cdot P$ for all $S_i \in S$), we also have

$$\begin{aligned}
\langle\psi|E_2 P S_i E_1|\psi\rangle &= \langle\psi|E_2 S_i P E_1|\psi\rangle \\
&= \langle\psi|E_2 S_i \lambda_P E_1|\psi\rangle \quad (\text{since } PE_1|\psi\rangle = \lambda_P E_1|\psi\rangle) \\
&= \langle\psi|E_2 \lambda_S \lambda_P E_1|\psi\rangle \quad (\text{since } S_i E_2|\psi\rangle = \lambda_S E_2|\psi\rangle) \\
&= \lambda_P \lambda_S \langle\psi|E_2 E_1|\psi\rangle.
\end{aligned}$$

Comparing the two expressions, we find

$$-\lambda_P \lambda_S \langle\psi|E_2 E_1|\psi\rangle = \lambda_P \lambda_S \langle\psi|E_2 E_1|\psi\rangle.$$

Assuming $\langle\psi|E_2E_1|\psi\rangle \neq 0$ (which can always be arranged by choosing a suitable $|\psi\rangle$), it follows that

$$-\lambda_P\lambda_S = \lambda_P\lambda_S,$$

which implies

$$2\lambda_P\lambda_S = 0.$$

However, since $\lambda_P, \lambda_S \in \{+1, -1\}$, their product $\lambda_P\lambda_S$ is also either $+1$ or -1, so this equality is impossible.

Thus, we arrive at a contradiction. Therefore, our initial assumption must be false, and no such operator P can exist. This completes the proof of **THEOREM 4.2**.