Quantum Error Correcting Code

Scribe: Raymond Liu

December 4, 2025

1 Quantum Error Correcting Code

We start by presenting a quantum code that can detect 1 bit flip, followed by a code that can correct 1 bit flip, then Shor's code, which can correct either 1 bit flip or 1 phase flip. We also introduce the definition of CSS code and hypergraph product code.

1.1 Detecting 1 Bit Flip

Let $C = span\{|00\rangle, |11\rangle\}$ be the code space. Let E be the error operator where $E \in \{X_1, X_2\}$ (one bit flip) or $E \in \{I, X_1X_2\}$ (no error or two bit flips). For any codeword $|\psi\rangle$, the received word is $E|\psi\rangle$. Observe that $EC = span\{|01\rangle, |10\rangle\}$ is an orthogonal space to C. This allows us to use a measure to distinguish between the two spaces.

Since Z_1Z_2 is a unitary matrix, there exists a unitary operator as follow:

$$E|\psi\rangle|0\rangle \mapsto \frac{I_1I_2 + Z_1Z_2}{2}E|\psi\rangle|0\rangle + \frac{I_1I_2 - Z_1Z_2}{2}E|\psi\rangle|1\rangle$$

If $E \in \{X_1, X_2\}$, then the above measurement yields ancilla $|1\rangle$. If $E \in \{I, X_1X_2\}$, then it yields ancilla $|0\rangle$. Hence, we can detect 1 bit flip with this code.

1.2 Correcting 1 Bit Flip

Though the code above is capable of detecting 1 bit flip, it cannot find out which bit flip has occurred exactly. To be able to correct 1 bit flip, we require one more bit of redundancy,

Let $C = span\{|000\rangle, |111\rangle\}$ be the code space. We show that we can correct from $X_1|\psi\rangle, X_2|\psi\rangle$, or $X_3|\psi\rangle$. Let $M_1 = Z_1Z_2$, and let $M_2 = Z_2Z_3$. Observe that for $|\psi\rangle \in C$,

$$M_1|\psi\rangle = |\psi\rangle \quad \text{and} \quad M_2|\psi\rangle = |\psi\rangle$$

and for any $E \in \{X_1, X_2\}$,

$$M_1(E|\psi\rangle) = -E|\psi\rangle$$

for any $E \in \{X_2, X_3\}$,

$$M_2(E|\psi\rangle) = -E|\psi\rangle$$

Hence, if we consider the unitary operators

$$E|\psi\rangle|0\rangle \mapsto \frac{I+M_1}{2}E|\psi\rangle|0\rangle + \frac{I-M_1}{2}E|\psi\rangle|1\rangle \tag{1.1}$$

$$E|\psi\rangle|0\rangle \mapsto \frac{I+M_2}{2}E|\psi\rangle|0\rangle + \frac{I-M_2}{2}E|\psi\rangle|1\rangle \tag{1.2}$$

if $E \in \{X_1, X_2\}$, the first measurement (1.1) gives ancilla 1, and otherwise 0. The second measurement (1.2) gives ancilla 1 if $E \in \{X_2, X_3\}$, and otherwise 0. Using the two measurements, we can thus distinguish what E is, and apply $EE|\psi\rangle = |\psi\rangle$ to recover the original codeword.

1.3 Shor's Code

The above code can correct from 1 bit flip, but not for a phase flip. We now show a code that can correct from both 1 bit flip and 1 phase flip.

Let $C_{shor} = span\{|0\rangle_{shor}, |1\rangle_{shor}\}$, where

$$|0\rangle_{shor} = \left(\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle\right)^{\otimes 3} \quad \text{and} \quad |1\rangle_{shor} = \left(\frac{1}{\sqrt{2}}|000\rangle - \frac{1}{\sqrt{2}}|111\rangle\right)^{\otimes 3}$$

Let $\mathcal{P} = \{Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9, X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9\}$ be the set of stabilizers. I.e. for any $|\psi\rangle \in C$, $P_i|\psi\rangle = |\psi\rangle$ for any $P_i \in \mathcal{P}$. The code C can be equivalently written as $C_{shor} = \{|\psi\rangle \mid P_i|\psi\rangle = |\psi\rangle, \forall P_i \in \mathcal{P}\}$.

Let E be the possible error, where $E \in \{X_1, \cdots, X_9, Z_1, \cdots, Z_9\}$, or $E = I$ (no error). There exists a measurement correspobding to each P_i:

$$E|\psi\rangle|0\rangle \mapsto \frac{I+P_i}{2}E|\psi\rangle|0\rangle + \frac{I-P_i}{2}E|\psi\rangle|1\rangle$$

For each error E, measuring $E|\psi\rangle$ with all the P_i's allows us to recover the codeword. The following is the outcomes table corresponding to each error.

	P1	P2	P3	P4	P5	P6	P7	P8
X1	1	0	0	0	0	0	0	0
X2	1	1	0	0	0	0	0	0
X3	0	1	0	0	0	0	0	0
X4	0	0	1	0	0	0	0	0
X5	0	0	1	1	0	0	0	0
X6	0	0	0	1	0	0	0	0
X7	0	0	0	0	1	0	0	0
X8	0	0	0	0	1	1	0	0
X9	0	0	0	0	0	1	0	0

	P1	P2	P3	P4	P5	P6	P7	P8
Z1	0	0	0	0	0	0	1	0
Z2	0	0	0	0	0	0	1	0
Z3	0	0	0	0	0	0	1	0
Z4	0	0	0	0	0	0	1	1
Z5	0	0	0	0	0	0	1	1
Z6	0	0	0	0	0	0	1	1
Z7	0	0	0	0	0	0	0	1
Z8	0	0	0	0	0	0	0	1
Z9	0	0	0	0	0	0	0	1

For $E \in \{X_1, \cdots, X_9\}$, the outcome uniquely identifies the error and thus we can correct it. For $E \in \{Z_1, \cdots, Z_9\}$, we can only distinguish between the three *groups* of errors $\{Z_1, Z_2, Z_3\}$, $\{Z_4, Z_5, Z_6\}$, and $\{Z_7, Z_8, Z_9\}$. However, applying any Z_i from the same group suffices to correct the error.

1.4 Stabilizer Code

The construction of Shor's code can be generalized to define codes based on different set of stabilizers.

Definition 1.1 (Pauli Group)**.** *The Pauli group is generated by the operators* $\{X_i\}_{i\in[n]}, \{Y_j\}_{j\in[n]}, \{Z_k\}_{k\in[n]}$, *where* $Y_j = iX_jZ_j$.

Definition 1.2 (Stabilizer Code)**.** *Let G be an abelian subgroup of the Pauli group, and let $P_1, \cdots, P_m$ be the generator of G. The stabilizer code is defined as*

$$C = \{|\psi\rangle \in (\mathbb{C}^2)^n \mid P_i|\psi\rangle = |\psi\rangle\ \forall i \in [m]\}$$

As long as we can show that all the error pattern gives different syndromes, or are equivalent up to degeneracy, the code can correct the given errors.

1.5 CSS Code (Calderbank-Shor-Steane Code) & Hypergraph Product Codes

We state the definition of CSS code and hypergraph product codes here.

Definition 1.3 (CSS Code)**.** *Let C_1, C_2 be $[n, k_1], [n, k_2]$ classical binary linear code, respectively, where $C_2 \subseteq C_1$. Let $\widetilde{G}$ be a $(k_1 - k_2) \times n$ matrix that generates a set of coset representatives for C_2 inside C_1. A CSS quantum error-correcting code is the subspace C spanned by the basis element $|u\rangle_L$ for $u \in \{0,1\}^{k_1-k_2}$ where*

$$|u\rangle_L = \frac{1}{\sqrt{|C_2|}} \sum_{y\in C_2} |u\widetilde{G} + y\rangle$$

Definition 1.4 (Hypergraph Product Code)**.** *Let* H_1, H_2 *be the parity checks of* $[n_1, k_1, d_1]$, $[n_2, k_2, d_2]$ *codes. The resulting hypergraph product code is a CSS code with*

$$H_X = \begin{bmatrix} H_1 \otimes I_{n_2} & I_{m_1} \otimes H_2^T \end{bmatrix} \quad \text{and} \quad H_Z = \begin{bmatrix} I_{n_1} \otimes H_2 & H_1^T \otimes I_{m_2} \end{bmatrix}$$

where one can verify that $H_X H_Z^T = 0$.