1 Classical Linear Code (contd.)

Definition 1 *Let $\vec{g}$ and $\vec{e}$ be any codeword and error respectively. The syndrome $\vec{s}$ of $\vec{e}$ is defined to be*

$$\vec{s} = H(\vec{e}) = H(\vec{g} \oplus \vec{e})$$

Note that the syndrome of $\vec{e}$ is independent of the encoded data g, a useful property in the quantum setting. For any $\vec{e}_1$, $\vec{e}_2$ with syndromes $\vec{s}_1$, $\vec{s}_2$, we have

$$\begin{aligned}(\vec{s}_1 = \vec{s}_2) &\iff H(\vec{e}_1) = H(\vec{e}_2) \\ &\iff H(\vec{e}_1 - \vec{e}_2) = 0 \\ &\iff D(\vec{e}_1, \vec{e}_2) \geq d\end{aligned}$$

where $D(\vec{e}_1, \vec{e}_2)$ is the Hamming distance between the two errors. In particular, each element in the set of errors $\{\vec{e}_i\}$ can be corrected as long as $\forall i$

$$\text{wt}(\vec{e}_i) = D(\vec{e}_i, 0) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$$

Example 2 *Consider the $[7,4,3]$ code. Let $\vec{e}_0 = 0$ and $\vec{e}_i$ be all zeroes except at the i^{th} entry. Then*

$$H(\vec{e}_i) = \textit{the } i^{th} \textit{ column of} H$$

In other words, the 3-bit syndrome encodes "which bit has an error" in base 2. The Hamming code above can be generalized to have parameters $[2^r, 2^r - 1 - r, 3]$, and the decoding property holds for all of them.

2 CSS (Calderbank-Shor-Steane) Codes

Consider two linear codes $C_B = [n, k_B, d_B]$ and $C_P = [n, k_P, d_P]$. Then, we may derive codes to correct for quantum bit flip and phase flip errors by doing the following

1. Generate M_Z from H_B by replacing 0 with I and 1 with Z.
2. Generate M_X from H_P by replacing 0 with I and 1 with X.

The rows (tensor product of Pauli matrices) are now called parity check stabilizers S_i with the property that $\forall i$

$$S_i \left|\psi\right\rangle_L = \left|\psi\right\rangle_L$$

In addition, for the stabilizer generators to commute, we require

$$\begin{aligned}C_P^{\perp} \leq C_B &\iff C_B^{\perp} \leq C_P \\ &\iff H_P G_B^T = 0 \\ &\iff H_B G_P^T = 0.\end{aligned}$$

Example 3 *7-bit Steane Code. Both C_P and C_B are taken to be the $[7,4,3]$ Hamming code.*

$$M_Z = \begin{pmatrix} Z & Z & Z & I & Z & I & I \\ Z & Z & I & Z & I & Z & I \\ Z & I & Z & Z & I & I & Z \end{pmatrix}$$

$$M_X \begin{pmatrix} X & X & X & I & X & I & I \\ X & X & I & X & I & X & I \\ X & I & X & X & I & I & X \end{pmatrix}$$

3 Explicit codewords

Let X_i, Z_i be the rows of M_X, M_Z.
Note that

1. For all $|\psi\rangle$ we have

$$\prod_i (I + X_i) \prod_j (I + Z_j) |\psi\rangle \in C$$

2. Let $l \in C_B$, then

$$\prod_j \left(\frac{I + Z_j}{2}\right) |l\rangle = |l\rangle$$

In order to obtain an explicit characterization of the codewords, we have

$$\begin{aligned} |l\rangle_L &= \frac{1}{\sqrt{2^{n-k+p}}} \prod_i (I + X_i) \prod_j \left(\frac{I + Z_j}{2}\right) |l\rangle \\ &= \frac{1}{\sqrt{2^{n-k+p}}} \prod_i (I + X_i) |l\rangle \\ &= \frac{1}{|C_p^{\perp}|} \sum_{w \in C_p^{\perp}} |l + w\rangle \end{aligned}$$

So, there are $\frac{2^{k_B}}{2^{n-k_P}}$ orthogonal $|l\rangle_L$. That gives the correct number of basis states for the stabilizers.
As an example, we obtain the following description for the logical encoding of the 7-bit Steane code

$$\begin{aligned} |0\rangle_l = \ & \tfrac{1}{\sqrt{8}} \ (|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ & + \ \ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle) \end{aligned}$$

$$\begin{aligned} |1\rangle_l = \ & \tfrac{1}{\sqrt{8}} \ (|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ & + \ \ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle) \end{aligned}$$