10.4 Seven-Qubit QECC

- In classical coding theory, encoding x as xxx has a redundancy 2.
- In general, using n-bit code words c for k-bit messages m has a redundancy $n-k$.
- In Hamming code on $\mathbb{Z}_2^n$, one use an $n \times (n-k)$ parity check matrix H to detect error such that $Hc' = 0$ if and only if there is no error.
- Moreover, Hc' will be the syndrome, and used for the correction.
- The set of code words has size 2^k.

Alice sent $\begin{bmatrix} c_1 \\ c_n \end{bmatrix}$

& Bob received $\begin{bmatrix} \hat{c}_1 \\ \hat{c}_n \end{bmatrix}$, Apply $\begin{bmatrix} & n \\ n-k & \end{bmatrix} \begin{bmatrix} \hat{c}_1 \\ \hat{c}_n \end{bmatrix} = 0$ Good.

Bob assume $\begin{bmatrix} \hat{c}_1 \\ \hat{c}_n \end{bmatrix} = \begin{bmatrix} c_1 \\ c_n \end{bmatrix}$ that Alice sent.

& $H\begin{bmatrix} \hat{c}_1 \\ \hat{c}_n \end{bmatrix} \neq 0$, then Bob assume that something is wrong & use this Hc' vector to help do correction

Example Let $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ so that $Hc^t = \begin{pmatrix} x_4 \oplus x_5 \oplus x_6 \oplus x_7 \\ x_2 \oplus x_3 \oplus x_6 \oplus x_7 \\ x_1 \oplus x_3 \oplus x_5 \oplus x_7 \end{pmatrix} \in \mathbb{Z}_2^3$

Suppose $(x_1 \cdots x_7)$ was sent and $\tilde{x}_1 \cdots \tilde{x}_7)$ is received. Assume there is a single error. Then ...

- The set of codewords $\mathbf{C} = \{c = (c_1, \ldots, c_7) : Hc^t = 0 \in \mathbb{Z}^3\}$ has 2^4 elements.
- So, c is a linear combination of the rows of a matrix M with row space equal to $\mathbf{C}$, i.e., kernel of H^t.
- Let $M = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} H \\ 1_{1\times 7} \end{pmatrix}$. Then

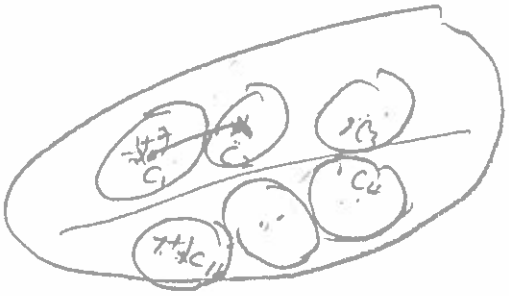
$$\mathbf{C} = \{(0000)M, \ldots, (1111)M\} = \{(0000000), \ldots, (0010110)\}.$$

- Note that the eight elements in $\mathbf{C}$ with even number of ones are

$$\{(0000000), (1010101), (0110011), (1100110), (0001111), (1011010), (0111100), (1101001)\},$$

which equals $\mathbf{C}^\perp$ and is generated by $(i_1 i_2 i_3 0)M$.

- The Hamming distance between two code words $x, y \in \mathbf{C}$ is the number of nonzero entries in $x - y = x + y$.
- An (n, k, d) code is a code with n-bit codewords, k-bit messages, and minimum Hamming distance between code words d.
- It can correct $(d-1)/2$ errors.
- In particular, to correct single error, we need $d \geq 3$.
- For Hamming codes, $d \leq n - k$.
- The geometry of the $\mathbf{C}$ in $\mathbb{Z}_2^7$:



$d(c_i, c_j)$

$= d(c_i - c_i, c_j - c_i)$

$= d(0, c)$

$2^4 = 16$ messages can be sent.

Image of a linear transformation $M: \mathbb{Z}_2^4 \to \mathbb{Z}_2^7$

$8 \to$ 1 code words

$8 \times 16 = 8 \times 16$ possible $2^3 \cdot 2^4$ words in $\mathbb{Z}_2^7$

$|\psi\rangle = |q_0 \cdots q_6\rangle \in (\mathbb{C}^2)^{\otimes 7}$

Seven-Qubits QECC

Inspired by the Hamming code, one can consider the Seven-Qubit QECC.

$X_0 = X \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$
$X_1 = I X I \cdots I$
$X_2 = I I X I \cdots I$
$X_6 = I \cdots I X$

Encoding

$\mathbb{Z}_2^7$

- Let $M_0 = X_4X_3X_2X_1$, $M_1 = X_5X_3X_2X_0$, $M_2 = X_6X_3X_1X_0$,

$|0\rangle_L = \frac{1}{\sqrt{8}}(I + M_0)(I + M_1)(I + M_2)|0\rangle^{\otimes 7}$

$= \frac{1}{\sqrt{8}}(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle)$,

and $|1\rangle_L = \frac{1}{\sqrt{8}}(I + M_0)(I + M_1)(I + M_2)|1\rangle^{\otimes 7}$

$= \frac{1}{\sqrt{8}}(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle)$.

- Let $\tilde{X} = X^{\otimes 7}$, $\tilde{Z} = Z^{\otimes 7}$, $N_0 = Z_4Z_3Z_2Z_1$, $N_1 = Z_5Z_3Z_2Z_0$, $N_2 = Z_6Z_3Z_1Z_0$.
- Then there are nice commuting and anti-commuting relationships on $\tilde{X}, \tilde{Z}, M_i, N_i$, etc.
- In particular, $M_i|x\rangle_L = N_i|x\rangle_L = |x\rangle_L$. Check $|x\rangle_L = |0\rangle_L, |1\rangle_L$.

$a|0\rangle + b|1\rangle \to a|0\rangle_L + b|1\rangle_L$.

Decoding

- Suppose $|\Psi\rangle = a|0\rangle_L + b|\rangle_L$ is send and $|\tilde{\Psi}\rangle$ is received.
- Use 6 ancillas, to get $M_i|\tilde{\Psi}\rangle = \mu_i|\tilde{\Psi}\rangle$ and $N_i|\tilde{\Psi}\rangle = \nu_i|\tilde{\Psi}\rangle$ with $\mu_i, \nu_i \in \{1, -1\}$.
- Assume that there is only one error of the X, Y, Z type on one of the 7 qubits, we can determine what error using $(\mu_1, \mu_2, \mu_3, \nu_1, \nu_2, \nu_3)$.
- We may then apply the correction.

See encoding / decoding circuits in the textbook.