Quantum Error Correction

Michele Pacenti
OPTI646

The [3,1,3] repetition code

$$[n, k, d]$$

Codelength

Code dimension

Minimum (Hamming) distance

$$R = \frac{k}{n}$$

Rate

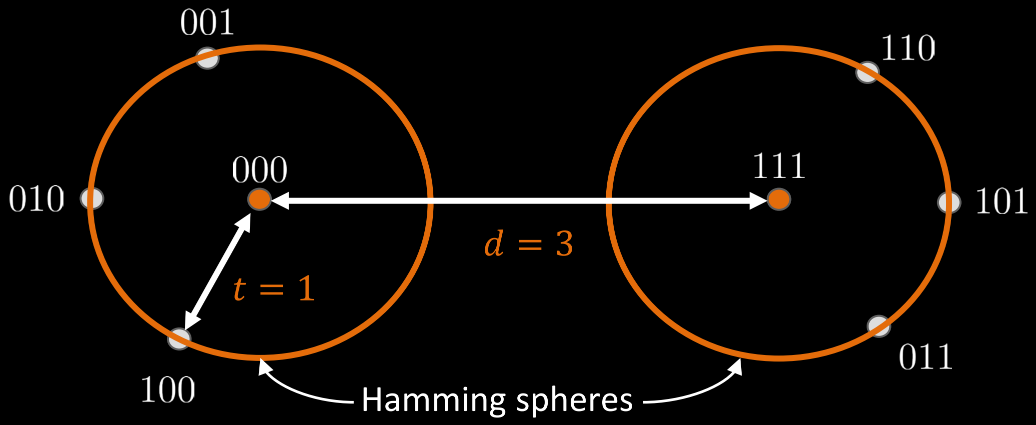
Hamming distance = the number of positions in which two binary vectors differ

$$0 \rightarrow 000$$
$$1 \rightarrow 111$$

Codewords

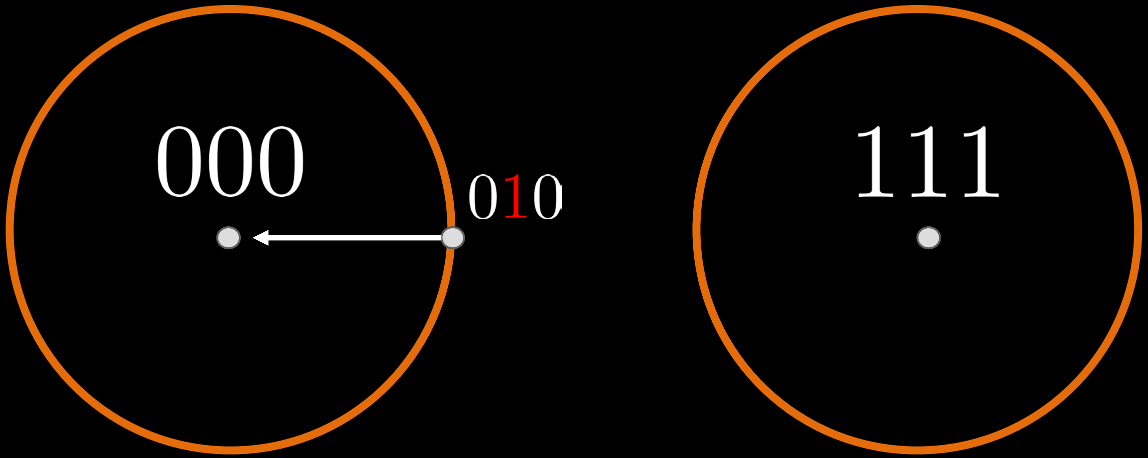
$$t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

Correctable errors



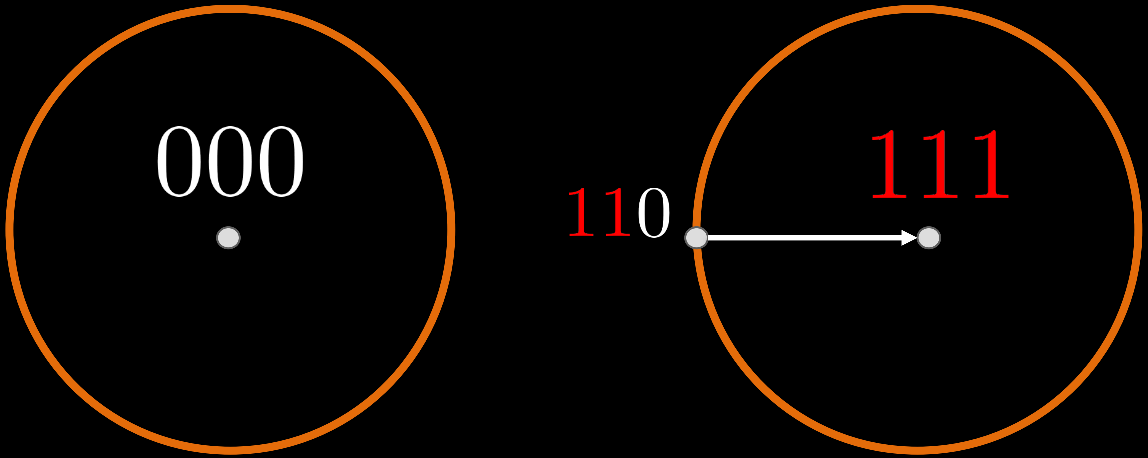
Maximum likelihood decoding on the repetition code

$$\begin{array}{ccccc} \mathbf{x} & & \mathbf{y} & & \hat{\mathbf{x}} \\ 000 & \xrightarrow{\text{BSC}} & 010 & \xrightarrow{\text{Decoder}} & 000 \end{array}$$



Decoding failure

$$\overset{\mathbf{x}}{000} \xrightarrow{\text{BSC}} \overset{\mathbf{y}}{110} \xrightarrow{\text{Decoder}} \overset{\hat{\mathbf{x}}}{111}$$



Codes as matrices

- Let $\mathbf{u}$ be a binary vector of length k
- Let $\mathbf{G}$ be the generator matrix of the code $\mathcal{C}$
- A codeword can be defined as $\mathbf{x} = \mathbf{u} \cdot \mathbf{G}$

$$\begin{cases} \mathbf{x} \in \mathrm{Im}\{\mathbf{G}\} \\ \mathbf{x} \in \ker\{\mathbf{H}\} \end{cases}$$

- Let $\mathbf{H}$ be the parity check matrix of the code $\mathcal{C}$
- If and only if $\mathbf{x} \cdot \mathbf{H}^T = \mathbf{0}$ then $\mathbf{x}$ is a codeword

$$\mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}$$

Matrices of the [3,1,3] rep. code

$$\mathbf{u} \in \{0, 1\}$$

$$\begin{cases} 0 \cdot \mathbf{G} = 000 \\ 1 \cdot \mathbf{G} = 111 \end{cases} \longrightarrow \mathbf{G} = \underbrace{\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}}_{n} \}k$$

$$\mathbf{H} = \underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}}_{n} \Bigg\} n-k$$

$$111 \cdot \mathbf{H}^T = \begin{pmatrix} 1+1+0 \\ 0+1+1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Error syndrome

- Assume we transmit a codeword $\mathbf{x}$ over a BSC
- The effect of the channel can be modeled as adding an error vector $\mathbf{e}$ to the codeword

- Received sequence $\mathbf{y} = \mathbf{x} + \mathbf{e}$

- Syndrome $\mathbf{s} = \mathbf{y} \cdot \mathbf{H}^T$

$$\mathbf{s} = (\mathbf{x} + \mathbf{e}) \cdot \mathbf{H}^T$$

$$\mathbf{s} = \cancel{\mathbf{x} \cdot \mathbf{H}^T} + \mathbf{e} \cdot \mathbf{H}^T$$

$$\mathbf{s} = \mathbf{e} \cdot \mathbf{H}^T$$

[3,2,2] Single Parity Check code

[3,1,3] Repetition code

$$\mathbf{G}_R = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

$$\mathbf{H}_R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

[3,2,2] Single Parity Check code

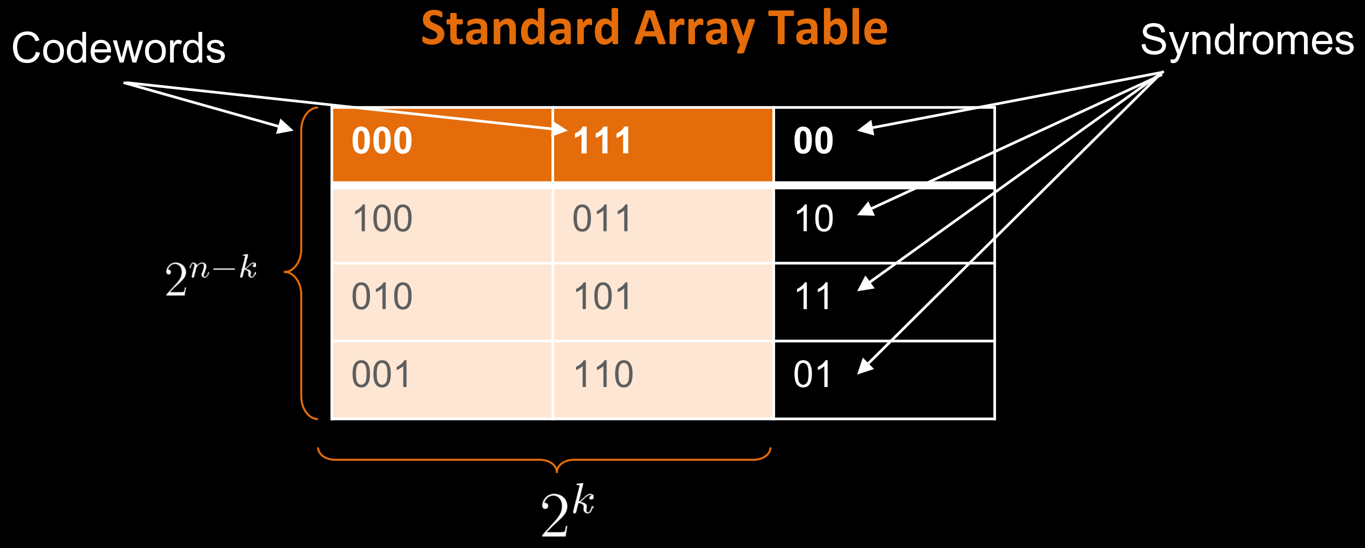
$$\mathbf{G}_S = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$$\mathbf{H}_S = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

$\mathbf{H}_R \cdot \mathbf{H}_S^T = \mathbf{0}$ Dual codes $\mathcal{C},\ \mathcal{C}^{\perp}$

Example

$$\begin{matrix}\mathbf{x}=000\\ \mathbf{e}=100\end{matrix} \longrightarrow \mathbf{y}=100 \longrightarrow \mathbf{s}=100\cdot\mathbf{H}^T=\begin{pmatrix}1\\0\end{pmatrix}$$



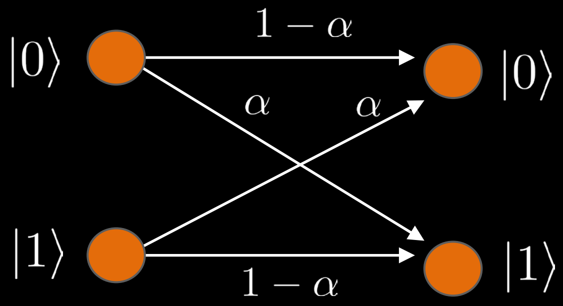
Standard Array Table

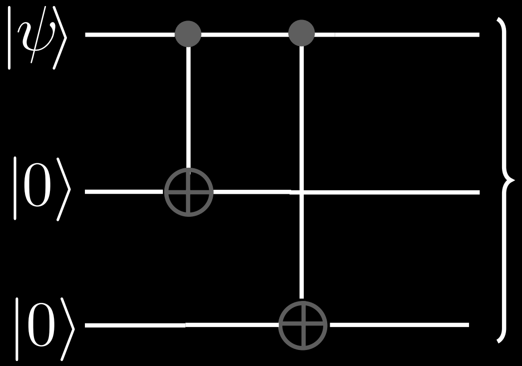
000	**111**	**00**
100	011	10
010	101	11
001	110	01

QEC: differences with classical

- No cloning
- Continuous errors
- State collapses after measurement

Three qubit bit flip repetition code





$$|\Psi\rangle = a\,|000\rangle + b\,|111\rangle$$

$$\begin{cases} X\,|0\rangle = |1\rangle \\ X\,|1\rangle = |0\rangle \end{cases}$$

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

Error detection

- 4 projection operators:

$$P_0 = |000\rangle \langle 000| + |111\rangle \langle 111| \longrightarrow \text{No flip}$$

$$P_1 = |100\rangle \langle 100| + |011\rangle \langle 011| \longrightarrow \text{1st qubit flip}$$

$$P_2 = |010\rangle \langle 010| + |101\rangle \langle 101| \longrightarrow \text{2nd qubit flip}$$

$$P_3 = |001\rangle \langle 001| + |110\rangle \langle 110| \longrightarrow \text{3rd qubit flip}$$

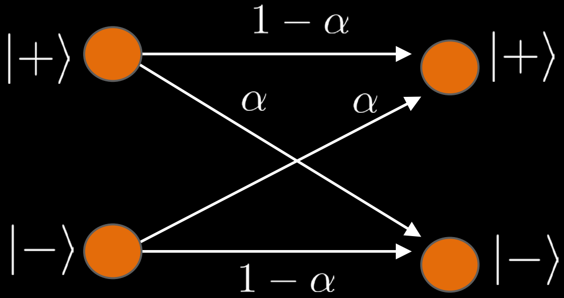
$$\mathbf{s} = \begin{cases} \langle\Psi| P_0 |\Psi\rangle \\ \langle\Psi| P_1 |\Psi\rangle \\ \langle\Psi| P_2 |\Psi\rangle \\ \langle\Psi| P_3 |\Psi\rangle \end{cases}$$

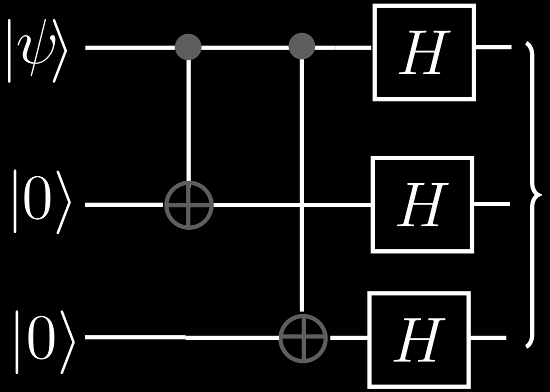
$$|\Psi\rangle = a\,|100\rangle + b\,|011\rangle \longrightarrow \langle\Psi| P_1 |\Psi\rangle = 1$$

$$|\Psi\rangle = a\,|100\rangle + b\,|011\rangle \longrightarrow \langle\Psi| P_0 |\Psi\rangle = 0$$

Syndrome

Three qubit phase flip repetition code





$$|\Psi\rangle = a\,|+++\rangle + b\,|---\rangle$$

$$\begin{cases} Z\,|0\rangle = |0\rangle \\ Z\,|1\rangle = -\,|1\rangle \end{cases}$$

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

Error detection

- 4 projection operators:

$P_0 = |+++\rangle \langle +++| + |---\rangle \langle ---| \longrightarrow$ No flip

$P_1 = |-++\rangle \langle -++| + |+--\rangle \langle +--| \longrightarrow$ 1st qubit flip

$P_2 = |+-+\rangle \langle +-+| + |-+-\rangle \langle -+-| \longrightarrow$ 2nd qubit flip

$P_3 = |++-\rangle \langle ++-| + |--+\rangle \langle --+| \longrightarrow$ 3rd qubit flip

$|\Psi\rangle = a\,|-++\rangle + b\,|+--\rangle \longrightarrow \langle\Psi| P_1 |\Psi\rangle = 1$

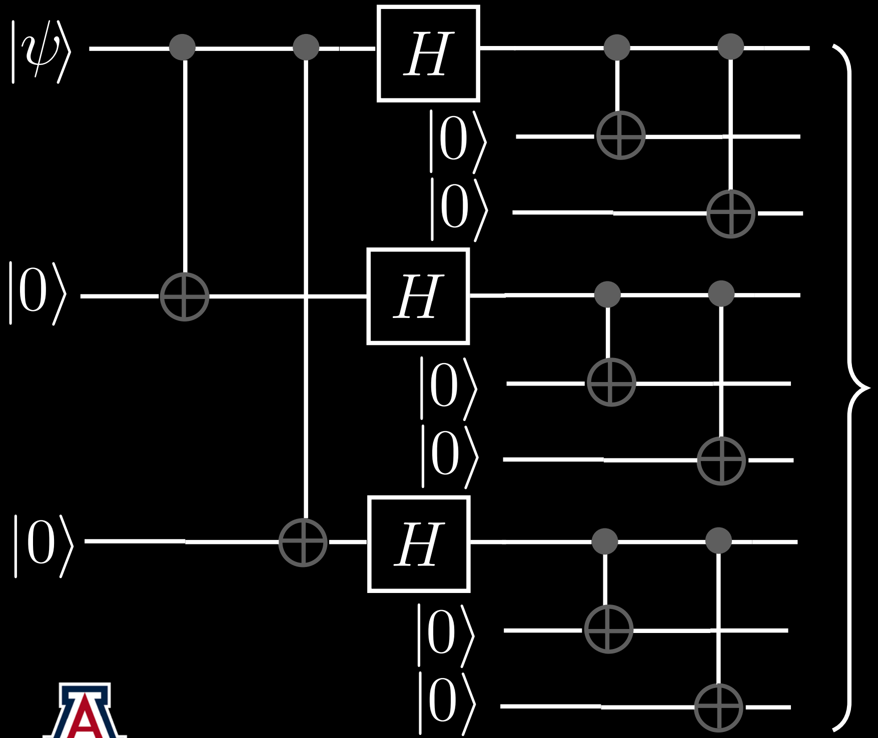
$\longrightarrow \langle\Psi| P_0 |\Psi\rangle = 0$

$$\mathbf{s} = \begin{cases} \langle\Psi| P_0 |\Psi\rangle \\ \langle\Psi| P_1 |\Psi\rangle \\ \langle\Psi| P_2 |\Psi\rangle \\ \langle\Psi| P_3 |\Psi\rangle \end{cases}$$

$\uparrow$

Syndrome

Concatenating two repetition codes: the [[9,1,3]] Shor code



$$|\Psi\rangle = \begin{array}{c} a(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)+ \\ b(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle) \end{array}$$

Depolarizing channel

$$|\Psi\rangle$$

$$E_i = e_{i0}I + e_{i1}X + e_{i2}Z + e_{i3}Y$$

$$\mathcal{E}$$

$$\mathcal{E}(|\Psi\rangle\langle\Psi|) = \sum_i E_i |\Psi\rangle\langle\Psi| E_i^\dagger$$

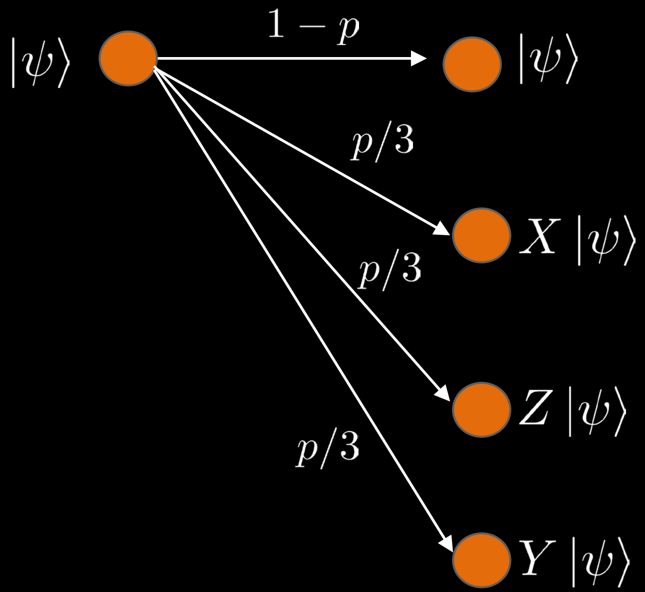
$$E_i|\Psi\rangle = e_{i0}|\Psi\rangle + e_{i1}X_i|\Psi\rangle + e_{i2}Z_i|\Psi\rangle + e_{i3}Y_i|\Psi\rangle$$

Measuring the syndrome makes the state collapse into one of the states

It’s sufficient to deal with discrete errors

Depolarizing channel

$$\mathcal{E}(\rho) = (1-p)\rho + \tfrac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$$



Stabilizer formalism

$$S\,|\psi\rangle = |\psi\rangle$$

$\uparrow$

Stabilizer

E.g. $|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

$$X_1 X_2\,|\psi\rangle = |\psi\rangle$$

$$Z_1 Z_2\,|\psi\rangle = |\psi\rangle$$

$$S = \langle X_1 X_2, Z_1 Z_2 \rangle$$

$$= \begin{pmatrix} X & X \\ Z & Z \end{pmatrix}$$

- The elements of S must commute
  - $-I$ is not in S

Stabilizers of the Shor code

$$S = \begin{pmatrix} Z_1 & Z_2 & I & I & I & I & I & I & I \\ I & Z_2 & Z_3 & I & I & I & I & I & I \\ I & I & I & Z_4 & Z_5 & I & I & I & I \\ I & I & I & I & Z_5 & Z_6 & I & I & I \\ I & I & I & I & I & I & Z_7 & Z_8 & I \\ I & I & I & I & I & I & I & Z_8 & Z_9 \\ X_1 & X_2 & X_3 & X_4 & X_5 & X_6 & I & I & I \\ I & I & I & X_4 & X_5 & X_6 & X_7 & X_8 & X_9 \end{pmatrix}$$

Binary representation

$I \rightarrow (0|0)$

$X \rightarrow (1|0)$

$Z \rightarrow (0|1)$

$Y \rightarrow (1|1)$

$ZZIIIIIII \rightarrow (000000000|110000000)$

$XXXXXXIII \rightarrow (111111000|000000000)$

$\mathbf{s} \in \{-1, +1\} \rightarrow \{0, 1\}$

$$S = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Binary representation

$$I \to (0|0)$$

$$X \to (1|0)$$

$$Z \to (0|1)$$

$$Y \to (1|1)$$

$$ZZIIIIIII \to (000000000|110000000)$$

$$XXXXXXIII \to (111111000|000000000)$$

$$\mathbf{s} \in \{-1,+1\} \to \{0,1\}$$

$$S = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Calderbank-Shor-Steane codes

$\mathcal{C}_1 \rightarrow [n, k_1]$ classical code

$\mathcal{C}_2 \rightarrow [n, k_2]$ classical code

$$\mathcal{C}_2 \subseteq \mathcal{C}_1$$

$$d_1, d_2^{\perp} \geq 2t + 1$$

Minimum distance of $\mathcal{C}_2^{\perp}$

$$CSS(\mathcal{C}_1, \mathcal{C}_2) \rightarrow [[n, k_1 - k_2]]$$

$$x \in \mathcal{C}_1$$

$$|x \oplus \mathcal{C}_2\rangle := \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |x \oplus y\rangle$$

Z stabilizers

$$\mathbf{S} = \begin{pmatrix} \mathbf{0}_{(n-k_1)\times n} & \mathbf{H}_1 \\ \mathbf{H}_2 & \mathbf{0}_{(n-k_2)\times n} \end{pmatrix}$$

X stabilizers

The [[7,1,3]] Steane code

$\mathcal{C}_1 \rightarrow [7,4,3]$ Hamming code

$$\mathbf{H}_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$\mathcal{C}_2 \rightarrow [7,3,4]$ Simplex code

$$\mathbf{H}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\mathbf{H}_1 \cdot \mathbf{H}_2^T = \mathbf{0} \mod 2$$

$$\mathbf{S} = \begin{pmatrix} \mathbf{0}_{(n-k_1)\times n} & \mathbf{H}_1 \\ \mathbf{H}_2 & \mathbf{0}_{(n-k_2)\times n} \end{pmatrix}$$

Quantum LDPC codes

- LDPC – Low Density Parity Check – codes, are codes with a sparse parity check matrix
- These codes are state of art for classical communications and storage
- Sparse stabilizer matrices would allow constant depth of syndrome measurement circuits
- Surface codes are a class of CSS QLDPC codes (stabilizer weight of 4)
- In 2022 asymptotically good QLDPC codes were discovered

Open problems

- Design of practical QLDPC codes
- Design of efficient decoding algorithms
- Hardware implementation of non-topological codes
- Need of more refined error models
- And more…