Quantum error correction

- General ideas, repetition code & Shor code
- Threshold theorem (without proof)
- Classical error correction
  - Hamming distance
  - Parity check matrix
- CSS codes

Errors in a quantum computation are unavoidable due to

- contact with environment leading to entanglement between quantum state and environment. Tracing over the environment causes **decoherence**.

- unitary gate set is continuous, so gate **errors** can be **arbitrarily small**: $U = U_{ideal}(1 + O(\varepsilon))$.

Quantum error correction codes (QECC) aim to protect quantum information provided by state $|\psi\rangle$ by encoding the message, adding some redundant information.

Classical error correction works the same and the simplest example is the (classical) **repetition code**:

$0 \longrightarrow (000)$ ← codewords of code C

$1 \longrightarrow (111)$ ← codewords of code C

Encode a single bit $k=1$ into three bits $n=3$.

If a single bit flip occurs, e.g., $(000) \mapsto (100)$ and $(111) \longmapsto (011)$, we can recover the original information and decode the bit correctly by **majority voting**: $(100) \xmapsto{\text{decoding}} (000)$, $(011) \longmapsto (111)$.

This fails if two or three bits flip and a logical error occurs. Which errors can be corrected is described by the **distance** of the code

$$d = \min_{x,y \in C} D_H(x,y).$$

Hamming distance

$D_H = |x - y|$ = number of components that differ between x and y.

Example: $D_H(000, 111) = 3$

Code distance determines which errors can be corrected.

Error $e \in \{0,1\}^{\otimes n}$. Weight of error $D_H(e, 0^{\otimes n}) =$

number of zeros: $\overset{c}{\downarrow}$ $y \xmapsto{\text{noise}} y + e = \tilde{y}$

Then, a code of distance d can correct errors up to a weight of $d = 2t+1$, where t

3-repetition code: $d = 3 \Rightarrow t = 1$.

Overall process:

$$x \xrightarrow{\text{encoding}} y \xrightarrow{\text{noise}} \tilde{y} \xrightarrow{\text{decoding}} \tilde{x}$$

Example:

$010 \longrightarrow 000\,111\,000 \longrightarrow 100\,101\,000 \longrightarrow 000\,111\,000$

Succesfull as errors of weight $t=1$ occured $e = 100, 010, 000$

Compare error rates: individual bit flip probability p

- not encoded: success $(1-p)$, failure p
- 3-repetition code:

Success: $(1-p)^3 + 3p(1-p)^2$

↑ no bit flip ↑ single bit flip

failure: $3p^2(1-p) + p^3 = 3p^2 - 2p^3$

Encoding is advantageous for

$$3p^2 - 2p^3 < p \iff 3p - 2p^2 < 1$$

Solve $p^2 - \frac{3}{2}p + \frac{1}{2} = 0 \Rightarrow p_{1/2} = \frac{3}{4} \pm \sqrt{\frac{9}{16} - \frac{1}{2}} =$

$$= \frac{3}{4} \pm \frac{1}{4} = \{1, \frac{1}{2}\}.$$

$$\Rightarrow 3p^2 - 2p^3 < p \Rightarrow \boxed{p < \frac{1}{2}}.$$

For sufficiently small bit flip error rate p, encoding with 3-repetition code is better.

We denote such a classical code as $[n, k, d]$.

n: # physical bits; k: # encoded "logical" bits; d: distance

Code with distance d can

- correct errors up to weight t such that $d = 2t+1$

  Example: $100 \longmapsto 000$.

- detect errors $\leadsto$ $t = d-1$

Example: 110 : is detectable, but not correctable.

In contrast: 3 bit flips $000 \longmapsto 111$ are not detectable.

Define rate of a code $[n, k, d]$ as $R = \frac{k}{n}$.

Good codes have large distance d and rate R.

However, there is usually a tradeoff, e.g. as expressed in the Singleton bound

$$k \leq n - d + 1 \iff \boxed{R \leq 1 - \frac{d-1}{n}}$$

This means that you cannot increase the distance without reducing the bound on the rate.

Challenges that arise when applying this principle to quantum error correction (QEC):

① Phase errors: $\mathcal{E}_Z(\rho) = (1-p)\rho + p Z\rho Z$

$|0\rangle \longrightarrow |0\rangle$

$|1\rangle \longrightarrow -|1\rangle$

$\Rightarrow$ $|\psi\rangle = a|0\rangle + b|1\rangle \longmapsto a|0\rangle - b|1\rangle$.

Most notably:

$|+\rangle_x = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle] \xmapsto{\mathcal{E}} \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle] = |-\rangle_x$

Classical coding provided no protection against phase errors, but only bit flip errors.

② Small errors (errors are continuous)

Amplitudes a, b of state $|\psi\rangle = a|0\rangle + b|1\rangle$ may change by small amount ε. Classical method designed

to correct large (bit flip) errors.

③ Measurement causes disturbance

We measured the bits in the classical code to apply the majority vote. Since measurements affect the quantum state (projection onto eigenstate of measurement operator in projective measurements), it seems as if we cannot measure the qubits without disturbing the quantum information they encode.

④ No cloning theorem

Quantum information cannot be copied, but such a repetition was used in the classical case

Turns out that QEC is still possible.

First example: protect against bit flips as described by the Pauli channel

$$\mathcal{E}_X(\rho) = (1-p)\rho + p\, X\rho X.$$

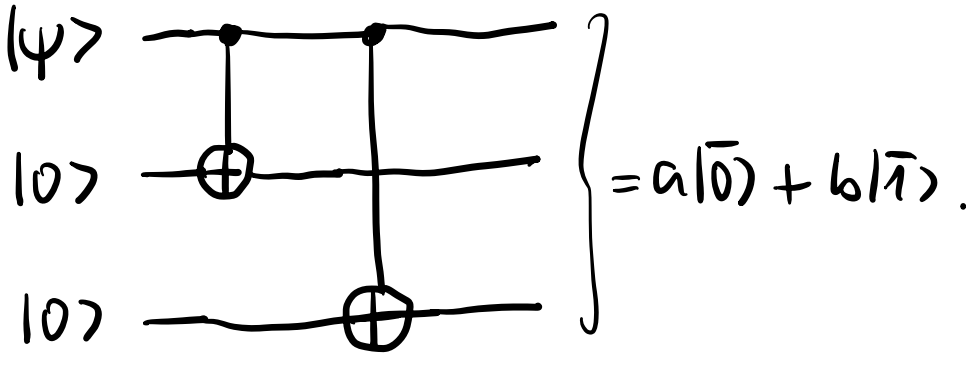
Encode:

$$|0\rangle \longmapsto |\bar{0}\rangle \equiv |000\rangle$$
$$|1\rangle \longmapsto |\bar{1}\rangle \equiv |111\rangle$$

} 3-qubit bit flip code

$$|\psi\rangle = a|0\rangle + b|1\rangle \longmapsto a|\bar{0}\rangle + b|\bar{1}\rangle \equiv a|000\rangle + b|111\rangle$$

Encoding circuit for 3-qubit bit flip code:



Error detection and correction

Measuring the Pauli strings (Z_1Z_2, Z_1Z_3) yields error syndrome: $(\pm 1, \pm 1)$. Pair of eigenvalues uniquely identifies states with no or a single bit flip. Can the be corrected (brought back into the code space by application of a unitary "decay" operator):

	Z_1Z_2	Z_1Z_3
$\|111\rangle, \|0001\rangle$	1	1
$\|011\rangle, \|1001\rangle$	−1	−1
$\|101\rangle, \|0101\rangle$	−1	1
$\|110\rangle, \|0011\rangle$	1	−1

Z_iZ_j measures parity of qubit i & j, i.e. $i+j \bmod 2$.

Note that the codespace is an eigenspace when the commuting Pauli operators $\{Z_1Z_2, Z_1Z_3\}$ have eigenvalue $+1$.

Example.

$$|\psi\rangle = a|0000\rangle + b|1111\rangle$$

$$\downarrow \text{noise}$$

$$|\tilde{\psi}\rangle = a[|0000\rangle + \varepsilon|1000\rangle] + b[|1111\rangle - \varepsilon|0111\rangle]$$

Performing (projective) measurement of (Z_1Z_2, Z_1Z_3) projects out a joint eigenstate of these observables:

- Find $(1,1)$ with probability $1-\varepsilon^2$.

  The state is projected back into the codespace:

  $$|\tilde{\psi}\rangle = a|0000\rangle + b|1111\rangle$$

- Find $(-1,1)$ with probability ε^2.

  The state is projected onto a subspace with one bit flip on the first qubit:

  $$|\tilde{\psi}\rangle = a|1000\rangle + b|0111\rangle.$$

Note that the measurement has "digitized" the small error. The projection has resulted in a state with a single bit flip (which occurs with a small probability ε).

Now we can correct the error by applying X_1:

$$X_1|\tilde{\psi}\rangle = a|0000\rangle + b|1111\rangle.$$

Note that we have not obtained any information about a and b (the quantum information encoded in the state) during this procedure.

This has addressed the challenges ②, ③, ④ above.

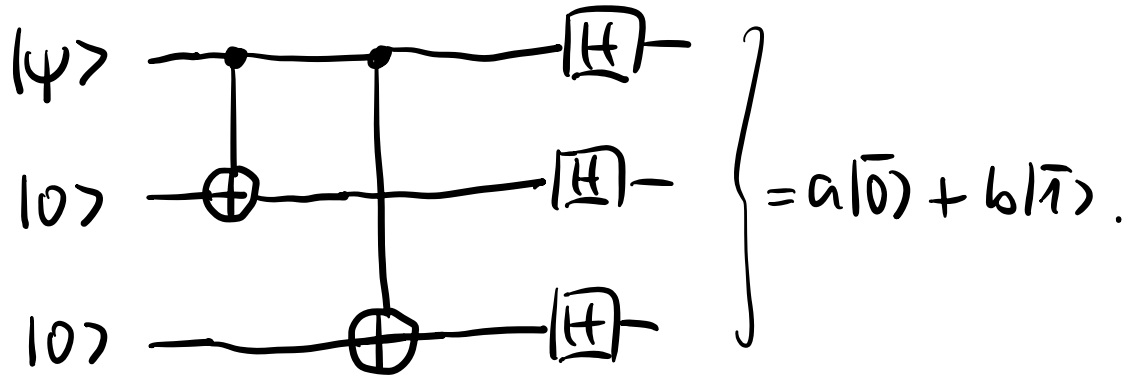
To address the remaining one (phase errors), we consider a different encoding in terms of X eigenstates $|\pm\rangle = \frac{1}{\sqrt{2}}[|0\rangle \pm |1\rangle]$.

3-qubit phase flip code

$$|0\rangle \longrightarrow |\bar{0}\rangle = |+++\rangle = \frac{1}{2^{3/2}}(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)$$

$$|1\rangle \longrightarrow |\bar{1}\rangle \equiv |---\rangle = \frac{1}{2^{3/2}}(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)$$

Encoding circuit: $|\psi\rangle = a|0\rangle + b|1\rangle$



Error syndromes = measurement results of (X_1X_2, X_1X_3) can detect single phase flips ($\mathcal{E}_z(\rho) = (1-p)\rho + p Z\rho Z$):

e.g. $Z_1|+++\rangle = |-++\rangle$, $Z_1|---\rangle = |+--\rangle$.

		X_1X_2	X_1X_3
$\|---\rangle$,	$\|+++\rangle$	1	1
$\|+--\rangle$,	$\|-++\rangle$	−1	−1
$\|-+-\rangle$	$\|+-+\rangle$	−1	1
$\|--+\rangle$	$\|++-\rangle$	1	−1

Correction of the error occurs via application of Z operator on the qubit that experienced the phase error.

9-qubit Shor code:

To protect both against bit flip (X) errors and phase flip (Z) errors [and also against their combination

$Y = iXY$), Shor suggested to concatenate the bit and phase flip codes:

$$|0\rangle \longrightarrow |\bar{0}\rangle = \frac{1}{2^{3/2}}(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)$$

$$|1\rangle \longrightarrow |\bar{1}\rangle = \frac{1}{2^{3/2}}(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)$$

Detect bit flips $X_i|\psi\rangle$ via measuring

$$(Z_1Z_2,\ Z_1Z_3,\ Z_4Z_5,\ Z_4Z_6,\ Z_7Z_8,\ Z_7Z_9)$$ (parity bits)

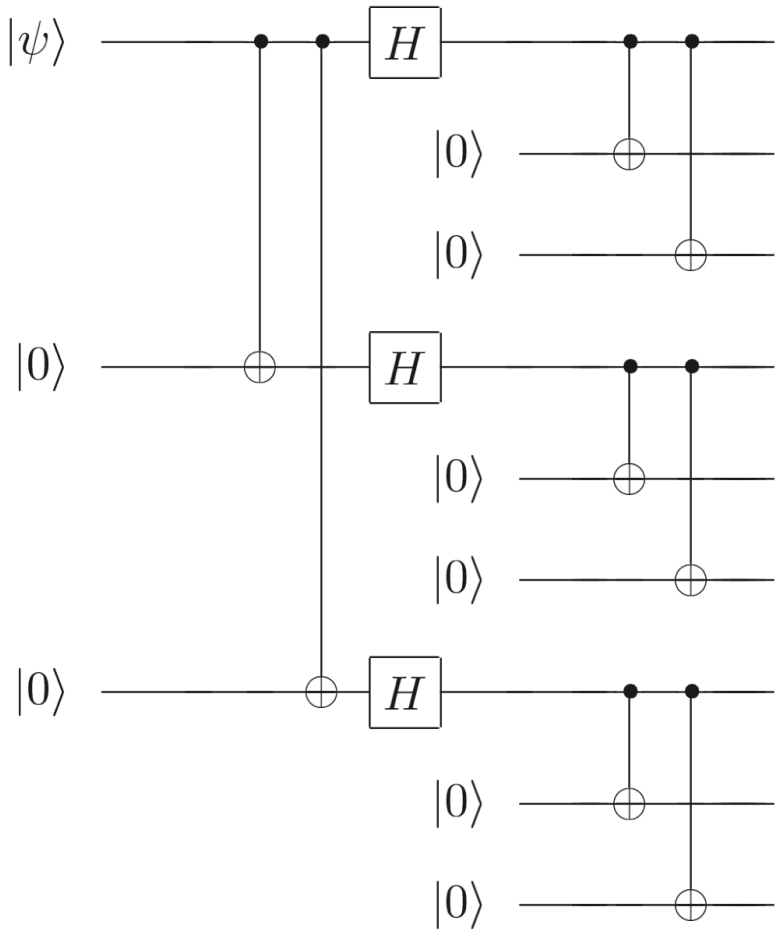
Detect phase flips $Z_i|\psi\rangle$ via measuring

$$(X_1X_2X_3X_4X_5X_6,\ X_4X_5X_6X_7X_8X_9)$$ (phase bits)

States in the codespace lie in the joint eigenspace with eigenvalue $+1$ of all these operators.

Logical qubit is encoded nonlocally. No way to distinguish $|\bar{0}\rangle$ and $|\bar{1}\rangle$ by measuring any one or two qubits in the block of nine.

Encoding circuit



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

$$|\psi\rangle|0\rangle|0\rangle \longrightarrow a|000\rangle + b|111\rangle \longrightarrow \underbrace{a|+++\rangle + b|---\rangle}$$

$$= \frac{a}{2^{3/2}}(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)$$

$$\longrightarrow \frac{a}{2^{3/2}}\left(|000\rangle + |111\rangle\right)\left(|000\rangle + |111\rangle\right)\left(|000\rangle + |111\rangle\right)$$

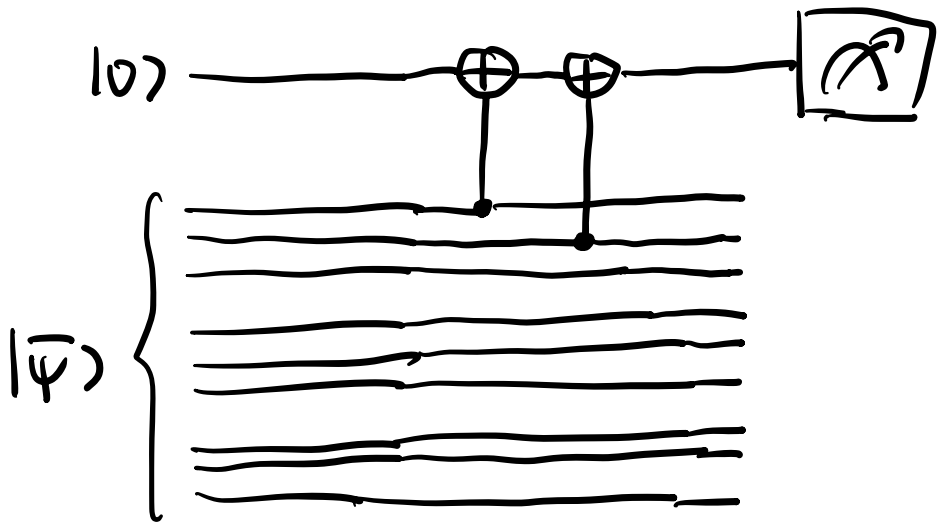
$$+ \frac{b}{2^{3/2}}\left(|000\rangle - |111\rangle\right)\left(|000\rangle - |111\rangle\right)\left(|000\rangle - |111\rangle\right) =$$

$$= a\left[\frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)\right]^{\otimes 3} + b\left[\frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right)\right]^{\otimes 3}.$$

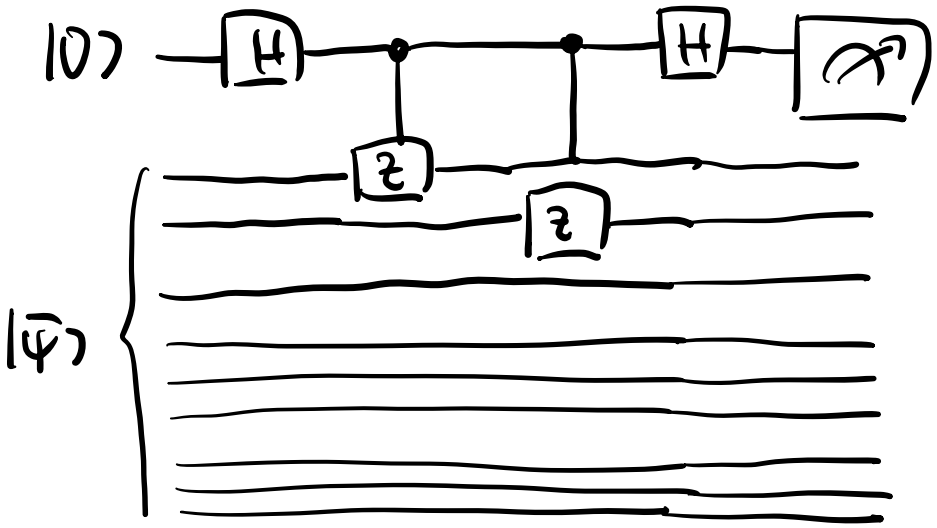
3-qubit cat state repeated 3 times.

Measurement circuits:

e.g. $Z_1 Z_2$ measurement



or



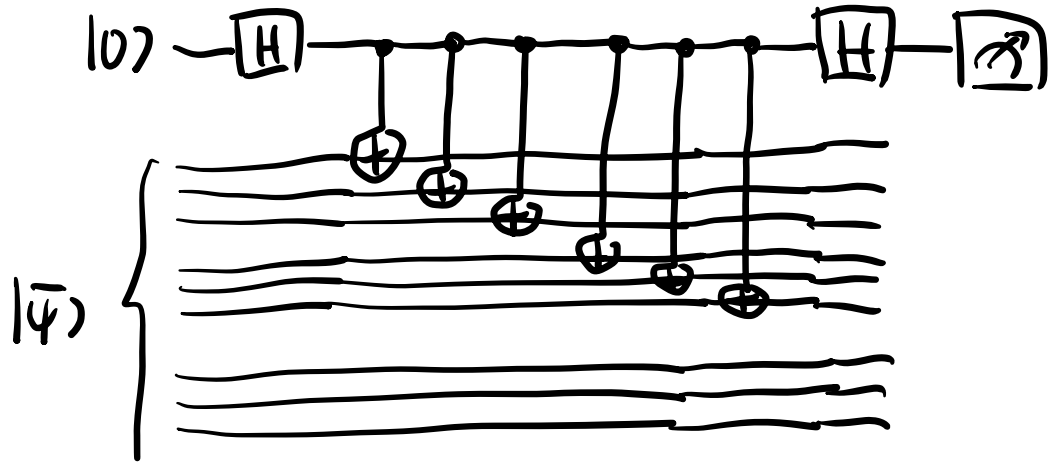
$$|0\rangle|\bar{\Psi}\rangle \rightarrow \left(\frac{1}{\sqrt{2}}|0\rangle + |1\rangle\right)|\bar{\Psi}\rangle \rightarrow \left(\frac{1}{\sqrt{2}}|0\rangle|\bar{\Psi}\rangle + Z_1 Z_2 |1\rangle|\bar{\Psi}\rangle\right)$$

$$\longrightarrow \frac{1}{2}(|0\rangle + |1\rangle)|\bar{\psi}\rangle + \frac{1}{2}(|0\rangle - |1\rangle) Z_1 Z_2 |\bar{\psi}\rangle =$$

$$= \frac{1}{2}(1 + Z_1 Z_2)|0\rangle|\bar{\psi}\rangle + \frac{1}{2}(1 - Z_1 Z_2)|1\rangle|\bar{\psi}\rangle .$$

Measurement of ancilla will yield 0 or 1 and collapse logical qubit to $\frac{I \pm Z_1 Z_2}{2}|\bar{\psi}\rangle$ eigenspaces, respectively.

Measurement circuit of $X_1 X_2 X_3 X_4 X_5 X_6$:



$$|0\rangle|\bar{\psi}\rangle \longrightarrow \frac{I + X_1 X_2 X_3 X_4 X_5 X_6}{2}|0\rangle|\bar{\psi}\rangle$$

$$+ \frac{I - X_1 X_2 X_3 X_4 X_5 X_6}{2}|1\rangle|\bar{\psi}\rangle .$$

Code distance and errors we cannot correct:

- Two bit flips in a single cluster of 3 qubits, e.g.,

$$X_1 X_2 |\bar{0}\rangle = \frac{1}{2^{3/2}} (|110\rangle + |001\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$X_1 X_2 |\bar{1}\rangle = \frac{1}{2^{3/2}} (|110\rangle - |001\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

will be falsely "corrected" via majority voting and application of a third bit flip operator X_3:

$$\left.\begin{aligned} X_1 X_2 X_3 |\bar{0}\rangle &= |0\rangle \\ X_1 X_2 X_3 |\bar{1}\rangle &= -|1\rangle \end{aligned}\right\} \Rightarrow \text{logical phase flip error}$$

$$Z_1 |\psi\rangle = Z_1 (a|\bar{0}\rangle + b|\bar{1}\rangle)$$

$$= a|\bar{0}\rangle - b|1\rangle$$

Similarly, two phase flip errors in different clusters cannot be corrected and result in a logical bit flip:

$$Z_1 Z_4 |\bar{0}\rangle = \frac{1}{2^{3/2}} (|0000\rangle - |1111\rangle)(|0000\rangle - |1111\rangle)(|000\rangle + |111\rangle)$$

$$Z_1 Z_4 |1\rangle = \frac{1}{2^{3/2}} (|0000\rangle + |1111\rangle)(|0000\rangle + |1111\rangle)(|000\rangle - |111\rangle)$$

will be falsely corrected by application of Z_7 (or equivalently Z_8 or Z_9), resulting in

$$\left.\begin{aligned} Z_1 Z_4 Z_7 |\bar{0}\rangle &= |\bar{1}\rangle \\ Z_1 Z_4 Z_7 |\bar{1}\rangle &= |\bar{0}\rangle \end{aligned}\right\} \text{ logical bit flip error.}$$

Code distance of Shor code is therefore $d = 3$ (can correct errors up to weight $t = 1$ (= weight of error Pauli strings). We can detect errors up to weight $d - 1 = 2$.

We write that Shor code is a

$$[[n, k, d]] = [[9, 1, 3]] \text{ code.}$$

physical qubits

logical qubits

distance

Error probabilities of encoded qubits

Consider depolarizing channel: $\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$

$\Rightarrow$ Unencoded qubit: failure with probability p

$\Rightarrow$ Slow logical qubit:

- Logical phase error (Z error) requires two bit flips on the same cluster:

  Probability for bit flip of physical qubit $= \frac{2}{3}p$

  (X and Y errors).

  $\Rightarrow$ Prob. for two bit flips on the same cluster is upper bounded by

$$\leq \binom{3}{2} \cdot 3 \cdot \left(\frac{2}{3}p\right)^2 = \frac{3 \cdot 2}{2} \cdot 3 \cdot \frac{4}{9}p^2 =$$

$$= 4p^2 \quad \text{(upper bound of logical phase flip)}$$

Reasoning

$$1 - F \leq \sum_{s=t+1}^{n} \binom{n}{s} p^s (1-p)^{n-s} \leq \binom{n}{t+1} p^{t+1}$$

for each of the $\binom{n}{t+1}$ ways of choosing $t+1$ error locations in n qubits, we disregard whether errors also occur in any of the other $n-t-1$ locations $\Rightarrow$ this is thus an upper bound on the prob. that at least $t+1$ errors occur in n qubits.

Similarly, logical bit flips require a physical