Quantum error correction (QEC)

- Challenges of QEC
- Bit flip code & phase flip code
- Encoding & error syndrome circuits
- Shor code [[9, 1, 3]]

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

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

$$|0\rangle \longrightarrow |0\rangle$$
$$|1\rangle \longrightarrow -|1\rangle$$

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

Most notably:

$$|+\rangle_x = \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right] \overset{\mathcal{E}}{\longmapsto} \frac{1}{\sqrt{2}}\left[|0\rangle - |1\rangle\right] = |-\rangle_x$$

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

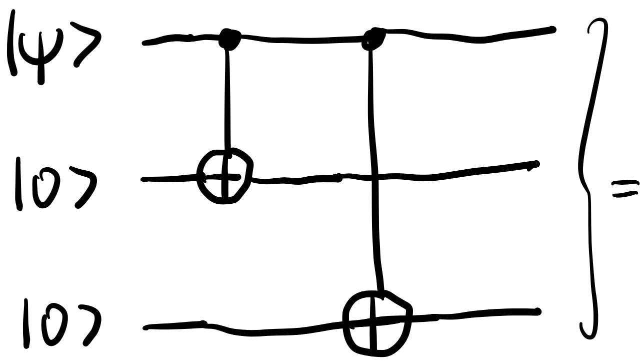
$$\mathcal{E}_X(\rho) = (1-p)\rho + p X\rho X .$$

Encode:

$$\left.\begin{array}{l} |0\rangle \longmapsto |\bar{0}\rangle \equiv |000\rangle \\[2em] |1\rangle \longmapsto |\bar{1}\rangle \equiv |111\rangle \end{array}\right\} \text{3-qubit bit flip code}$$

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

Encoding circuit for 3-qubit bit flip code:



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

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 then be corrected (brought back into the code space by application of a unitary „recovery" operator):

	Z_1Z_2	Z_1Z_3
$\vert 111\rangle, \vert 000\rangle$	1	1
$\vert 011\rangle, \vert 100\rangle$	-1	-1
$\vert 101\rangle, \vert 010\rangle$	-1	1
$\vert 110\rangle, \vert 001\rangle$	1	-1

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

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

Example.

$$|\psi\rangle = a|000\rangle + b|111\rangle$$

$$\Big\downarrow \text{ noise}$$

$$|\tilde{\psi}\rangle = a\big[|000\rangle + \varepsilon|100\rangle\big] + b\big[|111\rangle - \varepsilon|011\rangle\big]$$

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:

$$|\tilde{\psi}\rangle = a|000\rangle + b|111\rangle$$

- Find $(-1,1)$ with probability ε^2.

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

$$|\tilde{\psi}\rangle = a|100\rangle + b|011\rangle .$$

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:

$$X_1|\tilde{\psi}\rangle = a|000\rangle + b|111\rangle .$$

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.

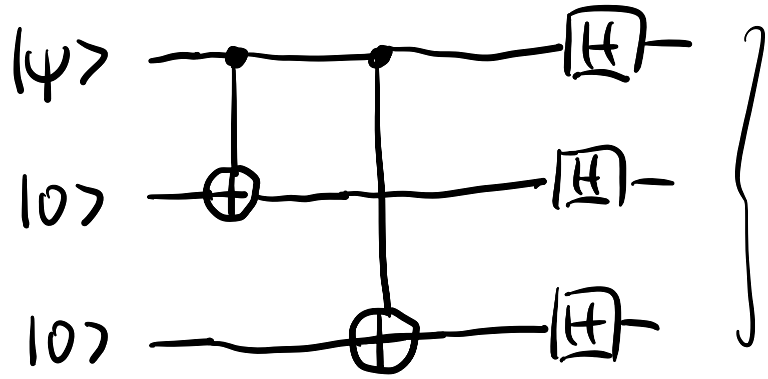
To address the remaining one (phase errors), we consider a different encoding in terms of X eigenstates $|\pm\rangle = \frac{1}{\sqrt{2}}[|0\rangle \pm |1\rangle]$.

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



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

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

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:

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

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

Detect bit flips $X_i|\bar{\Psi}\rangle$ via measuring

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

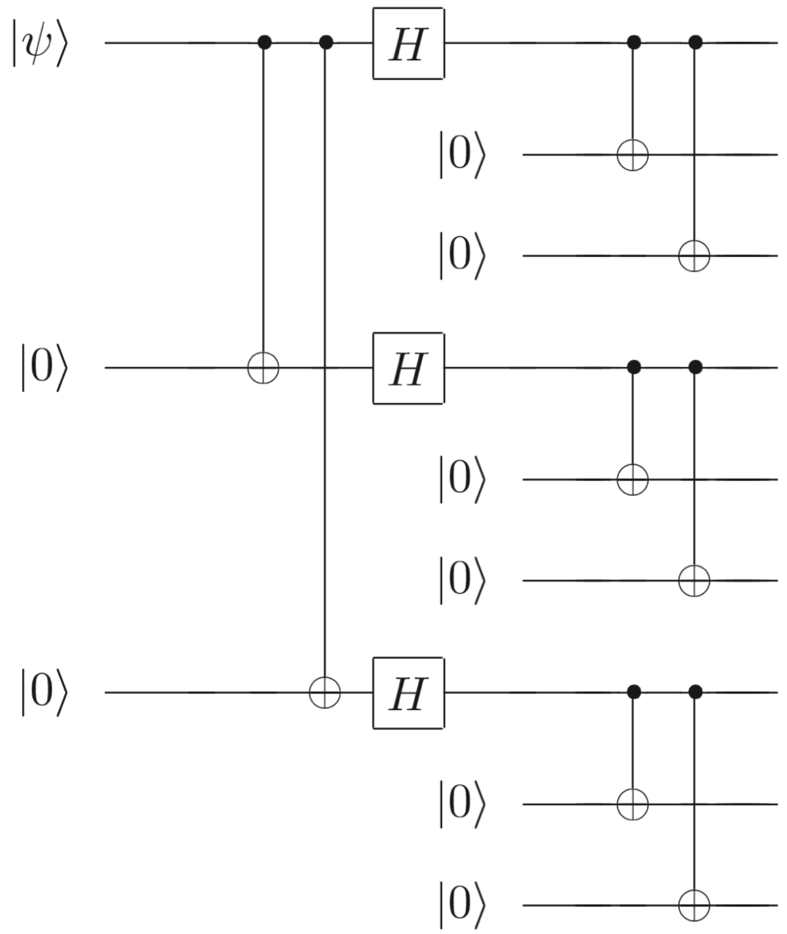
Detect phase flips $Z_i|\bar{\Psi}\rangle$ via measuring

$$\left(X_1X_2X_3X_4X_5X_6,\ X_4X_5X_6X_7X_8X_9\right)$$ (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



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

$$|\psi\rangle|0\rangle|0\rangle \longrightarrow a|000\rangle + b|111\rangle \longrightarrow \underbrace{a|{+}{+}{+}\rangle}_{= \frac{a}{2^{3/2}}(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)} + b|{-}{-}{-}\rangle$$

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

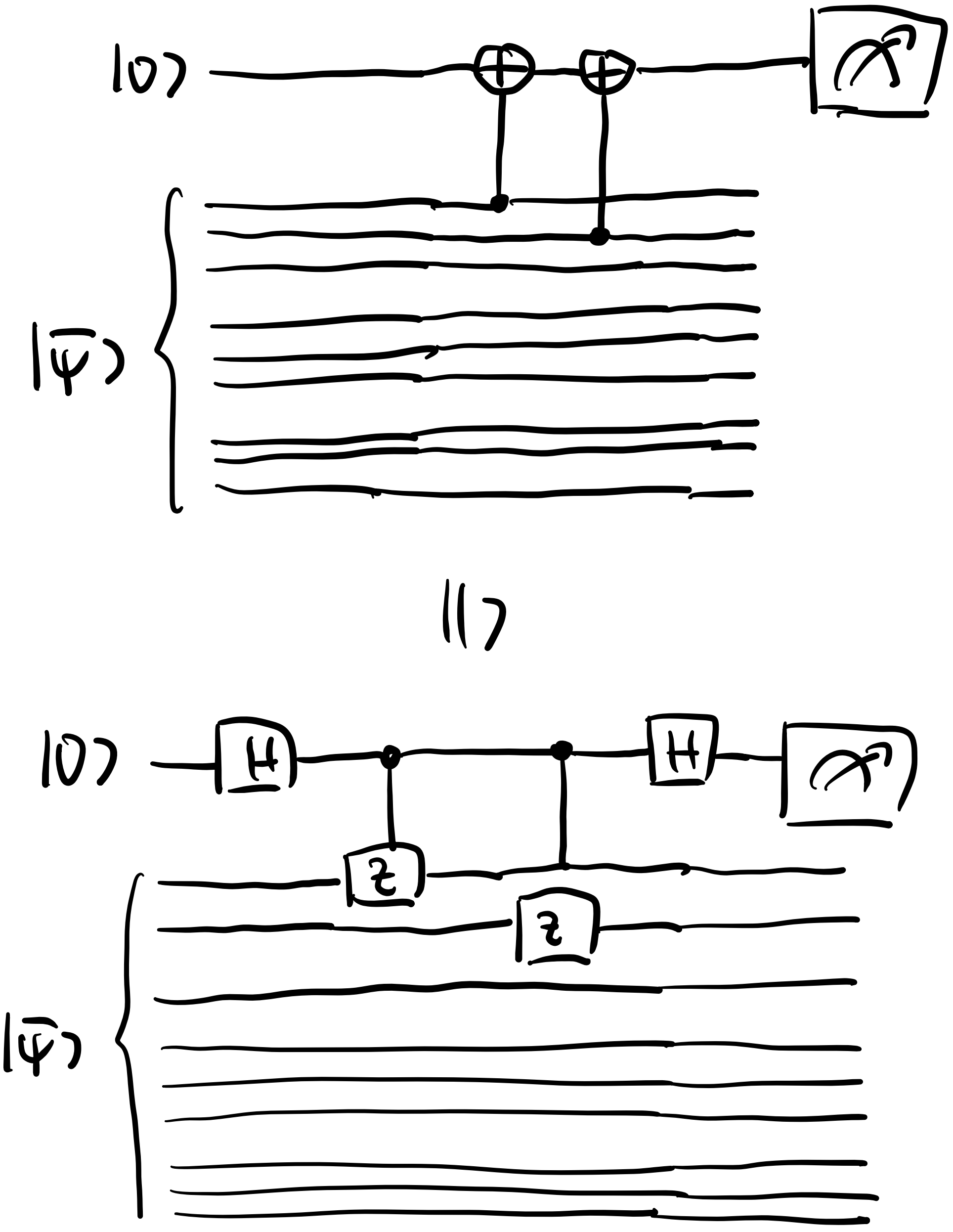
$$+ \frac{b}{2^{3/2}}\Big(|000\rangle - |111\rangle\Big)\Big(|000\rangle - |111\rangle\Big)\Big(|000\rangle - |111\rangle\Big) =$$

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

3-qubit cat state repeated 3 times.

Measurement circuits:

e.g. $Z_1 Z_2$ measurement



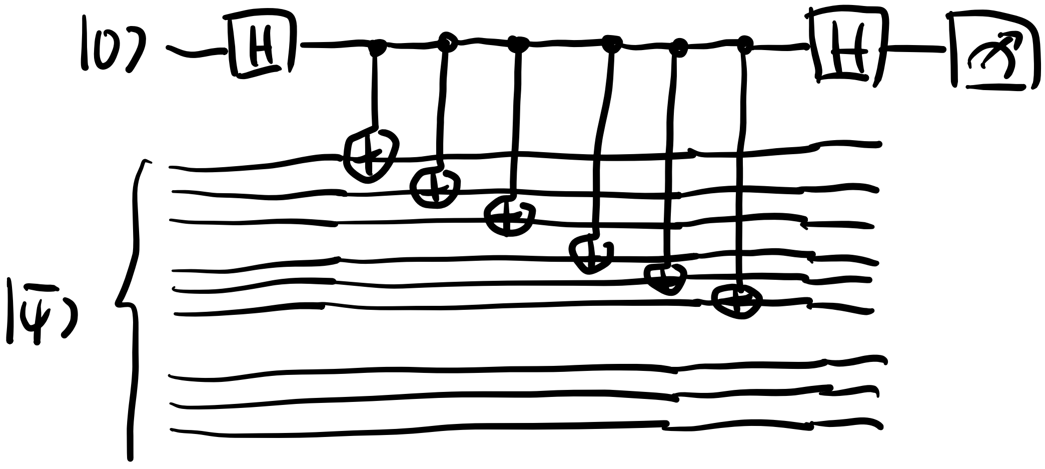
$$|0\rangle|\bar\Psi\rangle \longrightarrow \left(\frac{1}{\sqrt{2}}|0\rangle+|1\rangle\right)|\bar\Psi\rangle \longrightarrow \left(\frac{1}{\sqrt{2}}|0\rangle|\bar\Psi\rangle + Z_1 Z_2\,|1\rangle|\bar\Psi\rangle\right)$$

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

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

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 ditance and errors we cannot correct:

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

$$X_1X_2|\bar{0}\rangle = \frac{1}{2^{3/2}}\left(|110\rangle + |001\rangle\right)\left(|000\rangle + |111\rangle\right)\left(|000\rangle + |111\rangle\right)$$

$$X_1X_2|\bar{1}\rangle = \frac{1}{2^{3/2}}\left(|110\rangle - |001\rangle\right)\left(|000\rangle + |111\rangle\right)\left(|000\rangle + |111\rangle\right)$$

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

$$\left.\begin{aligned} X_1X_2X_3|\bar{0}\rangle &= |0\rangle \\ X_1X_2X_3|\bar{1}\rangle &= -|1\rangle \end{aligned}\right\} \Rightarrow \text{logical phase flip error}$$

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

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

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

$$Z_1Z_4|\bar{0}\rangle = \frac{1}{2^{3/2}}\left(|000\rangle - |111\rangle\right)\left(|000\rangle - |111\rangle\right)\left(|000\rangle + |111\rangle\right)$$

$$Z_1Z_4|1\rangle = \frac{1}{2^{3/2}}\left(|000\rangle + |111\rangle\right)\left(|000\rangle + |111\rangle\right)\left(|000\rangle - |111\rangle\right)$$

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

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

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

We write that Shor code is a

$$[[n, k, d]] = [[\underset{\substack{\uparrow \\ \#\text{physical} \\ \text{qubits}}}{9}, \underset{\substack{\uparrow \\ \#\text{ logical} \\ \text{qubits}}}{1}, \underset{\substack{\uparrow \\ \text{distance}}}{3}]] \text{ code.}$$

Error probabilities of encoded qubits

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

① Unencoded qubit: failure with probability p

② Shor 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

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

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

Reasoning

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

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 ⇒ this is thus an upper bound on the prob. that at least $t+1$ errors occur in n qubits.

Holds that

$$\sum_{s=t+2}^{n} \binom{n}{s} (1-p)^{n-s} \le 1$$

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$$

Similarly, logical bit flips require a physical phase flip to occur in two different clusters.

Probability for two phase flips on different clusters is upper bounded by

$$\binom{3}{2} \cdot 3^2 \cdot \left(\frac{2}{3}p\right)^2 = \underbrace{\frac{3!}{2!\,1!}}_{=\frac{3\cdot 2}{2}} \cdot 9 \cdot \frac{4}{9} p^2 = \underline{12 p^2}.$$

The total logical error probability is thus upper bounded by

$$P_{L,\text{Bit flip}} + P_{L,\text{phase flip}} = 4p^2 + 12p^2$$

$\Rightarrow$ Shor logical qubit has smaller error probability if

$$16p^2 < p \iff \boxed{p < \frac{1}{16}}$$

Criteria for QEC

General evolution of a qubit coupled to an environment (Stinespring dilation):

orthonormal basis

$$\mathcal{U} : |\psi\rangle|0\rangle_E \longmapsto \sum_a M_a |\psi\rangle |a\rangle_E$$

Kraus operator (not necessarily hermitian or unitary)

Can expand M_a in the Pauli basis $\mathcal{P}_m = \{I, X, Y, Z\}^{\otimes m}$ as

$$M_a = \sum_{b=0}^{4^m-1} C_{ab} P_b \quad , \; P_0 = I^{\otimes m} .$$

We use Preskill's notation $E_a \equiv P_a$ for Pauli operators now.

$\Rightarrow$ can also write most general qubit + E evolution as

$$\mathcal{U} : |\psi\rangle|0\rangle_E \longrightarrow \sum_a \sum_{b=1}^{4^m-1} C_{ab} E_b |\psi\rangle |a\rangle_E =$$

$$= \sum_{b=0}^{4^m-1} E_b |\psi\rangle \underbrace{\Big(\sum_a C_{ab} |a\rangle_E \Big)}_{=|e_b\rangle}$$

$$\Rightarrow \quad \mathcal{U} : |\psi\rangle|0\rangle_E \longmapsto \sum_{a=0}^{4^n-1} E_a |\psi\rangle |e_a\rangle_E$$

n-qubit Pauli operator is hermitian & unitary.

not necessarily orthogonal or normalized!

While not strictly true unless the $\{|e_a\rangle_E\}$ are orthogonal, we can interpret this expansion as the possible Pauli errors that can occur.

Definition:

The weight $t \in \mathbb{N}$ of a Pauli operator $P_a \in \mathcal{P}_n$ is the number of non-identity terms $\{X, Y, Z\}$ in the Pauli string. Example: $IIXZI$ has weight $t = 2$.

We denote a subset $\mathcal{E}$ of the n-qubit Pauli group P_n as the set of correctable errors (errors we wish to be able to correct): $\mathcal{E} \subseteq \mathcal{P}_n = \{E_a\} = \{I, X, Y, Z\}^{\otimes n}$.

Example: $\mathcal{E} = \{$ all $P_a \in \mathcal{P}_n$ with weight $t \leq 1\}$.

Conditions for QEC

Starting from a state in the codespace $|\bar{i}\rangle \in C$, we wish to undo any action composed of errors $\{E_a\} \in \mathcal{E}$:

General evolution under superoperator composed of correctable errors:

orthonormal

$$|\bar{i}\rangle|0\rangle_E \longmapsto \sum_{\mu} M_\mu |\bar{i}\rangle |\mu\rangle_E$$

Kraus operators $M_\mu = \sum_{a\in\mathcal{E}} c_{\mu a} E_a$

that are composed of Paulis in $\mathcal{E}$.

Fulfill $\sum_\mu M_\mu^\dagger M_\mu = I$.

The error can be reversed by a recovery superoperator if there exist Kraus operators $\{R_\nu\}$ such that

$$\sum_\nu R_\nu^\dagger R_\nu = I \quad \text{and}$$

orthonormal basis of Hilbert space of ancilla. Needed to implement recovery operation

$$\boxed{\sum_{\mu,\nu} R_\nu M_\mu |\bar{i}\rangle |\mu\rangle_E |\nu\rangle_A = |\bar{i}\rangle |\text{stuff}\rangle_{EA}}$$

Importantly:

- Entanglement b/w qubit and E has been moved to entanglement b/w E and A (ancillas).

- The state $|\text{stuff}\rangle_{EA}$ must not depend on i, so it is impossible to learn any information about the state of the logical qubit $|\bar{i}\rangle$ from observing EA.

- Note that we had seen that only unitary channels can be completely reversed. Here, we ask for less: $\{R_\nu\}$ only reverses the action of $\{M_\mu\}$ on the code subspace C.

[C is a 2^k- subspace of the 2^n-dim. full Hilbert space, $\{|\bar{i}\rangle\}$ is an orthonormal basis of C]

For this to hold, we need

$$R_\nu M_\mu |\bar{i}\rangle = \lambda_{\nu\mu} |\bar{i}\rangle \qquad \forall \mu, \nu.$$

The product $R_\nu M_\mu$ acts on the code subspace $\{|\bar{i}\rangle\}$ as a multiple of the identity.

Using that $\sum_\nu R_\nu^\dagger R_\nu = I$, we find

$$M_\delta^\dagger M_\mu |\bar{i}\rangle = M_\delta^\dagger \left(\sum_\nu R_\nu^\dagger R_\nu \right) M_\mu |\bar{i}\rangle =$$

$$= \sum_\nu \lambda_{\nu\delta}^* \lambda_{\nu\mu} |\bar{i}\rangle$$

so that $M_\delta^\dagger M_\mu$ is also a multiple of the identity when acting on the codespace C. A necessary and sufficient condition on the codespace C for allowing errors contained in $\mathcal{E}$ to be corrected is that

$$\boxed{\langle \bar{j} | M_\delta^\dagger M_\mu | \bar{i} \rangle = C_{\delta\mu} \delta_{ij}}$$

with $C_{\delta\mu}$ being an arbitrary hermitian matrix that is independent of i, j.

Note $C_{\delta\mu} = \sum_\nu \lambda_{\nu\delta}^* \lambda_{\nu\mu} \Rightarrow (C^\dagger)_{\delta\mu} = C_{\mu\delta}^* =$

$= \sum_\nu \lambda_{\nu\mu} \lambda_{\nu\delta}^* = C_{\delta\mu}$ is hermitian.

Since $M_\mu = \sum_a c_{\mu a} E_a$, this implies

$$\boxed{\begin{array}{c} \langle \bar{j} | E_b^\dagger E_a | \bar{i} \rangle = C_{ba}\, \delta_{ij} \\ \text{for } E_a, E_b \in \mathcal{E} \text{ and } C_{ba} = \langle \bar{i} | E_b^\dagger E_a | \bar{j} \rangle \end{array}}$$

being an arbitrary hermitian matrix $C^\dagger = C$ that is independent of i, j.

An alternative way to show that this condition is necessary is to note that if the code block is prepared in any state $|\psi\rangle$ and an error acts according to $U : |\psi\rangle|0\rangle_E \rightarrow \sum_\mu M_\mu |\psi\rangle |\mu\rangle_E$, then the reduced density matrix of the $\underline{\text{environment}}$ $\underline{\rho_E}$ after tracing over the code space C reads

$$\rho_E = \sum_{\mu,\nu} |\mu\rangle_E \langle \psi | M_\nu^\dagger M_\mu | \psi \rangle \langle \nu |_E .$$

Error recovery is only possible if it is impossible to obtain any information about $|\psi\rangle$ by performing a measurement on the environment.

Thus, ρ_E must be independent of $|\psi\rangle$, if $|\psi\rangle$ is any state in the codespace

$$\underset{C}{\underset{\cap}{|\psi\rangle}} = \sum_i c_i |\bar{i}\rangle$$

$$\Rightarrow \rho_E = \sum_{\substack{\mu,\nu \\ i,j}} c_i c_j^* |\mu\rangle_E \langle \bar{j} | M_\nu^\dagger M_\mu | \bar{i} \rangle \langle \nu |_E$$

Independence of ρ_E from $c_i c_j^*$ requires that

$$\langle \bar{j} | M_\nu^\dagger M_\mu | \bar{i} \rangle = C_{\nu\mu} \delta_{ij}$$

with $C_{\nu\mu}$ being independent of i,j.

Then,

$$\rho_E = \sum_{\mu,\nu} \sum_{i} |c_i|^2 \, |\mu\rangle_E \, C_{\mu\nu} \, \langle\nu|_E =$$

$$= \sum_{\mu,\nu} C_{\mu\nu} \, |\mu\rangle_E \langle\nu|_E$$

$\langle\psi|\psi\rangle = 1$

$\Rightarrow \sum_i |c_i|^2 = 1$

is independent of $|\psi\rangle$ as required.