## Quantum error correction

- A quantum system is always affected by external environment.
- When qubits are transmitted or processed, there will be errors, say, decoherence.
- Quantum channels, process, etc. are modeled by $\mathcal{E} : M_n \to M_m$ such that

$$\mathcal{E}(A) = \sum_{j=1}^{r} E_j A E_j^\dagger \quad \text{for all } A \in M_n,$$

  where $E_1, \ldots, E_r$ are $m \times n$ matrices, known as error (Kraus) operators of the channel, satisfying $\sum_{j=1}^{r} E_j^\dagger E_j = I_n$.
- We would like to find a recovery channel, process $\mathcal{R} : M_m \to M_n$ such that $R \circ \mathcal{E}(\rho) = \rho$ if $\rho \in D_n$ lies in some (code words) subspace.
- The coding subspace is called the quantum error correction code, and the scheme of encoding an decoding is the corresponding error correction schemes.

## Early approach to error correction

- For example, classical bits 0 or 1 is sent through a classical channel $\mathcal{E}$ such that there is a probability $p < 1/2$ such that $x$ is sent to $x \oplus 1$.
- So, the probability of correct transmission is $1 - p$.
- One may improve the hardware to improve (decreases) $p$.
- Using existing hardware, one may transmit the code words $(0,0,0)$ and $(1,1,1)$ in $\mathbf{Z}^3$ for 0 or 1.
- Then decode the received word $(x_1x_2x_3)$ by majority rule.
- If $(x,x,x)$ is sent, the received word has 0, 1, 2, 3 errors are

$$(1-p)^3, \quad 3p(1-p)^2, \quad 3p^2(1-p), \quad p^3.$$

- The majority decoding will give incorrect answer with probability.

$$p^3 + 2p^2(1-p) = p^2(2-p) << p.$$

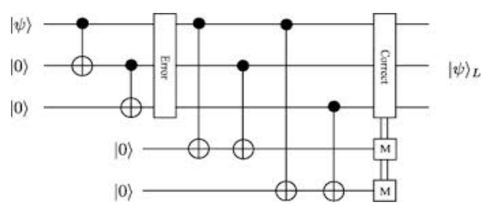
## Quantum error correction

- Can we use the idea of classical encoding?
- No-cloning theorem forbids use to get a unitary $U \in U(8)$ such that $U|x00\rangle = |xxx\rangle$.
- Nevertheless, we can have a unitary $U$ such that

  $$U|x00\rangle = |xxx\rangle \text{ for } |x\rangle \in \{|0\rangle, |1\rangle\} \text{ to encode}$$

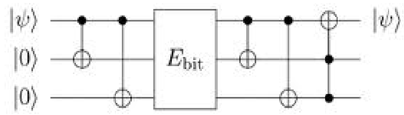
  $$|\psi\rangle = a|0\rangle + b|1\rangle \text{ as } |\psi\rangle_L = a|000\rangle + b|111\rangle,$$

  and use the following scheme with "syndrome" measurement was proposed.




- If $|\psi\rangle = |000\rangle$ is sent, one may receive $|000\rangle, |100\rangle, |010\rangle, |001\rangle, \ldots,$ and syndrome measurement will yield $|00\rangle, |11\rangle, |10\rangle, |01\rangle, \ldots$
- One may apply $III, XII, IXI, IIX$ for correction.
- The same holds if $|\psi\rangle = |111\rangle$ is sent,
- Thus, the scheme works for any $|\psi\rangle = a|000\rangle + b|111\rangle$.

- The following use the following QECC without syndrome measurement.




- The QECC scheme with syndrome measurement has been extended to study aribitrary error $|\psi\rangle \mapsto U|\psi\rangle$, where $U \in U(2)$ by Calderbank, Shor, Steane, etc. in mid 1990's.

  * Use logical qubit $|\psi\rangle_L = a|000000000\rangle + b|111111111\rangle \in \mathbf{C}^{2^9}$ with 6 ancillas to detect syndrome.

  * Use logical qubit in $\mathbf{C}^{2^7}$ with 6 ancillas to detect syndrome.

  * The optimal scheme: use local qubit in $\mathbf{C}^{2^5}$ and 4 ancillas to detect syndrome.

- (Shi and Sze, 2016) gave an explicit circuit for a QECC using logical qubit in $\mathbf{C}^{2^5}$ without syndrome measurement.

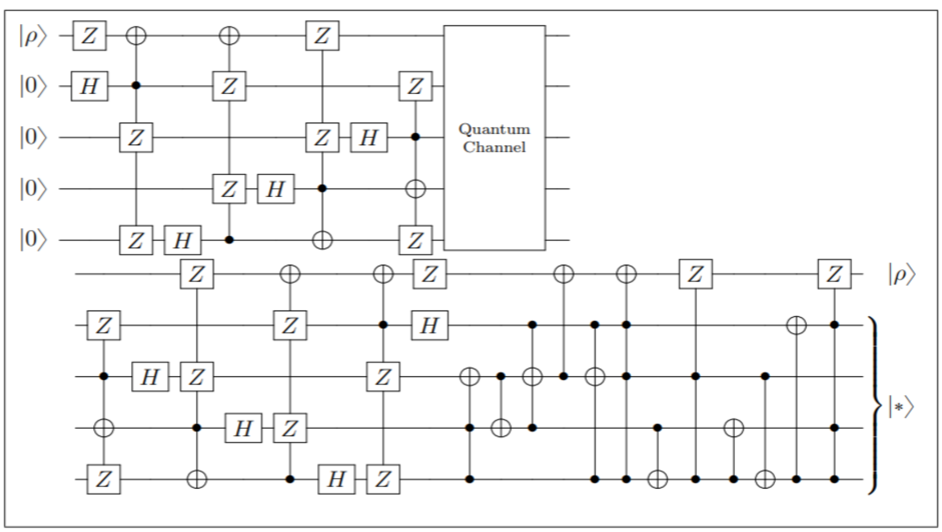



Figure 4.9: An encoding and decoding quantum circuit of [5,1,3] code.

**Linear algebra (Operator algebra) approach**

- A more realistic model(?). Suppose a quantum channel $\mathcal{E} : M_n \to M_n$ has error operators $E_1, \dots, E_r \in M_n$, say, determined by process tomography. Can we find a QECC for the channel? What is the maximum dimension of the QEC?

- (Knill-Laflamme, 1997). There is a QEC with dimension $k$ if and only if there is a unitary $U$ such that

$$UE_i^\dagger E_j U^\dagger = \begin{pmatrix} d_{ij} & \star \\ \star & \star \end{pmatrix} \text{ for all } i, j. \qquad (\star)$$

  The first $k$ columns of $U$ spans the QEC.

- In practice, we always assume that $n = 2^p$ and $k = 2^q$.

- (Li, Nakahara, Poon, Sze, 2012). Once the subspace There are unitary $U, R \in U(n)$ such that for any $\rho \in \mathbf{C}^k$, we can do the encoding and decoding as follows:

  Encoding: $\rho \mapsto \hat{\rho} = U(\sigma \otimes \rho)U^\dagger$.

  Transmission: $\hat{\rho} \mapsto \tilde{\rho} = \mathcal{E}(\hat{\rho})$.

  Decoding: $R^\dagger \tilde{\rho} R = (\tilde{\sigma} \otimes \rho) \oplus 0_\ell$.

  If $n = 2^p, k = 2^q$, we may assume that $\ell = 0$ so that

$$\mathrm{Tr}_1(\tilde{\sigma} \otimes \rho) = \rho.$$

- For some channels, we may let $U = R$. This has nice implications in QIS study...

- Open problem. Determine $U$ and $R$, and find efficient say to implement.

- Given $E_1, \dots, E_r$, we need $U$ satisfying $(\star)$ with large $k$.

- Find unitary $U$ are $R$ that can be implemented effectively.

  One may settle with a smaller $k$.

- Study special channels, use Lie theory, group theory, operator theory, etc.

- A lot of opportunities for further research.

- Thank you very much for your attention, and your valuable comments.
- Hope that the lectures can stimulate more research interest and interaction in QIC and QC.

**Happy New Year!**