Quantum error correction

10.1 Classical quantum error correction

In classical communication, suppose a noisy channel will change x to $x \oplus 1$ for $x = 0, 1$ with a probability $p < 1/2$. One may send xxx instead of x and use maximum likelihood decoding so that the probability of correct transmission for one bit is the sum of the probabilities of x sent to xxx, $xx\hat{x}$, $x\hat{x}x$, $\hat{x}xx$ sum up to:

$$(1-p)^3 + 3p(1-p)^2 = (1-p)^2(1+2p) \gg 1-p;$$

the probabilities of x sent to $\hat{x}\hat{x}\hat{x}$, $x\hat{x}\hat{x}$, $\hat{x}\hat{x}x$, $\hat{x}\hat{x}x$ sum up to:

$$p^3 + 3p^2(1-p) = p^2(3-2p) \ll p$$

if p is small.

10.2 Quantum error correction

10.2.1 Bit-Flip QECC

We cannot copy qubit because of no-cloning.

But, we can encode $|\psi\rangle = a|0\rangle + b|1\rangle$ as $|\psi\rangle_L = a|000\rangle + b|111\rangle$ using $CNOT$ gates on $|\psi\rangle|00\rangle$.

Then the set of **code words** is

$$\mathbf{C} = \{a|000\rangle + b|111\rangle : a, b \in \mathbb{C}, |a|^2 + |b|^2\}.$$

The QECC scheme can be done in the following steps.

- Encode $|\psi\rangle = a|0\rangle + b|1\rangle$ as $|\psi\rangle_L = a|000\rangle + b|111\rangle \in \mathbf{C}$.
- Transmit via the quantum channel.
- Apply error syndrome detection and correction
  * Suppose $|x_1x_2x_3\rangle$ is received.
  * Add two ancillas $|AB\rangle$ with $A = |x_1 \oplus x_2\rangle$, $B = |x_1 \oplus x_3\rangle$ to detect the **(error) syndrome**.
  * Apply correction to correct $|\psi\rangle_L$ accordingly.
- Reversing the encoding step, one gets $|\psi\rangle$.

Continuous rotation

Suppose the error operator is

$$U_\alpha = e^{i\alpha X} = \cos\alpha I + i\sin\alpha I$$

and U_α acts on each qubit with a probability $p \in (0, 1/2)$.

Suppose we use the same QECC scheme for the bit-flip channel.

If U_α acts on the first logical qubit $|\psi\rangle_L = a|000\rangle + b|111\rangle$, then the transmitted state becomes

$$(U_\alpha \otimes I \otimes I)|\psi\rangle_L = \cos\alpha|\psi\rangle_L + i\sin\alpha(\alpha|100\rangle + b|011\rangle\rangle).$$

Applying syndrome measurement $|AB\rangle$ to the transmitted state, we get

$$\cos\alpha|\psi\rangle|00\rangle + i\sin\alpha(\alpha|100\rangle + b|011\rangle\rangle)|11\rangle,$$

Case 1. If we get $|00\rangle$, the first register collapses to $|\psi\rangle_L$, and no correction is needed.

Case 2. If we get $|11\rangle$, the first register collapses to $\alpha|100\rangle + b|011\rangle$ and we may apply correction to recover $|\psi\rangle_L$.

10.2 Phase-Flip QECC

One may consider the phase flip channel $|x\rangle \mapsto Z|x\rangle = (-1)^x|x\rangle$ for $x \in \{0, 1\}$.

One may use the fact that $U_H Z U_H = X$ and adapt the QECC scheme of the bit-flip channel to the phase-flip channel.

One can also use the phase-flip QECC scheme to handle the continuous phase-flip channel

$$|x\rangle \mapsto U_\beta|x\rangle = e^{i\beta Z}|x\rangle \qquad \text{for } x \in \{0, 1\}.$$

The probability of error becomes $P(error) = p \sin^2 \alpha$.

Similar analysis can be done if U_α acts on other qubits.

10.3 Shor's Nine-Qubit Code

Consider $X = \sigma_x, Z = \sigma_z, Y = i\sigma_y = ZX$. They will induce the Bit-Flip, Phase-Flip, and Phase-and-Bit-Flip error on a vector state $|\psi\rangle$.

Every unitary $U \in M_2$ is a linear combination of I, X, Y, Z. If there is a QECC for errors induced by X, Y, Z, then it can be used to correct general error.

Let $|+\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$.

QECC scheme

1. Encode $|\psi\rangle = a|0\rangle + b|1\rangle$ by

$$|\psi\rangle = a|0\rangle + b|1\rangle \to a|000\rangle + b|111\rangle \to\to a|+++\rangle + b|---\rangle = |\psi\rangle_L.$$

2. Transmit the logical quit. The probability of one or no erros is $(1-p)^9 + 9p(1-p)^8 = (1+8p)(1-p)^8$ so that the probability of 2 or more error is

$$1 - (1+8p)(1-p)^2 = 36p^2 + O(p^3),$$

which is small if $p > 0$ is small.

3. Syndrome detection and correction.

   Send in 6 ancillas in the first round to detect Bit-Flip error and apply correction.

   Then send in 2 more ancillas to detect Phase-Flip error and apply correction.

Remark A QECC for error operators I, X, Y, Z corrects every single qubit error.

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 $(n-k) \times n$ parity check matrix H to detect error such that $Hc^t = 0$ if and only if there is no error.
- Moreover, Hc^t will be the syndrome, and used for the correction.
- The set of code words has size 2^k.

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 $Hc^t = \begin{pmatrix} x_4 \oplus x_5 \oplus x_6 \oplus x_7 \\ x_2 \oplus x_3 \oplus x_6 \oplus x_7 \\ x_1 \oplus x_3 \oplus x_5 \oplus x_7 \end{pmatrix}$.

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 2^3 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 $M = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} H \\ \mathbf{1}_{1\times 7} \end{pmatrix}$. 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 $\mathbb{Z}_2^7$:

Seven-Qubits QECC

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

Encoding

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

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

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

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

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

- 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 $|x\rangle_L = |0\rangle_L, |1\rangle_L$.

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.

Five-Qubit QECC

- Suppose n-qubits are used to set up the QECC for one qubit.
- There are $3n$ operators X_i with $0 \le i \le n-1$ single errors to detect.
- So, $3n+1$ vectors in $\mathbb{Z}_2^n$ will be decoded unambiguously as $|0\rangle_L$ and $3n+1$ vectors as $|1\rangle_L$. Hence, $2^n \ge 2(3n+1)$, i.e., $2^{n-1} \ge 3n+1$. Hence, the optimal value is $n=5$.

Let

$$M_0 = X_2X_3Z_1Z_4,\ M_1 = X_3X_4Z_2Z_0,\ M_2 = X_4X_0Z_3Z_1,\ M_3 = X_0X_1Z_4Z_2 \in M_{2^5}.$$

10.5.1 Encoding

Let

$$|0\rangle_L = \frac{1}{4}(I+M_0)(I+M_1)(I+M_2)(I+M_3)|00000\rangle$$

and

$$|1\rangle_L = \frac{1}{4}(I+M_0)(I+M_1)(I+M_2)(I+M_3)|11111\rangle,$$

which is a superposition of 16 basic vectors in $\mathbb{C}^{32}$.

See p.225 and p.227 for the circuit diagram.

10.5.2 Error Syndrome Detection

See (10.70) in p.227 and the circuit diagram in p.228.