Quantum Error Correction

知乎

朵渐贼流形丶

2024.6.28

version: 1.0

An introduction to quantum error-correction 量子纠错

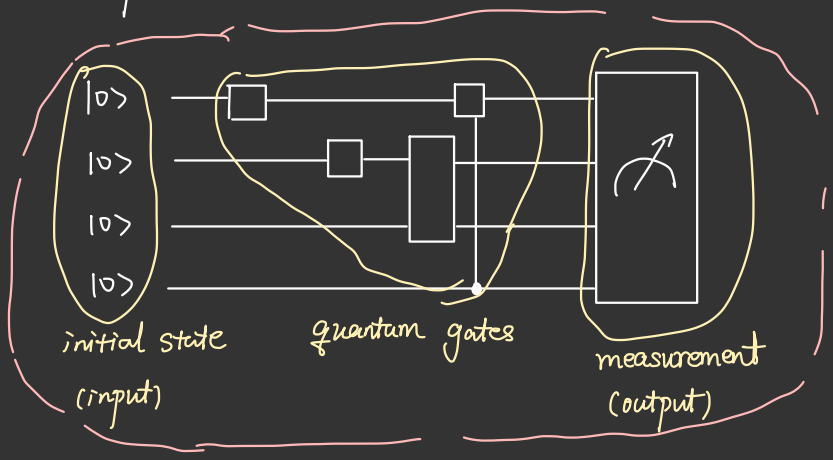
Reference: Nielson. Quantum Computation and Quantum Information Ref. 魏朝晖

Roffe. Quantum Error Correction: An introduction Guide. arXiv: 1907.11157

Outline:

- Background & motivation
- Some relevant properties of quantum information
- The Shor code
- Quantum error-correction conditions
- Stabilizer codes
- Fault-tolerant quantum computation

Quantum computing (QC)



quantum circuit

Single-qubit gates

$$\sigma_0 \equiv I \equiv \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \quad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \quad \sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{pmatrix} & -i \\ i & \end{pmatrix}, \quad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$$

$X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$

$ZX = iY$

$Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$ → phase

- X, Y, Z anti-commute, e.g. $-XZ = ZX$
- X, Y, Z are Hermitian, with eigenvalues 1 and -1

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & \\ & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & \\ & e^{\frac{i\pi}{4}} \end{pmatrix}$$

H → Hadamard gate

Multi-qubit gates

CNOT gate $\mathbb{Z}_2$

$|c\rangle|t\rangle \to |c\rangle|t \oplus c\rangle$

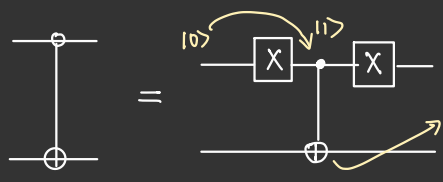
control, target

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}$$

e.g. $|0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle$

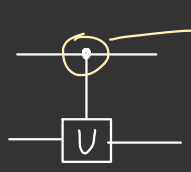
$|1\rangle|0\rangle \longrightarrow |1\rangle|1\rangle$

if $|c\rangle = |1\rangle$, $|t\rangle = \begin{cases} |0\rangle \to |1\rangle \\ |1\rangle \to |0\rangle \end{cases}$



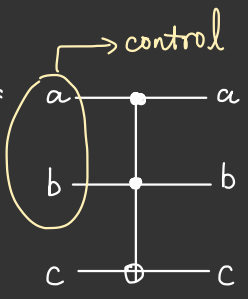
if $|c\rangle = |0\rangle$, $|t\rangle = \begin{cases} |0\rangle \longrightarrow |1\rangle \\ |1\rangle \longrightarrow |0\rangle \end{cases}$

Controlled-U gate : $|c\rangle|t\rangle \longrightarrow |c\rangle U^c|t\rangle$



if $|c\rangle = |1\rangle$, $|t\rangle \longrightarrow U|t\rangle$

Toffoli gate:



if $|a\rangle = |b\rangle = |1\rangle$, $|c\rangle \longrightarrow |c \oplus ab\rangle$

$\mathbb{Z}_2$, e.g. $1+1=0$

Foundamental difficulties in QC

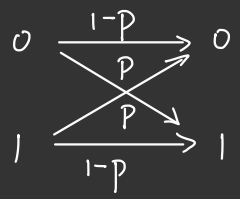
Size is too small. (Quantum information is extremely fragile)

↳ Requirement of quantum error corrections. (QEC)

Classical error correction

Redundancy

e.g. $0 \longrightarrow 000$, $1 \longrightarrow 111$ the noise flips the bit with probability $p>0$



Majority voting, e.g. $0\,0\,0 \Rightarrow 1\,0\,1$, $1\,1\,0$, $1\,1\,1$ ..... (p^3 p^2 p^2)

$\Rightarrow P_{failure} = 3p^2 - 2p^3$, two or more flips.

- If $p < \frac{1}{2}$, $\boxed{P_{failure} < p}$ ✓

QEC is challenging

- No cloning
- Quantum measurments destroy quantum information
- Errors are continuous.

But QEC is still possible

No-cloning theorem (1982)

e.g. $|0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle$, $|1\rangle|0\rangle \longrightarrow |1\rangle|1\rangle$ ← This can be implemented by CNOT gate. ✓

However $(|0\rangle+|1\rangle)|0\rangle \longrightarrow |0\rangle|0\rangle+|1\rangle|1\rangle \neq (|0\rangle+|1\rangle)(|0\rangle+|1\rangle)$ ✗

Quantum measurement ⟶ intrinsically random ⟶ also helpful

Two quantum states that are not orthogonal cannot be distinguished perfectly.

observable $M=\sum_m m P_m$ → projector, $\sum_m P_m = I$

$|\psi\rangle$, result m: $p(m)=\langle\psi|P_m|\psi\rangle$

After measurement: $|\psi\rangle \longrightarrow \frac{P_m|\psi\rangle}{\sqrt{p(m)}}$ → normalize coefficient

e.g. $|\psi\rangle=|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$

Observable $Z=|0\rangle\langle 0|-|1\rangle\langle 1| \Rightarrow p(1)=p(-1)=\frac{1}{2}$

$X=|+\rangle\langle +|-|-\rangle\langle -| \Rightarrow p(1)=1,\ p(-1)=0$

The operator-sum representation: $\mathcal{E}(\rho)=\sum_k E_k \rho E_k^\dagger$, where $\sum_k E_k^\dagger E_k = I$

Quantum noises can be described as quantum operations, which are continuous.

e.g. Depolarizing noise: $\mathcal{E}(\rho)=(1-p)\rho+\frac{p}{3}(X\rho X+Y\rho Y+Z\rho Z)$

Theorem: (Unitary freedom in the operator-sum representation)

$\mathcal{E}(\rho)=\sum_{k=1}^{m} E_k \rho E_k^\dagger=\sum_{j=1}^{n} F_j \rho F_j^\dagger$, (if $n<m \Rightarrow$ Let $\{F_1,\cdots,F_n\} \longrightarrow \{F_1,\cdots,F_n,\underbrace{0,0,\cdots 0}_{m-n}\}$)

Then $\mathcal{E}=\mathcal{F}$. There exist complex numbers u_{ij} such that $E_i=\sum_j u_{ij} F_j$, $(u_{ij})_{m\times m}$ is unitary.

Theorem: (Polar decomposition)

Let A be a linear operator on a vector space V. There exists unitary U and positive operators J and K such that $A=UJ=KU$ where $J\equiv\sqrt{A^\dagger A}$, $K\equiv\sqrt{AA^\dagger}$.

Moreover, if A is invertible then U is unique.

E.g. bit flip code

bit flip channel: $|\psi\rangle$ → p → $X|\psi\rangle$, $|\psi\rangle=a|0\rangle+b|1\rangle \longrightarrow a|1\rangle+b|0\rangle$

$|\psi\rangle$ → $1-p$ → $|\psi\rangle$

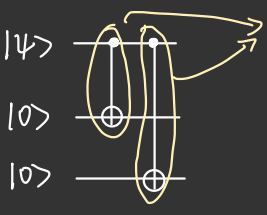
Encoding: $|0\rangle \longrightarrow |0_L\rangle \equiv |000\rangle$

$|1\rangle \longrightarrow |1_L\rangle \equiv |111\rangle$

$|\psi\rangle = a|0\rangle + b|1\rangle \longrightarrow a|000\rangle + b|111\rangle$

(redundancy without cloning)

Encoding circuit: $|\psi\rangle$, $|0\rangle$, $|0\rangle$ — CNOT gates



$M = \sum_i i P_i$, $\sum_i P_i = I$ error-detection / syndrome diagnosis → recover initial state

$P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111|$ no error

$P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011|$ bit flip on qubit one

$P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101|$ bit flip on qubit two

$P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110|$ bit flip on qubit three

A different way:

Measurement $\xrightarrow{①} Z_1Z_2\,(Z\otimes Z\otimes I) \xrightarrow{②} Z_2Z_3$

$$Z_1Z_2 = \left(|00\rangle\langle 00| + |11\rangle\langle 11|\right)\otimes I - \left(|01\rangle\langle 01| + |10\rangle\langle 10|\right)\otimes I$$

Compare the sign of qubits one and two

Similarly, Z_2Z_3 compare the sign of qubits two and three.

E.g. phase flip code

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

phase flip channel: $|\psi\rangle$ — p → $Z|\psi\rangle$; $1-p$ → $|\psi\rangle$

$Z|+\rangle = |-\rangle$, $Z|-\rangle = |+\rangle$

⇒ Encoding $|0_L\rangle \equiv |+++\rangle$, $|1_L\rangle \equiv |---\rangle$

⇒ The same as the bit flip channel.

Conjugated by Hadamard gates

Measurement (Detect) $\xrightarrow{①} H^{\otimes 3} Z_1Z_2 H^{\otimes 3} = X_1X_2 \xrightarrow{②} H^{\otimes 3} Z_2Z_3 H^{\otimes 3} = X_2X_3 \longrightarrow$ Recover

↓ Compare the sign of qubits one and two

↓ Compare the sign of qubits two and three

$$X_1X_2 = \left(|++\rangle\langle ++| + |--\rangle\langle --|\right)\otimes I - \left(|+-\rangle\langle +-| + |-+\rangle\langle -+|\right)\otimes I$$

The Shor code

$$|0_L\rangle \equiv |+++\rangle = \frac{(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)}{2\sqrt{2}}$$

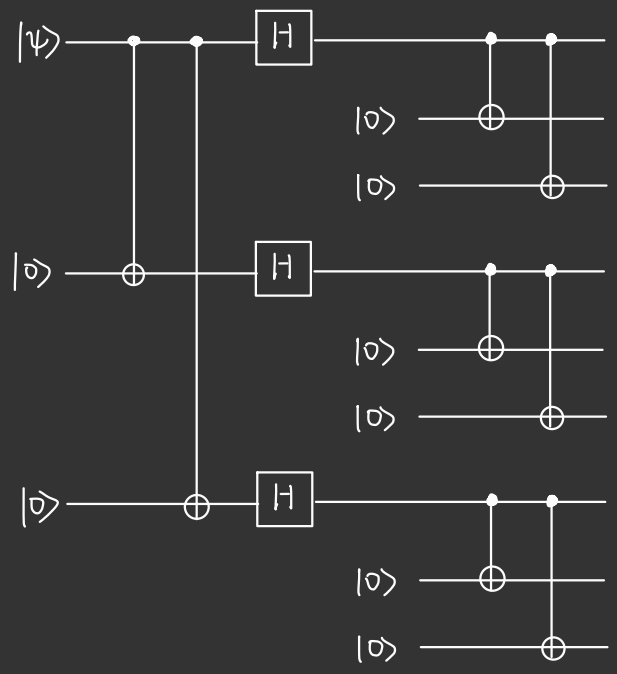
Combine the three qubit phase flip and bit flip codes

$$|0\rangle \longrightarrow |0_L\rangle \equiv \frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$|1\rangle \longrightarrow |1_L\rangle \equiv \frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

$|1_L\rangle \equiv |---\rangle$

concatenation



- Suppose a bit flip occurs on the first qubit. $\xrightarrow{\text{Measure}} Z_1Z_2$
- Suppose a phase flip occurs on the first qubit. $\xrightarrow{\text{Measure}} X_1X_2X_3X_4X_5X_6$
- Suppose both bit and phase flip errors occurs on the first qubit. $\xrightarrow{\text{Recover}} Z_1X_1$

If only one single qubit is polluted, the Shor code can correct completely arbitrary errors.

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger, \quad E_i = e_{i0} I + e_{i1} X_1 + e_{i2} Z_1 + e_{i3} X_1 Z_1$$

$\Rightarrow E_i|\psi\rangle \to \#|\psi\rangle + \# X_1|\psi\rangle + \# Z_1|\psi\rangle + \# X_1Z_1|\psi\rangle$ linear superposition

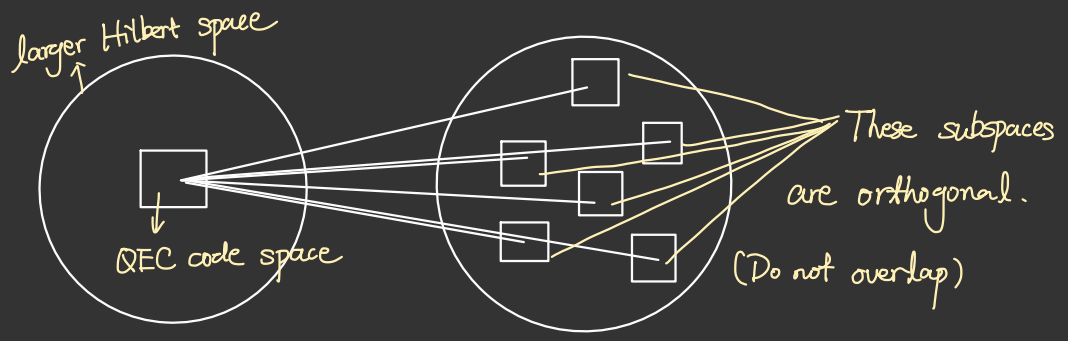
$\Rightarrow$ from which the original state can be recovered.

Foundamental and deep fact about QEC:

Continuous errors can be corrected by correcting just a discrete set of errors, where the key idea is to discretize continuous errors.

General theory of QEC

- Quantum states are encoded into a quantum error-correcting code, formally defined as a subspace C of some larger Hilbert space.
- After the code is subjected to noise, a syndrome measurement is performed to diagnose the type of error which occured - the error syndrome.
- Once this has been determined, a recovery operation is performed, to return the quantum system to the original state of the code.



Requirements:

- Different error syndromes correspond to orthogonal subspaces of the total Hilbert space.
- Different subspaces must be undeformed versions of the original code space — must take the orthogonal codewords to orthogonal states.

$$(\mathcal{R} \circ \mathcal{E})(\rho) = \rho$$

$\mathcal{R}$: error-correction, $\mathcal{E}$: noise

Theorem: (Quantum error-correction conditions)

C: quantum code, P: projector onto C. (General)

A necessary and sufficient condition for the existence of an error-correction operation $\mathcal{R}$ correcting $\mathcal{E}$ on C is that

$$P E_i^\dagger E_j P = \alpha_{ij} P, \quad (\alpha_{ij}) \text{ is Hermitian } (\alpha_{ij} = \alpha_{ji}^*)$$

Moreover, $\mathcal{F}$ with operation elements $\{F_j\}$ what are linear combinations of the E_i (i.e. $F_j = \sum_i m_{ji} E_i$) $\Rightarrow$ $\mathcal{R}$ also corrects noise $\mathcal{F}$ on the code C.

With the above theorem, we can directly talk about a set of error operators (or simply errors) $\{E_i\}$ which are correctable.

$\Rightarrow$ Any noise whose operation elements are built from linear combinations of $\{E_i\}$ will be corrected by the recovery operation R

E.g. the Shor code

$\{E_i\}$ $\xrightarrow{\text{linear combination}}$ $\sigma_0, \sigma_1, \sigma_2, \sigma_3$ (I, X, Y, Z)

$\xrightarrow{\text{Verify}}$ $P\sigma_i\sigma_j P = \alpha_{ij} P$ Exercise! △

Stabilizer codes

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

$\Rightarrow X_1X_2|\psi\rangle = |\psi\rangle$, $Z_1Z_2|\psi\rangle = |\psi\rangle$ $\Rightarrow$ $|\psi\rangle$ is stabilized by X_1X_2 and Z_1Z_2

Interestingly, it can be proved that (up to a global phase) only this state is stabilized by X_1X_2 and Z_1Z_2

Consider $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$

- $X_1X_2|\psi\rangle = |\psi\rangle \Rightarrow a=d,\ b=c$
- $Z_1Z_2|\psi\rangle = |\psi\rangle \Rightarrow b=c=0$

$\Rightarrow |\psi\rangle = e^{i\theta}\frac{|00\rangle + |11\rangle}{2}$ ($e^{i\theta}$: global phase)

(Surface codes are stabilizer codes)

Many quantum states can be more easily described by working with the operators that stabilize them.

Many quantum codes can be much more compactly described using stabilizers than state vector description.

Errors and operations on the qubit can be potentially described using the stabilizer formalism.

Pauli group for a single qubit: $G_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$

for n qubits: $G_n = \underbrace{G_1 \otimes G_1 \otimes \cdots \otimes G_1}_{n \text{ copies}}$

Suppose S is a subgroup of G_n. V_S is the set of n-qubit states that are fixed by every element of S (linear space)

- V_S is stabilized by S.
- S is said to be a stabilizer of the space V_S.

e.g. $S \equiv \{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\} \leq G_3$ (notation of subgroup)

- The subspace fixed by Z_1Z_2 is spanned by $|000\rangle$, $|001\rangle$, $|110\rangle$ and $|111\rangle$
- ——— Z_2Z_3 ——— $|000\rangle$, $|100\rangle$, $|011\rangle$ and $|111\rangle$
- $\Rightarrow V_S$ is the subspace spanned by $|000\rangle$ and $|111\rangle$

$S = \langle Z_1Z_2, Z_2Z_3 \rangle$ (generators of S)

To see that a particular vector is stabilized by S, we need only check that the vector is stabilized by the generators.

Moreover, if V_S is a nontrivial vector space.

- The elements of S commute
- $-I$ is not an element of S

} They are also sufficient.

Independence: $g_1 \cdots g_L$ are independent if $\langle g_1 \cdots g_{i-1} g_{i+1} \cdots g_L \rangle \neq \langle g_1 \cdots g_L \rangle$ (remove g_i)

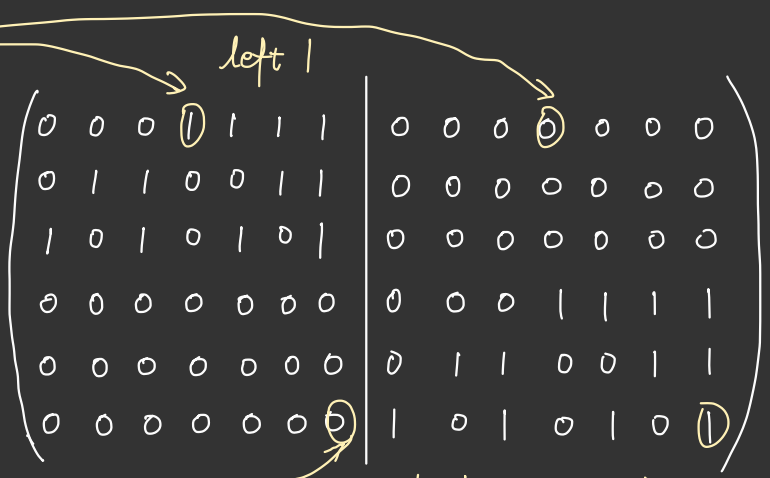
- X: left |
- Z: right |

Each row represents one generator

- Y: both sides |

e.g.

g_1	I	I	I	X	X	X	X
g_2	I	X	X	I	I	X	X
g_3	X	I	X	I	X	I	X
g_4	I	I	I	Z	Z	Z	Z
g_5	I	Z	Z	I	I	Z	Z
g_6	Z	I	Z	I	Z	I	Z



Check matrix

Let $\Lambda = \begin{pmatrix} & I \\ I & \end{pmatrix}$.

Two elements g and g' commute if and only if $r(g)\Lambda r(g')^T = 0$.

Proposition: $S = \langle g_1, \cdots, g_l \rangle$ and $-I \notin S$. The generators $g_1 \cdots g_l$ are indepent if and only if the rows of the corresponding check matrix are linearly independent.

Key observation: $r(g) + r(g') = r(gg')$

Propsition: $S = \langle g_1 \cdots g_l \rangle$ and $-I \notin S$, $g_1 \cdots g_l$ are independent. Fix i in the range $1, \cdots, l$. Then there exists $g \in G_n$ such that $g g_i g^\dagger = -g_i$ and $g g_j g^\dagger = g_j$ for all $j \neq i$.

Note that any two elements of G_n can only commute or anti-commute.

Proposition: $S = \langle g_1, \cdots g_{n-k} \rangle$ and $-I \notin S$, $g_1 \cdots g_{n-k}$ are independent and commute. Then V_S is a 2^k-dimensional vector space.

Let $x = (x_1, \cdots, x_{n-k})$ be a vector of $n-k$ elements of Z_2. Define

completeness $$P_S^x \equiv \prod_{j=1}^{n-k} \frac{I + (-1)^{x_j} g_j}{2}$$ orthogonality

Then $P_S^{(0,\cdots,0)} = V_S$, $I = \sum_x P_S^x$. And if $x \neq x'$, then $P_S^x \cdot P_S^{x'} = 0$.

Furthermore, there exists a g_x such that $g_x P_S^{(0,\cdots,0)} (g_x)^\dagger = P_S^x$.

Suppose V_S is stabilized by S. Let $|\psi\rangle \in V_S$. Then

$$U|\psi\rangle = Ug|\psi\rangle = (UgU^\dagger)(U|\psi\rangle)$$

e.g. H gate: $HXH^\dagger = Z$, $HYH^\dagger = -Y$, $HZH^\dagger = X$

C-NOT gate (denoted U): $UX_1U^\dagger = X_1X_2$, $UX_2U^\dagger = X_2$, $UZ_1U^\dagger = Z_1$, $UZ_2U^\dagger = Z_1Z_2$

Similarly, for measurement $g \in G_n$, the resulting state can also described by stabilizers. Suppose $|\psi\rangle$ is a state with stabilizer $\langle g_1, \cdots, g_n \rangle$ and if g commutes with all the generators of the stabilizer

- $g_j g|\psi\rangle = g g_j|\psi\rangle = g|\psi\rangle$
- $g|\psi\rangle$ is in the stabilized space.
- Since $g^2 = I$, $g|\psi\rangle = \pm|\psi\rangle$ $\Rightarrow$ outcome is deterministic.

measurement does not disturb the state.

Suppose g anti-commutes with g_1 and commutes with others.

$p(+1) = \mathrm{Tr}\left[\frac{I+g}{2}|\psi\rangle\langle\psi|\right]$

$p(-1) = \mathrm{Tr}\left[\frac{I-g}{2}|\psi\rangle\langle\psi|\right]$

$g_1|\psi\rangle = |\psi\rangle$

$\Rightarrow p(+1) = \mathrm{Tr}\left[\frac{I+g}{2} g_1|\psi\rangle\langle\psi|\right] = \mathrm{Tr}\left[g_1 \frac{I-g}{2}|\psi\rangle\langle\psi|\right] = \mathrm{Tr}\left[\frac{I-g}{2}|\psi\rangle\langle\psi|\right] = p(-1)$

$\Rightarrow p(+1) = p(-1) = \frac{1}{2}$

If the result is 1, the new state is $|\psi^+\rangle = \frac{I+g}{\sqrt{2}}|\psi\rangle$, which is stabilized by $(g, g_2, \cdots, g_n)$

——— -1, ——— $|\psi^-\rangle = \frac{I-g}{\sqrt{2}}|\psi\rangle$, ——— $(-g, g_2, \cdots, g_n)$

How to design an $[n, k]$ stabilizer code $C(S)$: (n qubit, subspace 2^k)

- Find $S \leq G_n$ such that $-I \notin S$ and $S = \langle g_1, \cdots, g_{n-k}\rangle$ where $g_1 \cdots g_{n-k}$ are independent and commuting.
- Choose $\bar{Z}_1 \cdots \bar{Z}_k \in G_n$ such that $g_1 \cdots g_{n-k} \bar{Z}_1 \cdots \bar{Z}_k$ forms an independent and commuting set.
- $|x_1, \cdots x_k\rangle_L$ is the state with stabilizers $\langle g_1, \cdots g_{n-k}, (-1)^{x_1}\bar{Z}_1, \cdots, (-1)^{x_k}\bar{Z}_k\rangle$
- $\bar{X}_j \bar{Z}_j = -\bar{Z}_j \bar{X}_j$ determines $\bar{X}_j$

Suppose $C(S)$ is a stabilizer code corrupted by an error $E \in G_n$.

- If E anti-commute with an element of the stabilizer, then E takes $C(S)$ to an orthogonal subspace, which can be detected.
- If $E \in S$, then the error does not corrupt the state at all. $E|\psi\rangle = |\psi\rangle$
- Danger! If E commutes with all elements of S and $E \notin S$.

Define $N(S) = \{E \mid E \in G_n, EgE^\dagger \in S \text{ for all } g \in S\}$

Theorem: Error-correction conditions for stabilizer codes

Let S be the stabilizer for a stabilizer code $C(S)$. Suppose $\{E_j\}$ is a set of operators in G_n such that $E_j^\dagger E_k \notin N(S) - S$ for all j and k. Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.

Distance of a stabilizer code $C(S)$: the minimum weight of an element of $N(S) - S$.

If $C(S)$ is an $[n,k]$ code with distance d then we say that $C(S)$ is an $[n,k,d]$ stabilizer code.

E.g. the Shor code

g_1	Z	Z	I	I	I	I	I	I	I
g_2	I	Z	Z	I	I	I	I	I	I
g_3	I	I	I	Z	Z	I	I	I	I
g_4	I	I	I	I	Z	Z	I	I	I
g_5	I	I	I	I	I	I	Z	Z	I
g_6	I	I	I	I	I	I	I	Z	Z
g_7	X	X	X	X	X	X	I	I	I
g_8	I	I	I	X	X	X	X	X	X
$\bar{Z}$	X	X	X	X	X	X	X	X	X
$\bar{X}$	Z	Z	Z	Z	Z	Z	Z	Z	Z

$n=9,\ k=1$

$$|0\rangle \to |0_L\rangle \equiv \frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$|1\rangle \to |1_L\rangle \equiv \frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

X_1X_4 anti-commutes with Z_1Z_2, thus is not in $N(S)$.

Fault-tolerant quantum computation

- Replace each qubit in the quantum circuit with an encoded block of qubits, using an error-correcting code.
- Perform an encoded gate acting on the encoded state.
- By performing error-correction periodically on the encoded state we prevent accumulation of errors in the state. For example, each time the first order is removed.
- Any failure anywhere during the procedure for performing the encoded gate can only propogate to a small number of qubits in each block of the encoded data, which is called fault-tolerant.
- Error-correction itself can introduce errors, so it cannot introduce too many errors into the encoded data.

To reduce the effective error rate:

e.g. Actually failure probability p $\xrightarrow{\text{1st level}}$ cp^2 $\xrightarrow{\text{2nd level}}$ $c(cp^2)^2$ $\xrightarrow{\text{k-th level}}$ $\frac{(cp)^{2^k}}{c}$

(cp^2: coefficient)

Suppose the circuit size is $p(n)$, and the accuracy we need is ϵ. Then

$$\frac{(cp)^{2^k}}{c} \leq \frac{\epsilon}{p(n)}$$

- If $p \leq p_{th} \equiv \frac{1}{c} \Rightarrow pc < 1$, k can be found $\Longrightarrow$ p_{th} is threshold
- The encoded circuit has size $O(\text{poly}(\log \frac{p(n)}{\epsilon}) p(n))$

Surface code – the most realistic choice for QEC

Advantage:

- High threshold 1%
- Easy to implement: a simple two-dimensional physical layout with only nearest-neighbor coupling (generally it is hard to perform high-fidelity long-range interactions)

Disadvantage:

- A reasonable fault-tolerant logical qubit in a surface code takes of order $10^3 \sim 10^4$ physical qubits.

Quantum error mitigation (QEM) ← Another way.

- Compared with QEC, the cost is much lower.
- But for general general quantum algorithms, this is a temporary solution.
- Two typical methods: extrapolation & quasi-probability