量子信息与量子计算

高健硕

量子力学讨论班

2026 年 6 月 10 日

参考 Lukin 和袁骁老师讲义

量子信息的三类技术

量子精密测量	量子通信	量子计算
用相干叠加和纠缠提高参数估计精度。例如 GHZ 态中相位变成 $N\phi$，理想灵敏度可从 $1/\sqrt{N}$ 改到 $1/N$。	未知量子态不能克隆，非正交态不能完美区分。窃听会引入扰动，纠缠还能支持 teleportation 和 dense coding。	把计算写成幺正演化，通过 phase kickback、QFT、amplitude amplification 等方法提取全局结构。

量子态、测量和开放系统

纯态、bra-ket 和内积

d 维 Hilbert 空间中的纯态写作

$$|\psi\rangle = \sum_{k=1}^{d} a_k |k\rangle, \qquad \langle\psi| = \sum_{k=1}^{d} a_k^* \langle k|, \qquad \langle\psi|\psi\rangle = \sum_k |a_k|^2 = 1.$$

两个态的内积是一个复数：

$$\langle\phi|\psi\rangle = \sum_{k=1}^{d} c_k^* a_k, \qquad |\langle\phi|\psi\rangle| \leq 1.$$

一个 rank-1 算符可以写作外积：

$$A = |\phi\rangle\langle\psi|, \qquad A|\chi\rangle = |\phi\rangle\langle\psi|\chi\rangle.$$

观测量和投影测量

观测量 $A = A^\dagger$ 可谱分解为

$$A = \sum_n a_n P_n, \qquad P_n = |n\rangle \langle n|, \qquad P_n P_m = \delta_{nm} P_n, \qquad \sum_n P_n = \mathbb{I}.$$

若系统处于 $|\psi\rangle$，测量 A 时得到 a_n 的概率为

$$p_n = \langle\psi| P_n |\psi\rangle = |\langle n|\psi\rangle|^2.$$

测后态为

$$|\psi\rangle \longmapsto \frac{P_n |\psi\rangle}{\sqrt{p_n}}.$$

期望值来自重复制备-测量：

$$\langle A\rangle = \langle\psi| A |\psi\rangle = \sum_n a_n \langle\psi| P_n |\psi\rangle = \sum_n a_n p_n.$$

幺正演化：Schrödinger 方程的解

封闭系统满足

$$\mathrm{i}\hbar\frac{\mathrm{d}}{\mathrm{d}t}\left|\psi(t)\right\rangle = H\left|\psi(t)\right\rangle .$$

若 H 不显含时间，解为

$$\left|\psi(t)\right\rangle = U(t)\left|\psi(0)\right\rangle , \qquad U(t) = \exp\left(-\frac{\mathrm{i}Ht}{\hbar}\right) .$$

矩阵指数定义为

$$\mathrm{e}^{A} = \sum_{n=0}^{\infty}\frac{A^n}{n!}.$$

若 $H = H^\dagger$，则

$$U^\dagger U = \mathrm{e}^{\mathrm{i}Ht/\hbar}\mathrm{e}^{-\mathrm{i}Ht/\hbar} = \mathbb{I},$$

所以范数守恒：

$$\langle\psi(t)|\psi(t)\rangle = \langle\psi(0)|\, U^\dagger U\,|\psi(0)\rangle = 1.$$

量子比特和 Bloch 球

一般单量子比特:

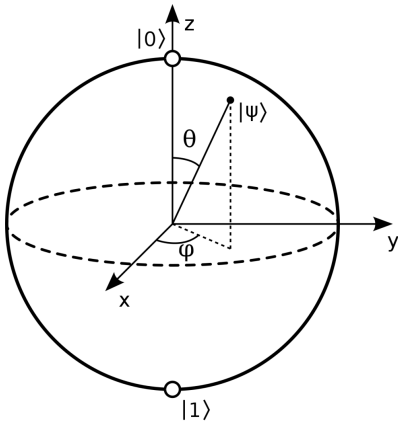
$$|\psi\rangle = c_0\,|0\rangle + c_1\,|1\rangle\,, \qquad |c_0|^2 + |c_1|^2 = 1.$$

去掉整体相位后:

$$|\psi(\theta,\phi)\rangle = \cos\frac{\theta}{2}\,|0\rangle + \mathrm{e}^{\mathrm{i}\phi}\sin\frac{\theta}{2}\,|1\rangle\,.$$

测 Z 基时

$$p(0) = \cos^2\frac{\theta}{2}, \qquad p(1) = \sin^2\frac{\theta}{2}.$$



Bloch 球示意

Pauli 矩阵和本征基

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

代数性质

$$\sigma_\alpha^2 = \mathbb{I}, \quad \mathrm{Tr}\,\sigma_\alpha = 0, \quad [\sigma_\alpha, \sigma_\beta] = 2\mathrm{i}\epsilon_{\alpha\beta\gamma}\sigma_\gamma.$$

$$\sigma_\alpha\sigma_\beta = \delta_{\alpha\beta}\mathbb{I} + \mathrm{i}\epsilon_{\alpha\beta\gamma}\sigma_\gamma.$$

本征态

$$Z: \ |0\rangle, |1\rangle;$$

$$X: \ |\pm x\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}};$$

$$Y: \ |\pm y\rangle = \frac{|0\rangle \pm \mathrm{i}\,|1\rangle}{\sqrt{2}}.$$

单量子比特 Hamiltonian 的指数

单比特 Hamiltonian 为

$$H = \frac{\hbar}{2}\sum_{i=1}^{3} h_i\sigma_i \equiv \frac{\hbar\omega}{2}\,\hat{n}\cdot\boldsymbol{\sigma}, \qquad \omega = \sqrt{h_1^2+h_2^2+h_3^2}, \quad \hat{n} = \frac{\boldsymbol{h}}{\omega}.$$

利用恒等式

$$(\hat{n}\cdot\boldsymbol{\sigma})^2 = \sum_{ij} n_i n_j \sigma_i\sigma_j = \sum_i n_i^2\mathbb{I} + \mathrm{i}\sum_{ij} n_i n_j \epsilon_{ijk}\sigma_k = \mathbb{I}.$$

因此

$$\begin{aligned} U(t) &= \exp\left[-\mathrm{i}\frac{\omega t}{2}\hat{n}\cdot\boldsymbol{\sigma}\right] \\ &= \cos\frac{\omega t}{2}\,\mathbb{I} - \mathrm{i}\sin\frac{\omega t}{2}\,\hat{n}\cdot\boldsymbol{\sigma}. \end{aligned}$$

绕 z 轴进动：相对相位变化

取 $\hat{n}=\hat{z}$，则

$$U_z(t)=\cos\frac{\omega t}{2}\mathbb{I}-\mathrm{i}\sin\frac{\omega t}{2}Z=\begin{pmatrix}\mathrm{e}^{-\mathrm{i}\omega t/2} & 0\\ 0 & \mathrm{e}^{\mathrm{i}\omega t/2}\end{pmatrix}.$$

作用在

$$|\psi(0)\rangle=\cos\frac{\theta}{2}|0\rangle+\mathrm{e}^{\mathrm{i}\phi}\sin\frac{\theta}{2}|1\rangle$$

上，得到

$$|\psi(t)\rangle=\mathrm{e}^{-\mathrm{i}\omega t/2}\left(\cos\frac{\theta}{2}|0\rangle+\mathrm{e}^{\mathrm{i}(\phi+\omega t)}\sin\frac{\theta}{2}|1\rangle\right).$$

整体相位 $\mathrm{e}^{-\mathrm{i}\omega t/2}$ 不可观测；可观测的是相对相位 $\phi\mapsto\phi+\omega t$。

概率幅方程和 Rabi oscillation

令

$$|\psi(t)\rangle = a_0(t)\,|0\rangle + a_1(t)\,|1\rangle\,, \qquad H = \frac{\hbar}{2}(h_1 X + h_2 Y + h_3 Z).$$

代入 Schrödinger 方程，得到

$$\begin{cases} \mathrm{i}\dot{a}_0 = \dfrac{h_3}{2}a_0 + \dfrac{h_1 - \mathrm{i}h_2}{2}a_1, \\ \mathrm{i}\dot{a}_1 = -\dfrac{h_3}{2}a_1 + \dfrac{h_1 + \mathrm{i}h_2}{2}a_0. \end{cases}$$

共振驱动时

$$\Omega \equiv \frac{h_1 - \mathrm{i}h_2}{2}, \qquad h_3 = 0.$$

若 Ω 实且初态 $|0\rangle$，则

$$a_0(t) = \cos(|\Omega|t), \qquad a_1(t) = -\mathrm{i}\sin(|\Omega|t),$$

所以

$$P_1(t) = |a_1(t)|^2 = \sin^2(|\Omega|t).$$

脉冲面积和旋转参考系

若 Rabi 频率随时间变为 $\Omega(t)$，在相位固定且近似共振时，态翻转由脉冲面积决定：

$$\Theta = \int \Omega(t)\,\mathrm{d}t.$$

典型地

$$\Theta = \frac{\pi}{4}:\ |0\rangle \mapsto \frac{|0\rangle - \mathrm{i}\,|1\rangle}{\sqrt{2}}, \qquad \Theta = \frac{\pi}{2}:\ |0\rangle \mapsto -\mathrm{i}\,|1\rangle\,.$$

若驱动项带相位 $\Omega_0 \mathrm{e}^{\mathrm{i}\nu t}$，可作旋转参考系变换

$$a_0 = \tilde{a}_0 \mathrm{e}^{\mathrm{i}\nu t/2}, \qquad a_1 = \tilde{a}_1 \mathrm{e}^{-\mathrm{i}\nu t/2},$$

等价于

$$U_{\mathrm{rot}} = \mathrm{e}^{\mathrm{i}\nu t Z/2}.$$

当 $\nu \simeq h_3$ 时，快振荡被消去，能级之间发生有效 Rabi 振荡。

常用量子门都可以看成旋转

$$R_\alpha(\theta) = \exp\left(-\mathrm{i}\frac{\theta}{2}\sigma_\alpha\right).$$

例如

$$R_x(\pi) = -\mathrm{i}X, \qquad R_z(\pi) = -\mathrm{i}Z.$$

Hadamard 门可以写成绕 $(\hat{x}+\hat{z})/\sqrt{2}$ 的 π 旋转，差一个整体相位：

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \qquad H^2 = \mathbb{I}.$$

它把计算基和 X 基互相转换：

$$H|0\rangle = |+\rangle, \quad H|1\rangle = |-\rangle, \qquad HZH = X, \quad HXH = Z.$$

要点

后面的算法几乎都反复用 H：制备均匀叠加，或者把相位差转换成测量概率。

复合系统和张量积

若系统 A, B 的 Hilbert 空间维数分别为 d_A, d_B，则

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B, \qquad \dim \mathcal{H}_{AB} = d_A d_B.$$

若

$$|\phi\rangle_A = \begin{pmatrix} a \\ b \end{pmatrix}, \qquad |\chi\rangle_B = \begin{pmatrix} c \\ d \end{pmatrix},$$

则

$$|\phi\rangle_A \otimes |\chi\rangle_B = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}.$$

n 个量子比特的一般纯态：

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} a_x |x\rangle, \qquad \sum_x |a_x|^2 = 1.$$

Bell 态

四个 Bell 态：

$$\left|\Phi^{\pm}\right\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \qquad \left|\Psi^{\pm}\right\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}.$$

它们构成正交归一基。例如

$$\left\langle\Phi^{+}\middle|\Phi^{-}\right\rangle = \frac{1}{2}(\langle 00| + \langle 11|)(|00\rangle - |11\rangle) = 0.$$

但 $\left|\Phi^{+}\right\rangle$ 不能写成 $|\phi\rangle_A |\chi\rangle_B$。若假设

$$(a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle,$$

要等于 $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$，需 $ad = bc = 0$ 且 $ac, bd \neq 0$，矛盾。

密度矩阵：从纠缠态看子系统

考虑

$$|\psi\rangle_{AB} = a\,|0\rangle_A\,|0\rangle_B + b\,|1\rangle_A\,|1\rangle_B\,, \qquad |a|^2 + |b|^2 = 1.$$

只测 A 上的观测量 M_A：

$$\begin{aligned}\langle M_A \otimes \mathbb{I}_B\rangle &= \langle\psi|\, M_A \otimes \mathbb{I}_B\,|\psi\rangle \\ &= |a|^2\,\langle 0|\, M_A\,|0\rangle + |b|^2\,\langle 1|\, M_A\,|1\rangle \\ &= \mathrm{Tr}_A(M_A\rho_A),\end{aligned}$$

其中

$$\rho_A = |a|^2\,|0\rangle\langle 0| + |b|^2\,|1\rangle\langle 1|\,.$$

对 Bell 态 $|a|^2 = |b|^2 = 1/2$，所以

$$\rho_A = \frac{1}{2}\mathbb{I},$$

局域完全混合，但整体 AB 是纯态。

偏迹的显式推导

令总态

$$|\psi\rangle_{AB} = \sum_{i,\mu} a_{i\mu} \, |i\rangle_A \, |\mu\rangle_B \, , \qquad \rho_{AB} = |\psi\rangle\langle\psi|_{AB} \, .$$

对 A 上任意算符 M_A，有

$$\begin{aligned} \langle M_A \rangle &= \sum_{j,\nu,i,\mu} a^*_{j\nu} a_{i\mu} \, \langle j| \langle \nu| \left(M_A \otimes \mathbb{I}_B \right) |i\rangle \, |\mu\rangle \\ &= \sum_{i,j,\mu} a^*_{j\mu} a_{i\mu} \, \langle j| \, M_A \, |i\rangle \, . \end{aligned}$$

这等于 $\mathrm{Tr}_A(M_A \rho_A)$，其中

$$\rho_A = \mathrm{Tr}_B \, \rho_{AB} = \sum_{i,j,\mu} a_{i\mu} a^*_{j\mu} \, |i\rangle \, \langle j| \, .$$

矩阵元为

$$(\rho_A)_{ij} = \sum_{\mu} a_{i\mu} a^*_{j\mu} .$$

单量子比特密度矩阵和纯度

任意单量子比特密度矩阵可写成

$$\rho = \frac{1}{2}(\mathbb{I} + \boldsymbol{P}\cdot\boldsymbol{\sigma}) = \frac{1}{2}\begin{pmatrix} 1+P_z & P_x - \mathrm{i}P_y \\ P_x + \mathrm{i}P_y & 1-P_z \end{pmatrix}.$$

正定性给出

$$\det\rho = \frac{1}{4}(1-|\boldsymbol{P}|^2) \geq 0, \qquad |\boldsymbol{P}| \leq 1.$$

纯度为

$$\begin{aligned} \mathrm{Tr}\,\rho^2 &= \frac{1}{4}\,\mathrm{Tr}\,(\mathbb{I} + 2\boldsymbol{P}\cdot\boldsymbol{\sigma} + P_iP_j\sigma_i\sigma_j) \\ &= \frac{1}{2}(1+|\boldsymbol{P}|^2). \end{aligned}$$

因此

$$|\boldsymbol{P}| = 1 \Longleftrightarrow \rho \text{ 为纯态}, \qquad |\boldsymbol{P}| = 0 \Longleftrightarrow \rho = \mathbb{I}/2.$$

从总系统幺正演化到 Kraus 表示

设初态可写成

$$\rho_{AB} = \rho_A \otimes |E\rangle\langle E|_B .$$

总系统演化：

$$\rho'_{AB} = U_{AB}(\rho_A \otimes |E\rangle\langle E|)U_{AB}^{\dagger}.$$

只看 A：

$$\rho'_A = \mathrm{Tr}_B\, \rho'_{AB} = \sum_{\mu} \langle\mu|\, U_{AB}\, |E\rangle\, \rho_A\, \langle E|\, U_{AB}^{\dagger}\, |\mu\rangle .$$

定义

$$M_\mu = \langle\mu|\, U_{AB}\, |E\rangle ,$$

得到 Kraus operator-sum representation：

$$\rho'_A = \sum_{\mu} M_\mu \rho_A M_\mu^{\dagger}.$$

归一化条件来自 $U^{\dagger}U = \mathbb{I}$：

$$\sum_{\mu} M_\mu^{\dagger} M_\mu = \mathbb{I}_A.$$

去极化信道：Bloch 向量缩短

Kraus 算符：

$$M_0 = \sqrt{1-p}\,\mathbb{I}, \qquad M_{1,2,3} = \sqrt{\frac{p}{3}}\,X, Y, Z.$$

所以

$$\rho' = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z).$$

令 $\rho = \frac{1}{2}(\mathbb{I} + r_x X + r_y Y + r_z Z)$。利用

$$XXX = X, \quad XYX = -Y, \quad XZX = -Z,$$

及循环置换，可得

$$X\rho X + Y\rho Y + Z\rho Z = \frac{1}{2}(3\mathbb{I} - r_x X - r_y Y - r_z Z).$$

因此

$$\rho' = \frac{1}{2}\left[\mathbb{I} + \left(1 - \frac{4p}{3}\right)\boldsymbol{r}\cdot\boldsymbol{\sigma}\right].$$

退相位信道：只减小相干项

Kraus 算符：

$$M_0 = \sqrt{1-p}\,\mathbb{I}, \qquad M_1 = \sqrt{p}\,Z.$$

于是

$$\rho' = (1-p)\rho + pZ\rho Z.$$

若

$$\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix}, \qquad Z\rho Z = \begin{pmatrix} \rho_{00} & -\rho_{01} \\ -\rho_{10} & \rho_{11} \end{pmatrix},$$

所以

$$\rho' = \begin{pmatrix} \rho_{00} & (1-2p)\rho_{01} \\ (1-2p)\rho_{10} & \rho_{11} \end{pmatrix}.$$

物理图像

布居数 ρ_{00}, ρ_{11} 不变；相干项 ρ_{01} 因环境记录相位信息而衰减。

Fermi golden rule

设初态 $|0\rangle$ 与连续谱 $|k\rangle$ 弱耦合：

$$|\psi(t)\rangle = c_0(t)\,|0\rangle + \sum_k c_k(t)\,|k\rangle\,.$$

在相互作用表象下，一阶微扰给

$$\tilde{c}_k(t) = \frac{V_{k0}}{E_0 - E_k}\left(\mathrm{e}^{-\mathrm{i}(E_0-E_k)t/\hbar} - 1\right), \qquad V_{k0} = \langle k|\,V\,|0\rangle\,.$$

离开初态的概率为

$$p(t) = \sum_k |\tilde{c}_k(t)|^2 = 4\sum_k |V_{k0}|^2 \frac{\sin^2[(E_0 - E_k)t/(2\hbar)]}{(E_0 - E_k)^2}.$$

连续谱极限下，尖峰函数只选择近共振态：

$$\sum_k \to \int \rho(E)\,\mathrm{d}E, \qquad p(t) \simeq \Gamma t, \qquad \Gamma = \frac{2\pi}{\hbar}\rho(E_0)|V(E_0)|^2.$$

这就是不可逆 Markov 衰减率的来源。

Lindblad 主方程的短时推导

Markov 假设下，短时间 δt 的演化仍可写成 Kraus 形式：

$$\rho(t+\delta t) = \sum_{\mu} M_\mu \rho(t) M_\mu^\dagger .$$

取

$$M_0 = \mathbb{I} + (K - \mathrm{i}H)\delta t, \qquad M_\mu = L_\mu \sqrt{\delta t} \quad (\mu > 0).$$

完备性 $\sum_\mu M_\mu^\dagger M_\mu = \mathbb{I}$ 给出

$$K = -\frac{1}{2} \sum_{\mu>0} L_\mu^\dagger L_\mu .$$

于是

$$\begin{aligned} \dot\rho &= (K - \mathrm{i}H)\rho + \rho(K + \mathrm{i}H) + \sum_{\mu>0} L_\mu \rho L_\mu^\dagger \\ &= -\mathrm{i}[H, \rho] + \sum_{\mu>0} \left(L_\mu \rho L_\mu^\dagger - \frac{1}{2}\{L_\mu^\dagger L_\mu, \rho\} \right). \end{aligned}$$

自发辐射：jump operator

两能级原子 $|1\rangle \to |0\rangle$ 发射光子，取

$$L = \sqrt{\gamma}\,|0\rangle\langle 1|\,, \qquad K = -\frac{1}{2}L^\dagger L = -\frac{\gamma}{2}\,|1\rangle\langle 1|\,.$$

量子跃迁项为

$$L\rho L^\dagger = \gamma\,|0\rangle\langle 1|\,\rho\,|1\rangle\langle 0| = \gamma\rho_{11}\,|0\rangle\langle 0|\,.$$

代入 Lindblad 方程，不含相干驱动时得到 optical Bloch equations：

$$\dot\rho_{11} = -\gamma\rho_{11}, \qquad \dot\rho_{00} = \gamma\rho_{11}, \qquad \dot\rho_{01} = -\frac{\gamma}{2}\rho_{01}.$$

同时有相干驱动和衰减

若 Hamiltonian 中有 Rabi 驱动 Ω 和 detuning h_z，方程为

$$\begin{cases} \dot{\rho}_{11} = -\gamma\rho_{11} + \mathrm{i}\Omega\rho_{10} - \mathrm{i}\Omega^*\rho_{01}, \\ \dot{\rho}_{00} = \gamma\rho_{11} - \mathrm{i}\Omega\rho_{10} + \mathrm{i}\Omega^*\rho_{01}, \\ \dot{\rho}_{01} = -\dfrac{\gamma}{2}\rho_{01} - \mathrm{i}h_z\rho_{01} - \mathrm{i}\Omega(\rho_{00} - \rho_{11}). \end{cases}$$

看法

Ω 项让布居数在两能级间相干振荡；γ 项把布居数从 $|1\rangle$ 泄露到 $|0\rangle$，并让 Rabi oscillation 衰减到稳态。

强驱动极限下稳态激发态布居数最多接近 $1/2$，因为自发辐射不断把系统拉回基态。

广义测量：POVM 从系统-仪器耦合来

设系统 A 和测量仪器 B 先幺正耦合：

$$|\phi\rangle_A |0\rangle_B \longmapsto U_{AB} |\phi\rangle_A |0\rangle_B .$$

插入 B 的完备基：

$$\begin{aligned} U_{AB} |\phi\rangle_A |0\rangle_B &= \sum_\mu |\mu\rangle_B \langle\mu| U_{AB} |0\rangle_B |\phi\rangle_A \\ &= \sum_\mu |\mu\rangle_B M_\mu |\phi\rangle_A . \end{aligned}$$

测量仪器得到结果 μ 的概率为

$$p_\mu = \langle\phi| M_\mu^\dagger M_\mu |\phi\rangle .$$

定义 POVM 元素

$$F_\mu = M_\mu^\dagger M_\mu, \qquad F_\mu \geq 0, \qquad \sum_\mu F_\mu = \mathbb{I}.$$

注意：F_μ 决定概率，但测后态由 M_μ 决定，不唯一。

POVM 例子：区分非正交态

Alice 发送两个非正交态之一：

$$|\psi_1\rangle = |0\rangle, \qquad |\psi_2\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

Bob 可用一个带“不确定”结果的 POVM：

$$F_1 = c\,|1\rangle\langle 1|, \qquad F_2 = c\frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2}, \qquad F_3 = \mathbb{I} - F_1 - F_2,$$

其中 $c = \frac{\sqrt{2}}{1+\sqrt{2}}$。

- 若测到 F_1，一定不是 $|0\rangle$，所以推断是 $|\psi_2\rangle$。
- 若测到 F_2，一定不是 $|\psi_2\rangle$，所以推断是 $|\psi_1\rangle$。
- F_3 是 inconclusive；它保证完备性，也体现非正交态不能无歧义地总被区分。

量子信息工具：距离、熵与信道

迹、偏迹和子系统态

迹定义为

$$\mathrm{Tr}\, A = \sum_i \langle i|\, A\, |i\rangle\,, \qquad \mathrm{Tr}(AB) = \mathrm{Tr}(BA).$$

若 X_{AB} 在直积基中写作

$$X_{AB} = \sum_{i\mu,j\nu} x_{i\mu,j\nu}\, |i\rangle\, |\mu\rangle\, \langle j|\, \langle \nu|\,,$$

对 B 做偏迹为

$$\mathrm{Tr}_B\, X_{AB} = \sum_\mu (I_A \otimes \langle \mu|) X_{AB} (I_A \otimes |\mu\rangle) = \sum_{i,j,\mu} x_{i\mu,j\mu}\, |i\rangle\, \langle j|\,.$$

如果整体态是 ρ_{AB}，那么 A 上任意观测量 O_A 的期望值只依赖

$$\rho_A = \mathrm{Tr}_B\, \rho_{AB}, \qquad \mathrm{Tr}[(O_A \otimes I_B)\rho_{AB}] = \mathrm{Tr}(O_A \rho_A).$$

从 SVD 到 Schmidt 分解

二体纯态写作

$$|\psi\rangle_{AB} = \sum_{i,j} C_{ij} \, |i\rangle_A \, |j\rangle_B \, .$$

把系数看成矩阵 C，做奇异值分解

$$C = U \Lambda V^\dagger, \qquad \Lambda = \mathrm{diag}(s_1, s_2, \ldots), \qquad s_k \geq 0.$$

于是

$$|\psi\rangle_{AB} = \sum_k s_k \left(\sum_i U_{ik} \, |i\rangle_A \right) \left(\sum_j V^*_{jk} \, |j\rangle_B \right) = \sum_k s_k \, |u_k\rangle_A \, |v_k\rangle_B \, .$$

归一化给出 $\sum_k s_k^2 = 1$。约化密度矩阵为

$$\rho_A = \mathrm{Tr}_B \, |\psi\rangle\langle\psi| = \sum_k s_k^2 \, |u_k\rangle\langle u_k| \, , \qquad \rho_B = \sum_k s_k^2 \, |v_k\rangle\langle v_k| \, .$$

密度矩阵的三个来源

线性泛函

态给每个观测量 O 一个期望值：

$$\langle O\rangle_\rho = \mathrm{Tr}(O\rho).$$

概率非负和归一化要求

$$\rho \geq 0, \quad \mathrm{Tr}\,\rho = 1.$$

经典混合

若以概率 p_j 制备 $|\psi_j\rangle$，

$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j| .$$

期望值是

$$\sum_j p_j \langle\psi_j| O |\psi_j\rangle = \mathrm{Tr}(O\rho).$$

子系统

若整体是纯态 $|\Psi\rangle\langle\Psi|_{AB}$，局域态为

$$\rho_A = \mathrm{Tr}_B |\Psi\rangle\langle\Psi| .$$

它可能是混合态，原因不是经典混合，而是与 B 纠缠。

纯态判据：

$$\rho \text{ pure} \iff \rho^2 = \rho \iff \mathrm{Tr}\,\rho^2 = 1.$$

同一个混合态有很多 ensemble 表示

最大混合态的两个等价分解：

$$\frac{I}{2} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|\,.$$

更一般地，若

$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j| = \sum_k q_k |\phi_k\rangle\langle\phi_k|\,,$$

那么这两个 ensemble 的统计预言完全相同，因为任意观测量 O 只看到

$$\mathrm{Tr}(O\rho).$$

一个常用构造是纯化：

$$|\Psi\rangle_{AR} = \sum_j \sqrt{p_j}\,|\psi_j\rangle_A\,|j\rangle_R\,, \qquad \mathrm{Tr}_R\,|\Psi\rangle\langle\Psi| = \sum_j p_j |\psi_j\rangle\langle\psi_j| = \rho_A.$$

物理含义

对纯化系统 R 做不同基的测量，会在 A 上诱导不同 ensemble；但只要不告诉 A 测量结果，A 的密度矩阵不变。

量子信道：CPTP map

量子态演化的最一般形式是线性映射

$$\mathcal{E} : \rho \mapsto \mathcal{E}(\rho).$$

为了把任意输入态变成合法输出态，要求：

1. trace preserving：$\operatorname{Tr} \mathcal{E}(\rho) = \operatorname{Tr} \rho$；
2. completely positive：对任意辅助系统 R，

$$(\mathbb{I}_R \otimes \mathcal{E})(X_{RA}) \geq 0 \quad \text{whenever } X_{RA} \geq 0.$$

“positive” 不够，因为转置映射 $T(\rho) = \rho^T$ 单独作用在一个系统上保持正性，但

$$(\mathbb{I} \otimes T)(|\Phi^+\rangle\langle\Phi^+|)$$

可以有负本征值。因此物理信道必须是 CPTP，而不是只要求正映射。

要点

完全正定是指这个系统可能和别的系统纠缠，局域操作也不能把整体态变成非法态。

Choi–Jamiolkowski 表示

设 $\mathcal{E} : A \to B$，取未归一化最大纠缠态

$$|\Phi\rangle_{AA'} = \sum_i |i\rangle_A |i\rangle_{A'} .$$

Choi 矩阵定义为

$$\Phi_{\mathcal{E}} = (\mathbb{I}_A \otimes \mathcal{E}_{A' \to B})(|\Phi\rangle\langle\Phi|) = \sum_{i,j} |i\rangle\langle j|_A \otimes \mathcal{E}(|i\rangle\langle j|)_B.$$

反变换是

$$\mathcal{E}(\rho) = \mathrm{Tr}_A\big[(\rho_A^T \otimes I_B)\Phi_{\mathcal{E}}\big].$$

验证 trace-preserving 条件：

$$\mathrm{Tr}\,\mathcal{E}(\rho) = \mathrm{Tr}\,\big[(\rho^T \otimes I_B)\Phi_{\mathcal{E}}\big] = \mathrm{Tr}\,\big[\rho^T\,\mathrm{Tr}_B\,\Phi_{\mathcal{E}}\big].$$

要让它对所有 ρ 等于 $\mathrm{Tr}\,\rho$，必须有

$$\mathrm{Tr}_B\,\Phi_{\mathcal{E}} = I_A.$$

因此

$$\mathcal{E}\ \text{CPTP} \quad\Longleftrightarrow\quad \Phi_{\mathcal{E}} \geq 0, \quad \mathrm{Tr}_B\,\Phi_{\mathcal{E}} = I_A.$$

从 Choi 分解得到 Kraus 表示

若 $\Phi_{\mathcal{E}} \geq 0$，可谱分解为

$$\Phi_{\mathcal{E}} = \sum_{\ell} |K_\ell\rangle\!\rangle\langle\!\langle K_\ell| \,,$$

其中向量化约定为

$$|K\rangle\!\rangle = \sum_{i,j} K_{ji} \, |i\rangle_A \, |j\rangle_B \,.$$

代入 Choi 反变换：

$$\begin{aligned}\mathcal{E}(\rho) &= \mathrm{Tr}_A \left[(\rho^T \otimes I) \sum_{\ell} |K_\ell\rangle\!\rangle\langle\!\langle K_\ell| \right] \\ &= \sum_{\ell} K_\ell \rho K_\ell^\dagger .\end{aligned}$$

trace preserving 条件变成

$$\sum_{\ell} K_\ell^\dagger K_\ell = I.$$

这就是 Kraus 表示。反过来，只要一组 K_ℓ 满足上式，映射

$$\rho \mapsto \sum_{\ell} K_\ell \rho K_\ell^\dagger$$

就是 CPTP。

trace norm 和 trace distance

矩阵 A 的 trace norm 定义为奇异值之和：

$$\|A\|_1 = \mathrm{Tr}\sqrt{A^\dagger A}.$$

两个量子态的 trace distance：

$$D_{\mathrm{tr}}(\rho,\sigma) = \frac{1}{2}\|\rho-\sigma\|_1 .$$

令 $\Delta = \rho - \sigma$，谱分解

$$\Delta = \sum_k \lambda_k |k\rangle\langle k| = \Delta_+ - \Delta_-,$$

其中 Δ_+ 收集正本征值，Δ_- 收集负本征值的相反数。因为 $\mathrm{Tr}\,\Delta = 0$，有

$$D_{\mathrm{tr}}(\rho,\sigma) = \mathrm{Tr}\,\Delta_+ = \mathrm{Tr}\,\Delta_-.$$

变分形式：

$$D_{\mathrm{tr}}(\rho,\sigma) = \max_{0\le M\le I} \mathrm{Tr}[M(\rho-\sigma)].$$

最优 M 是 Δ 的正本征子空间投影。

trace distance 的意义：态区分

假设输入态以等概率为 ρ 或 σ。做二结果 POVM $\{M, I-M\}$，若结果 M 就猜 ρ，否则猜 σ。

$$\begin{aligned} p_{\mathrm{succ}}(M) &= \frac{1}{2}\operatorname{Tr}(M\rho) + \frac{1}{2}\operatorname{Tr}[(I-M)\sigma] \\ &= \frac{1}{2}\big(1 + \operatorname{Tr}[M(\rho-\sigma)]\big). \end{aligned}$$

对 M 优化得到 Helstrom 界：

$$p_{\mathrm{succ}}^{\max} = \frac{1}{2}\big(1 + D_{\mathrm{tr}}(\rho,\sigma)\big).$$

两个极端

$$D_{\mathrm{tr}} = 0 \Rightarrow p_{\mathrm{succ}}^{\max} = 1/2 \quad (\text{只能瞎猜}), \qquad D_{\mathrm{tr}} = 1 \Rightarrow p_{\mathrm{succ}}^{\max} = 1 \quad (\text{可完美区分}).$$

trace distance 在信道下单调

量子信道不能增加态的可区分性：

$$D_{\mathrm{tr}}(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq D_{\mathrm{tr}}(\rho, \sigma).$$

用 Stinespring 表示证明。设

$$\mathcal{E}(\rho) = \mathrm{Tr}_E[U(\rho \otimes |0\rangle\langle 0|_E)U^\dagger].$$

由于 trace distance 对幺正不变，

$$\begin{aligned} D_{\mathrm{tr}}(\rho, \sigma) &= D_{\mathrm{tr}}(\rho \otimes |0\rangle\langle 0|, \sigma \otimes |0\rangle\langle 0|) \\ &= D_{\mathrm{tr}}(U(\rho \otimes |0\rangle\langle 0|)U^\dagger, U(\sigma \otimes |0\rangle\langle 0|)U^\dagger). \end{aligned}$$

偏迹是把环境信息丢掉，因此由变分形式可得

$$D_{\mathrm{tr}}(X_{AE}, Y_{AE}) \geq D_{\mathrm{tr}}(\mathrm{Tr}_E X_{AE}, \mathrm{Tr}_E Y_{AE}).$$

合起来得到单调性。

保真度 fidelity

量子态保真度定义为

$$F(\rho,\sigma)=\mathrm{Tr}\left|\sqrt{\rho}\sqrt{\sigma}\right|.$$

几个常用特例：

$$F(|\psi\rangle\langle\psi|,|\phi\rangle\langle\phi|)=|\langle\psi|\phi\rangle|,\qquad F(|\psi\rangle\langle\psi|,\sigma)=\sqrt{\langle\psi|\,\sigma\,|\psi\rangle}.$$

若 ρ 和 σ 可同时对角化，

$$\rho=\sum_i p_i|i\rangle\langle i|,\quad \sigma=\sum_i q_i|i\rangle\langle i|,\qquad F(\rho,\sigma)=\sum_i\sqrt{p_iq_i},$$

退化为经典概率分布的 Bhattacharyya coefficient。

和 trace distance 的关系

$$1-F(\rho,\sigma)\le D_{\mathrm{tr}}(\rho,\sigma)\le\sqrt{1-F(\rho,\sigma)^2}.$$

Shannon 熵和典型集

经典概率分布 $p = (p_1, \ldots, p_d)$ 的 Shannon 熵为

$$H(p) = -\sum_i p_i \log_2 p_i.$$

对 i.i.d. 序列 $X^n = (X_1, \ldots, X_n)$，典型序列的概率近似为

$$p(x^n) = \prod_{k=1}^{n} p(x_k) \approx 2^{-nH(X)}.$$

因此典型集大小约为

$$\left| T_\epsilon^{(n)} \right| \approx 2^{nH(X)}.$$

这就是 Shannon noiseless coding 的核心：

$$n \text{ 个样本} \quad \Longrightarrow \quad nH(X) \text{ bits 可压缩表示.}$$

Von Neumann 熵和互信息

量子态 ρ 的 Von Neumann 熵定义为

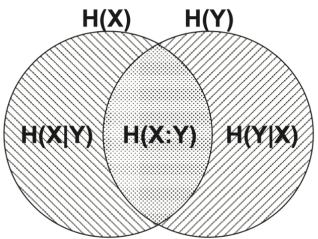
$$S(\rho) = -\operatorname{Tr}(\rho \log_2 \rho).$$

若 $\rho = \sum_i \lambda_i |i\rangle\langle i|$，则

$$S(\rho) = -\sum_i \lambda_i \log_2 \lambda_i.$$

二体态的条件熵和互信息：

$$S(A|B) = S(AB) - S(B),$$
$$I(A:B) = S(A) + S(B) - S(AB).$$



经典 Venn 图能辅助记忆：互信息是两个随机变量共享的不确定性。量子里也保留

$$I(A:B) \geq 0,$$

但条件熵 $S(A|B)$ 可以为负，这是纠缠的一种信号。

纯态纠缠熵：$S(A) = S(B)$

若 AB 整体纯态 Schmidt 分解为

$$|\psi\rangle_{AB} = \sum_k \sqrt{\lambda_k}\,|k\rangle_A\,|k\rangle_B\,, \qquad \lambda_k \geq 0, \quad \sum_k \lambda_k = 1,$$

则

$$\rho_A = \sum_k \lambda_k\,|k\rangle\langle k|_A\,, \qquad \rho_B = \sum_k \lambda_k\,|k\rangle\langle k|_B\,.$$

因此两个约化态本征值相同：

$$S(A) = S(B) = -\sum_k \lambda_k \log_2 \lambda_k.$$

对 Bell 态，$\lambda_1 = \lambda_2 = 1/2$，所以

$$S(A) = S(B) = 1.$$

对 product state，只有一个 Schmidt 系数为 1，所以

$$S(A) = S(B) = 0.$$

要点

二体纯态的纠缠量可以直接由任一边的混合度读出。

相对熵

量子相对熵定义为

$$D(\rho\|\sigma) = \operatorname{Tr}\rho(\log\rho - \log\sigma), \qquad \operatorname{supp}(\rho) \subseteq \operatorname{supp}(\sigma).$$

最重要的性质是单调性：对任意量子信道 $\mathcal{E}$，

$$D(\rho\|\sigma) \geq D(\mathcal{E}(\rho)\|\mathcal{E}(\sigma)).$$

许多信息量都能写成相对熵：

$$S(\rho) = \log d - D\big(\rho\|I/d\big),$$
$$I(A:B) = D\big(\rho_{AB}\|\rho_A \otimes \rho_B\big).$$

由 $D(\rho\|\sigma) \geq 0$ 立刻得到

$$I(A:B) \geq 0,$$

也就是 subadditivity：

$$S(AB) \leq S(A) + S(B).$$

纠缠：资源、悖论和通信协议

纠缠的定义和 Bell 态

二体纯态若不能写成乘积

$$|\psi\rangle_{AB} \neq |\phi\rangle_A \otimes |\chi\rangle_B ,$$

则称为纠缠态。
Bell 态是最基本的两比特纠缠基：

$$\left|\Phi^{\pm}\right\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \qquad \left|\Psi^{\pm}\right\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}.$$

用一个局域 Pauli 门就能在它们之间转换，例如

$$X_A \left|\Phi^{+}\right\rangle = \left|\Psi^{+}\right\rangle , \qquad Z_A \left|\Phi^{+}\right\rangle = \left|\Phi^{-}\right\rangle .$$

Bell 态的两体关联

以

$$\left|\Phi^{+}\right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

为例。单体平均值为

$$\langle X_A \rangle = \langle Y_A \rangle = \langle Z_A \rangle = 0.$$

但二体算符有确定本征值：

$$X_A X_B \left|\Phi^{+}\right\rangle = \left|\Phi^{+}\right\rangle, \qquad Z_A Z_B \left|\Phi^{+}\right\rangle = \left|\Phi^{+}\right\rangle.$$

对于 Y：

$$Y|0\rangle = \mathrm{i}\,|1\rangle, \quad Y|1\rangle = -\mathrm{i}\,|0\rangle,$$

所以

$$Y_A Y_B\,|00\rangle = -\,|11\rangle, \quad Y_A Y_B\,|11\rangle = -\,|00\rangle,$$

从而

$$Y_A Y_B \left|\Phi^{+}\right\rangle = -\left|\Phi^{+}\right\rangle.$$

纠缠熵和纯态纠缠判据

由 Schmidt 分解可得

$$\rho_A = \mathrm{Tr}_B\,|\psi\rangle\langle\psi| = \sum_k \lambda_k\,|u_k\rangle\langle u_k|\,.$$

可分态

仅一个 $\lambda_k = 1$:

$$\rho_A^2 = \rho_A, \qquad S(\rho_A) = 0.$$

最大纠缠

$d = \min(d_A, d_B)$,

$$\lambda_k = \frac{1}{d}, \qquad S(\rho_A) = \log_2 d.$$

纠缠熵定义为

$$S(\rho_A) = -\,\mathrm{Tr}(\rho_A \log_2 \rho_A) = -\sum_k \lambda_k \log_2 \lambda_k.$$

要点

纯态时，子系统越混合，说明它与另一边越纠缠；混合态时不能这样直接判断。

Bell 不等式：从 singlet 的关联开始

取 singlet

$$\left|\Psi^-\right\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Alice 沿 $\hat{a}$ 测，Bob 沿 $\hat{b}$ 测。投影算符为

$$P_A^{\pm}(\hat{a}) = \frac{1}{2}(\mathbb{I} \pm \hat{a}\cdot\boldsymbol{\sigma}_A), \qquad P_B^{\pm}(\hat{b}) = \frac{1}{2}(\mathbb{I} \pm \hat{b}\cdot\boldsymbol{\sigma}_B).$$

对 singlet 有

$$\langle\sigma_A^i\rangle = \langle\sigma_B^i\rangle = 0, \qquad \langle\sigma_A^i\sigma_B^j\rangle = -\delta_{ij}.$$

所以相关函数

$$E(\hat{a},\hat{b}) = \langle(\hat{a}\cdot\boldsymbol{\sigma}_A)(\hat{b}\cdot\boldsymbol{\sigma}_B)\rangle = -\hat{a}\cdot\hat{b}.$$

同号概率为

$$P_{\text{same}} = \frac{1+E}{2} = \frac{1-\hat{a}\cdot\hat{b}}{2}.$$

Bell 不等式

若每次测量结果在实验前已由局域隐藏变量决定，则对三组测量方向必有

$$S = P_{\text{same}}(e_1^A, -e_2^B) + P_{\text{same}}(e_1^A, -e_3^B) + P_{\text{same}}(e_2^A, -e_3^B) \geq 1.$$

理由：三个二值变量不可能两两都不同，至少有一对相同。
量子力学取 e_1, e_2, e_3 两两夹角为 $2\pi/3$。在第一项中测量方向是

$$\hat{a} = e_1, \qquad \hat{b} = -e_2,$$

因此

$$\hat{a} \cdot \hat{b} = -e_1 \cdot e_2 = -\cos(2\pi/3) = \frac{1}{2}, \qquad P_{\text{same}} = \frac{1 - \hat{a} \cdot \hat{b}}{2} = \frac{1}{4}.$$

三项相同，所以

$$S = \frac{3}{4} < 1.$$

结论

量子关联不能由预先存在、局域可访问的隐藏变量同时解释。

CHSH 形式和纠缠 witness

更常用的 CHSH 量为

$$C = |E(a_1, b_1) + E(a_2, b_1) + E(a_1, b_2) - E(a_2, b_2)|.$$

局域隐变量理论给出

$$C \leq 2,$$

量子力学最大值为 Tsirelson bound：

$$C \leq 2\sqrt{2}.$$

作为纠缠 witness

若实验测得 $C > 2$，则态一定纠缠；反过来，纠缠态不一定都违反某个给定 Bell 不等式。

QKD

若 Alice 和 Bob 用部分数据检验 Bell 违背，窃听者的测量会破坏纠缠，从而降低违背程度或提高误码率。

Superdense coding：一个 qubit 传两个 classical bits

共享 Bell 对

$$\left|\Phi^+\right\rangle_{AB} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Alice 在自己的比特上编码：

消息	Alice 操作	得到的 Bell 态
00	$\mathbb{I}$	$\left\|\Phi^+\right\rangle$
01	Z	$\left\|\Phi^-\right\rangle$
10	X	$\left\|\Psi^+\right\rangle$
11	XZ	$\left\|\Psi^-\right\rangle$

然后 Alice 把自己的 qubit 发给 Bob。Bob 做 Bell 基测量，四个正交 Bell 态可完美区分，因此解出两位经典信息。

要点

优势来自预先共享的纠缠；发送的单个 qubit 本身不是孤立携带两位信息。

Teleportation：两个 classical bits 传一个 qubit

Alice 要传未知态

$$|\phi\rangle_1 = \alpha|0\rangle + \beta|1\rangle,$$

Alice 和 Bob 共享

$$\left|\Psi^-\right\rangle_{23} = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

总态为

$$\begin{aligned}|\psi\rangle_{123} &= |\phi\rangle_1 \left|\Psi^-\right\rangle_{23} \\ &= \frac{\alpha}{\sqrt{2}}(|001\rangle - |010\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle - |110\rangle).\end{aligned}$$

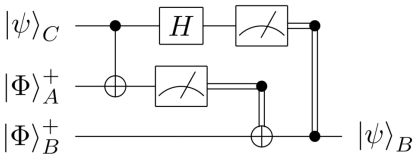
把 12 两个 qubit 改写到 Bell 基，得到

$$\begin{aligned}|\psi\rangle_{123} = \frac{1}{2}(&\left|\Psi^-\right\rangle_{12}(-\alpha|0\rangle_3 - \beta|1\rangle_3) + \left|\Psi^+\right\rangle_{12}(-\alpha|0\rangle_3 + \beta|1\rangle_3) \\ &+ \left|\Phi^-\right\rangle_{12}(\alpha|1\rangle_3 + \beta|0\rangle_3) + \left|\Phi^+\right\rangle_{12}(\alpha|1\rangle_3 - \beta|0\rangle_3)).\end{aligned}$$

Teleportation：两个 classical bits 传一个 qubit

Alice 对 qubit $1,2$ 做 Bell 基测量，结果有四种，各概率 $1/4$。
Bob 根据两位经典信息做一个 Pauli 修正。

Alice 测量结果	Bob 修正
$\lvert\Psi^-\rangle_{12}$	$-\mathbb{I}$
$\lvert\Psi^+\rangle_{12}$	$-Z$
$\lvert\Phi^-\rangle_{12}$	X
$\lvert\Phi^+\rangle_{12}$	XZ



Teleportation 线路示意

整体相位无物理意义，所以符号 $-$ 不影响结果。

两点澄清

未知态没有被复制，Alice 的原态被 Bell 测量破坏；也没有超光速通信，因为 Bob 必须等到经典信息。

纠缠作为资源：free states 和 LOCC

二体混合态若可写成

$$\rho_{AB}^{\mathrm{sep}} = \sum_k p_k \rho_A^{(k)} \otimes \rho_B^{(k)}, \qquad p_k \geq 0, \quad \sum_k p_k = 1,$$

则称为 separable state。这种关联可由“局域制备 + 共享随机变量 k”产生。

$$\text{separable} \iff \text{没有量子纠缠资源.}$$

自由操作是 LOCC：

$$\text{Local Operations} + \text{Classical Communication.}$$

LOCC 不能从 separable state 产生纠缠，因此任何合理纠缠量 E 应满足

$$E(\Lambda_{\mathrm{LOCC}}(\rho)) \leq E(\rho).$$

要点

把纠缠看成资源后，teleportation 和 dense coding 都是在“消耗纠缠”。

纯态纠缠转换：majorization

纯态 Schmidt 系数按降序记为

$$\lambda^{\psi} = (\lambda_1^{\psi} \geq \lambda_2^{\psi} \geq \cdots), \qquad \lambda^{\phi} = (\lambda_1^{\phi} \geq \lambda_2^{\phi} \geq \cdots).$$

Nielsen 定理：存在确定性 LOCC 使

$$|\psi\rangle \longrightarrow |\phi\rangle$$

当且仅当

$$\lambda^{\psi} \prec \lambda^{\phi}, \qquad \sum_{i=1}^{k} \lambda_i^{\psi} \leq \sum_{i=1}^{k} \lambda_i^{\phi}, \quad \forall k.$$

例子：Bell 态的 Schmidt 向量是 $(1/2, 1/2)$，product state 是 $(1, 0)$，有

$$(1/2, 1/2) \prec (1, 0),$$

所以 Bell 态可通过 LOCC 退化成 product state；反过来不行。

资源不等式：teleportation 和 dense coding

用资源符号表示：

$$[q \to q]：\text{一个量子比特信道}，\quad [c \to c]：\text{一个经典比特信道}，\quad [qq]：\text{一对 Bell 态}.$$

Teleportation 消耗一对纠缠和两位经典通信，模拟一个量子信道：

$$2[c \to c] + [qq] \geq [q \to q].$$

Dense coding 消耗一对纠缠和一个量子信道，传两位经典信息：

$$[q \to q] + [qq] \geq 2[c \to c].$$

如果把共享纠缠看作免费资源，两者给出形式关系

$$[q \to q] \simeq 2[c \to c].$$

要点

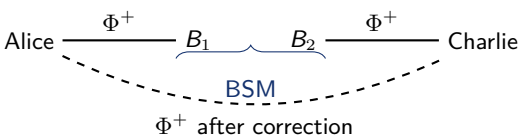
一比特量子信息相当于两比特经典信息！（当然是在有 free 纠缠资源的前提下）

Entanglement swapping

Alice–Bob 共享 $\left|\Phi^+\right\rangle_{AB}$，Bob–Charlie 共享 $\left|\Phi^+\right\rangle_{BC}$。把中间两个 Bob 量子比特作 Bell 测量：

$$\left|\Phi^+\right\rangle_{AB_1}\left|\Phi^+\right\rangle_{B_2C} = \frac{1}{2}\sum_{m\in\{00,01,10,11\}} |B_m\rangle_{B_1B_2}\, P_m \left|\Phi^+\right\rangle_{AC}.$$

测量结果 m 公开后，Alice 或 Charlie 做对应 Pauli 修正，A 和 C 就共享 Bell 对。



量子中继器的基本想法

光纤中光子探测概率随距离指数衰减，可写成

$$p_{\mathrm{det}}(L) \sim \mathrm{e}^{-L/L_0}.$$

若直接传输，总尝试次数量级为

$$N_{\mathrm{direct}} \sim \mathrm{e}^{L/L_0}.$$

把总距离切成 m 段，每段长度 L/m：

$$p_{\mathrm{seg}} \sim \mathrm{e}^{-L/(mL_0)}.$$

每段先建立短程纠缠并存入量子存储器，再通过 entanglement swapping 连接起来。

$$\text{短程 Bell 对} \quad + \quad \text{局域 BSM} \quad \Longrightarrow \quad \text{长程 Bell 对}.$$

GHZ 态：stabilizer 和部分测量

$$|GHZ_N\rangle = \frac{|0\rangle^{\otimes N} + |1\rangle^{\otimes N}}{\sqrt{2}}.$$

它是以下算符的 $+1$ 本征态：

$$Z_1Z_2, \quad Z_2Z_3, \quad \cdots, \quad Z_{N-1}Z_N, \quad X_1X_2\cdots X_N.$$

若测第一个 qubit 的 Z，态坍缩到

$$|0\rangle^{\otimes N} \quad \text{或} \quad |1\rangle^{\otimes N}.$$

若测第一个 qubit 的 X，余下 $N-1$ 个 qubit 变成

$$\frac{|0\rangle^{\otimes N-1} \pm |1\rangle^{\otimes N-1}}{\sqrt{2}},$$

符号由测量结果决定。测量基决定“泄露路径信息”还是“保留相干”。

GHZ 态的退相干和精密测量

Trace 掉一个 qubit：

$$\mathrm{Tr}_1 \left|GHZ_N\right\rangle\left\langle GHZ_N\right| = \frac{1}{2}\left(|0\rangle\langle 0|^{\otimes N-1} + |1\rangle\langle 1|^{\otimes N-1}\right).$$

交叉项消失，因此 GHZ 纠缠对粒子损失很敏感。
但同样的敏感性可用于相位估计。若

$$H = h\sum_{j=1}^{N} Z_j,$$

则

$$\frac{|0\rangle^{\otimes N} + |1\rangle^{\otimes N}}{\sqrt{2}} \mapsto \frac{|0\rangle^{\otimes N} + \mathrm{e}^{\mathrm{i}N\phi}\,|1\rangle^{\otimes N}}{\sqrt{2}}.$$

独立粒子重复 N 次测量有

$$\delta\phi \sim \frac{1}{\sqrt{N}},$$

而理想 GHZ 有

$$\delta\phi \sim \frac{1}{N}.$$

GHZ 悖论：不用不等式的非局域性

三比特 GHZ 态

$$|\mathrm{GHZ}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}.$$

它满足

$$X_1X_2X_3\,|\mathrm{GHZ}\rangle = +\,|\mathrm{GHZ}\rangle\,,$$

$$X_1Y_2Y_3\,|\mathrm{GHZ}\rangle = Y_1X_2Y_3\,|\mathrm{GHZ}\rangle = Y_1Y_2X_3\,|\mathrm{GHZ}\rangle = -\,|\mathrm{GHZ}\rangle\,.$$

若每个局域观测量在测量前已有确定值 $x_i, y_i = \pm 1$，则后三式相乘给

$$(x_1y_2y_3)(y_1x_2y_3)(y_1y_2x_3) = (-1)^3 = -1.$$

左边化简为

$$x_1x_2x_3(y_1^2y_2^2y_3^2) = x_1x_2x_3.$$

但第一式要求 $x_1x_2x_3 = +1$，矛盾。

量子线路模型和通用门

量子线路模型

量子计算可以抽象成三步：

$$|0\rangle^{\otimes n} \xrightarrow{U=U_L\cdots U_2U_1} U|0\rangle^{\otimes n} \xrightarrow{\text{measure}} z \in \{0,1\}^m.$$

每一步 U_j 通常只作用在一两个量子比特上：

$$U_j = I \otimes \cdots \otimes G_j \otimes \cdots \otimes I.$$

输出概率由 Born rule 给出：

$$p(z) = \langle 0|^{\otimes n} U^\dagger (|z\rangle\langle z| \otimes I) U |0\rangle^{\otimes n}.$$

为什么只允许局域门仍然通用

任意物理可实现的控制通常都是局域相互作用；通用性定理说明，一组足够简单的局域门可以近似任意整体幺正演化。

单比特门：Euler 分解

去掉整体相位后，任意单比特幺正演化属于 $SU(2)$，可以写成

$$U = R_z(\alpha) R_y(\beta) R_z(\gamma),$$

其中

$$R_z(\phi) = \begin{pmatrix} \mathrm{e}^{-\mathrm{i}\phi/2} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\phi/2} \end{pmatrix}, \qquad R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}.$$

常用门：

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi/4} \end{pmatrix}.$$

H, S 是 Clifford 门；加入非 Clifford 的 T 后可获得通用近似能力。

Bloch 球上的旋转和幺正共轭

若

$$\rho = \frac{1}{2}(I + \vec{r}\cdot\boldsymbol{\sigma}), \qquad U = \mathrm{e}^{-\mathrm{i}\theta\hat{n}\cdot\boldsymbol{\sigma}/2},$$

则

$$\rho' = U\rho U^\dagger = \frac{1}{2}\big(I + (R_{\hat{n}}(\theta)\vec{r})\cdot\boldsymbol{\sigma}\big).$$

例如

$$R_z(\theta) X R_z^\dagger(\theta) = X\cos\theta + Y\sin\theta,$$
$$R_z(\theta) Y R_z^\dagger(\theta) = Y\cos\theta - X\sin\theta.$$

这说明 $SU(2)$ 单比特幺正对应 Bloch 球上的 $SO(3)$ 旋转。

受控门

受控 U 定义为

$$C(U) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U.$$

CNOT 是 $U = X$ 的情况：

$$\mathrm{CNOT}\,|a, b\rangle = |a, b \oplus a\rangle\,.$$

CZ 是 $U = Z$：

$$\mathrm{CZ} = \mathrm{diag}(1, 1, 1, -1).$$

二者互相等价：

$$\mathrm{CNOT} = (I \otimes H)\,\mathrm{CZ}(I \otimes H).$$

SWAP 门可由三个 CNOT 实现：

$$\mathrm{SWAP}_{12} = \mathrm{CNOT}_{12}\,\mathrm{CNOT}_{21}\,\mathrm{CNOT}_{12}\,.$$

纠缠生成

$\mathrm{CNOT}(H \otimes I)\ |00\rangle = \left|\Phi^+\right\rangle$，所以 CNOT 与单比特门一起已经能产生纠缠。

Toffoli 门和可逆经典计算

Toffoli 门是三比特受控受控非门：

$$\mathrm{Toffoli}\,|a, b, c\rangle = |a, b, c \oplus ab\rangle\,.$$

它能实现 NAND：令 $c = 1$，则

$$c' = 1 \oplus ab = \neg(a \wedge b).$$

由于 NAND 对经典布尔电路通用，Toffoli 对可逆经典计算通用。

为什么经典计算要先变可逆

量子线路中的封闭演化必须幺正，而幺正必然可逆。不可逆的经典函数 $f(x)$ 通常改写成

$$U_f\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus f(x)\rangle\,.$$

这样 U_f 是一个置换矩阵，因此是幺正。

通用门集：精确和近似

精确通用门集的一种表述：任意 n 比特幺正都可由

$$\{\text{arbitrary one-qubit gates},\ \mathrm{CNOT}\}$$

精确分解。

近似通用

实际硬件不会给出连续无限精度门集，因此常用离散门集：

$$\{H, S, T, \mathrm{CNOT}\}.$$

其中 H, S, CNOT 是 Clifford；T 提供非 Clifford 资源。Solovay–Kitaev 定理说明，对足够好的有限门集，任意单比特门可用长度

$$O\big(\log_c(1/\epsilon)\big)$$

的门序列近似到误差 ϵ。

参数计数

一般 n 比特幺正有 $4^n - 1$ 个实参数，所以任意幺正分解通常需要指数多门。算法有优势，是因为目标幺正有特殊结构。

Clifford 门为什么容易经典模拟

Pauli 群

$$\mathcal{P}_n = \{\pm 1, \pm \mathrm{i}\}\{I, X, Y, Z\}^{\otimes n}.$$

Clifford 群定义为 Pauli 群的正规化子：

$$U \in \mathrm{Clifford} \quad \Longleftrightarrow \quad UPU^\dagger \in \mathcal{P}_n, \quad \forall P \in \mathcal{P}_n.$$

几个共轭关系：

$$HXH = Z, \quad HZH = X, \quad SXS^\dagger = Y, \quad SZS^\dagger = Z.$$

Clifford 线路把 stabilizer 态映到 stabilizer 态，Gottesman–Knill 定理说明这类线路可高效经典模拟。

为什么还要 T 门

只有 Clifford 不能通用；非 Clifford 门打破 stabilizer 封闭性，是实现通用量子计算的必要资源之一。

phase kickback

oracle 写作

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle .$$

若第二寄存器取

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

则

$$U_f |x\rangle |-\rangle = \begin{cases} |x\rangle |-\rangle , & f(x) = 0, \\ |x\rangle X|-\rangle = -|x\rangle |-\rangle , & f(x) = 1, \end{cases}$$

所以

$$U_f |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |-\rangle .$$

相位被“踢回”到输入寄存器。很多算法第一步都是

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle \longmapsto \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle .$$

量子算法：用相位和干涉读出结构

量子 oracle 和 phase kickback

把经典函数 f 嵌入可逆幺正：

$$U_f |x\rangle_n |y\rangle_m = |x\rangle_n |y \oplus f(x)\rangle_m .$$

若第二个寄存器为

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

则

$$\begin{aligned} U_f |x\rangle |-\rangle &= |x\rangle \frac{|f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \\ &= (-1)^{f(x)} |x\rangle |-\rangle . \end{aligned}$$

核心机制

函数值没有作为可读 bit 留在辅助寄存器，而是“踢回”到 $|x\rangle$ 分量的相位上。

均匀叠加和“不能直接读出”的限制

Hadamard 制备所有输入的等幅叠加：

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle .$$

若直接做函数评估：

$$U_f \frac{1}{2^{n/2}} \sum_x |x\rangle |0\rangle = \frac{1}{2^{n/2}} \sum_x |x\rangle |f(x)\rangle .$$

测量只给一个随机样本 $x, f(x)$，并不能一次读出所有函数值。
真正有用的结构通常是

$$\frac{1}{2^{n/2}} \sum_x (-1)^{f(x)} |x\rangle ,$$

再通过 $H^{\otimes n}$、QFT 或 Grover diffusion 让相位变成可测概率。

Deutsch 问题

问题：$f\colon \{0,1\} \to \{0,1\}$，判断 f 是常数还是 balanced。先制备

$$|+\rangle\,|-\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\,\frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

作用 oracle：

$$U_f\,|+\rangle\,|-\rangle = \frac{(-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle}{\sqrt{2}}\,|-\rangle\,.$$

若 $f(0) = f(1)$，第一比特为 $\pm|+\rangle$；若 $f(0) \neq f(1)$，第一比特为 $\pm|-\rangle$。
最后测 X 基即可一次区分。

Deutsch–Jozsa：推导到振幅公式

承诺：$f\colon \{0,1\}^n \to \{0,1\}$ 要么常数，要么 balanced。经过 phase kickback 后

$$|\psi\rangle = \frac{1}{2^{n/2}} \sum_x (-1)^{f(x)} |x\rangle .$$

再做 $H^{\otimes n}$。用恒等式

$$H^{\otimes n} |x\rangle = \frac{1}{2^{n/2}} \sum_y (-1)^{x\cdot y} |y\rangle ,$$

得到

$$H^{\otimes n} |\psi\rangle = \frac{1}{2^n} \sum_y \left[\sum_x (-1)^{x\cdot y + f(x)} \right] |y\rangle .$$

其中 $|0^n\rangle$ 的振幅为

$$A_{0^n} = \frac{1}{2^n} \sum_x (-1)^{f(x)}.$$

常数函数 $A_{0^n} = \pm 1$；balanced 函数 $A_{0^n} = 0$。**一次测量即可判断。**

Bernstein–Vazirani：一次读出隐藏串

设

$$f_a(x) = a \cdot x \pmod 2, \qquad a, x \in \{0,1\}^n.$$

经过同样电路，输出态为

$$\frac{1}{2^n} \sum_y \sum_x (-1)^{x \cdot y + a \cdot x} |y\rangle .$$

内层求和可分解：

$$\begin{aligned} \sum_x (-1)^{x \cdot y + a \cdot x} &= \prod_{j=1}^{n} \sum_{x_j=0}^{1} (-1)^{(y_j + a_j) x_j} \\ &= \prod_{j=1}^{n} 2\delta_{y_j, a_j} = 2^n \delta_{y,a}. \end{aligned}$$

所以最终态就是

$$|a\rangle .$$

经典要查询 n 次才能逐位确定 a；量子只需一次 oracle。

Grover 搜索：oracle 和两个反射

无结构搜索：N 个元素中唯一目标为 w。定义相位 oracle

$$O_w |x\rangle = (-1)^{[x=w]} |x\rangle , \qquad O_w = \mathbb{I} - 2 |w\rangle\langle w| .$$

初态为

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle .$$

关于 $|s\rangle$ 的反射是

$$D = 2 |s\rangle\langle s| - \mathbb{I}.$$

Grover 迭代

$$G = DO_w.$$

Grover 的二维旋转推导

定义

$$|r\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq w} |x\rangle\,, \qquad |s\rangle = \sin\theta\,|w\rangle + \cos\theta\,|r\rangle\,,$$

其中

$$\sin\theta = \frac{1}{\sqrt{N}}, \qquad \theta \simeq \frac{1}{\sqrt{N}}.$$

O_w **把** $|w\rangle$ **分量反号，** D **再关于** $|s\rangle$ **反射。每轮总旋转角为** 2θ**，所以**

$$G^k |s\rangle = \sin((2k+1)\theta)\,|w\rangle + \cos((2k+1)\theta)\,|r\rangle\,.$$

令

$$(2k+1)\theta \simeq \frac{\pi}{2},$$

得到

$$k \simeq \frac{\pi}{4}\sqrt{N}.$$

测量成功概率接近 1**。**

离散 Fourier 变换到 QFT

经典离散 Fourier 变换：

$$g(y) = \sum_{x=0}^{N-1} \mathrm{e}^{2\pi \mathrm{i} xy/N} f(x).$$

QFT 是作用在计算基上的幺正演化：

$$QFT_N |x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \mathrm{e}^{2\pi \mathrm{i} xy/N} |y\rangle .$$

区别

QFT 不输出长度 N 的经典数组；它输出的是一个量子态。算法只测量其中少量信息，但这些信息因干涉集中在周期相关位置。

若 $N = 2^n$，QFT 可用 $O(n^2)$ 个门实现；经典 FFT 对 N 维向量需 $O(N \log N) = O(n2^n)$ 次操作。

QFT 的二进制相位展开

令

$$x = x_0 + 2x_1 + \cdots + 2^{n-1}x_{n-1}, \qquad y = y_0 + 2y_1 + \cdots + 2^{n-1}y_{n-1}.$$

相位为

$$\frac{2\pi xy}{2^n}.$$

只保留模 2π 后，得到二进制小数形式：

$$\frac{xy}{2^n} \bmod 1 = y_{n-1}(0.x_0) + y_{n-2}(0.x_1x_0) + \cdots + y_0(0.x_{n-1}\cdots x_0).$$

因此

$$QFT|x_{n-1}\cdots x_0\rangle = \frac{1}{2^{n/2}}\left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0.x_0}|1\rangle\right) \otimes \left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0.x_1x_0}|1\rangle\right) \otimes \cdots .$$

量子相位估计

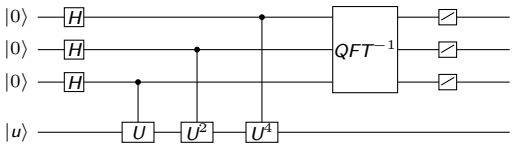
设

$$U|u\rangle = \mathrm{e}^{2\pi \mathrm{i}\phi}|u\rangle,$$

目标是估计 $\phi \in [0,1)$ 的二进制展开

$$\phi = 0.\phi_1\phi_2\cdots\phi_m.$$

量子线路是：辅助寄存器做 $H^{\otimes m}$，再依次控制 U^{2^j}，最后做 QFT^{-1}。



相位估计的状态推导

辅助寄存器先变为

$$\frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} |k\rangle .$$

控制幺正作用为

$$|k\rangle\,|u\rangle \longmapsto |k\rangle\, U^k\,|u\rangle = \mathrm{e}^{2\pi \mathrm{i} k\phi}\,|k\rangle\,|u\rangle .$$

因此辅助寄存器处于

$$\frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} \mathrm{e}^{2\pi \mathrm{i} k\phi}\,|k\rangle .$$

若 ϕ 恰好有 m 位二进制展开，记 $j = 2^m\phi$，则

$$\frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} \mathrm{e}^{2\pi \mathrm{i} kj/2^m}\,|k\rangle = QFT|j\rangle .$$

再施加 QFT^{-1} 即得到

$$|j\rangle = |\phi_1\phi_2\cdots\phi_m\rangle .$$

因数分解

要分解奇合数 N。随机选 $a < N$，先算

$$\gcd(a, N).$$

若不为 1，已经找到因子。否则寻找 a 模 N 的阶 r:

$$a^r \equiv 1 \pmod{N}.$$

若 r 为偶数，则

$$a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \pmod{N}.$$

若

$$a^{r/2} \not\equiv \pm 1 \pmod{N},$$

则

$$\gcd(a^{r/2} - 1, N), \qquad \gcd(a^{r/2} + 1, N)$$

给出非平凡因子。量子部分就是高效找 r。

Shor 算法

定义

$$U_a |y\rangle = |ay \bmod N\rangle .$$

若 r 是 a 的阶，则轨道

$$|1\rangle , |a\rangle , \left|a^2\right\rangle , \ldots , \left|a^{r-1}\right\rangle$$

长度为 r。构造

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{m=0}^{r-1} \mathrm{e}^{-2\pi \mathrm{i} s m/r} |a^m \bmod N\rangle .$$

作用 U_a：

$$\begin{aligned} U_a |u_s\rangle &= \frac{1}{\sqrt{r}} \sum_{m=0}^{r-1} \mathrm{e}^{-2\pi \mathrm{i} s m/r} \left|a^{m+1} \bmod N\right\rangle \\ &= \mathrm{e}^{2\pi \mathrm{i} s/r} |u_s\rangle . \end{aligned}$$

于是相位估计可给出 s/r。

量子计算机的物理实现

硬件必须同时满足的条件

一台可扩展量子计算机至少需要同时满足：

1. 可初始化：快速、重复地准备低熵初态，例如 $|0\rangle^{\otimes n}$。
2. 长相干时间：T_1, T_2 相比门时间和纠错周期足够长。
3. 高保真单比特控制：任意 Bloch 球旋转，且串扰可控。
4. 两比特纠缠门：如 CZ、CNOT、iSWAP 或平台原生等价门。
5. 高保真中途读出与重置：测量不能淹没 syndrome 信息。
6. 可扩展连接和并行控制：布线、寻址、泄漏、频率拥挤和标定成本可管理。

现在最关键的评价口径

物理 qubit 数只是容量。更核心的是

$$p_{1q},\quad p_{2q},\quad p_{\mathrm{meas}},\quad t_{\mathrm{cycle}},\qquad p_L(d)$$ 是否随 code distance 增大而下降。

超导量子比特：transmon、可调耦合器和表面码

超导 qubit 通过 Josephson 结产生非谐性，只取最低两个能级作为

$$|0\rangle, \quad |1\rangle, \qquad H \simeq 4E_C(n - n_g)^2 - E_J \cos\phi.$$

单比特门由微波脉冲实现；两比特门通过总线、交叉共振或可调耦合器得到有效相互作用，例如

$$H_{\text{int}} \sim J(X_1X_2 + Y_1Y_2), \qquad \chi Z_1Z_2.$$

当前前沿

二维近邻结构天然适配表面码。Google Willow 已演示 $d = 5, 7$ 表面码 memory；$d = 7$ 使用 101 个量子比特，逻辑错误率约为 1.43×10^{-3}/cycle，且达到 beyond breakeven。IBM Heron 路线则强调固定频率 qubit、可调耦合器和 EPLG/CLOPS 等系统指标。

Acharya et al., Nature 2025；IBM Quantum hardware roadmap。

离子阱：运动模、QCCD 和极高门保真度

离子阱中 qubit 是离子的内部态。Mølmer–Sørensen 型门用自旋依赖力耦合内部态和集体运动模：

$$H_{\mathrm{MS}} \propto \left(a e^{-i\delta t} + a^{\dagger} e^{i\delta t}\right) S_{\phi}, \qquad S_{\phi} = \sum_{j} (\cos\phi\, X_j + \sin\phi\, Y_j).$$

若相空间轨迹闭合，运动模复原，只留下几何相位，从而得到纠缠门。

当前前沿

QCCD 架构通过离子搬运连接不同操作区。Quantinuum Helios 报告 98 个 $^{137}\mathrm{Ba}^{+}$ qubit，平均单比特门 infidelity 2.5×10^{-5}，两比特门 7.9×10^{-4}，SPAM 4.8×10^{-4}。Oxford Ionics/IonQ 的电子控制 smooth gate 在两离子实验中给出 $> 99.99\%$ 两比特门保真度。

Ransford et al., arXiv:2511.05465；Ballance et al., arXiv:2510.17286。

中性原子：Rydberg 门、可重构阵列和擦除错误

中性原子阵列用光镊排布，常把 qubit 编码在超精细态或亚稳态。两比特门仍基于 Rydberg blockade：

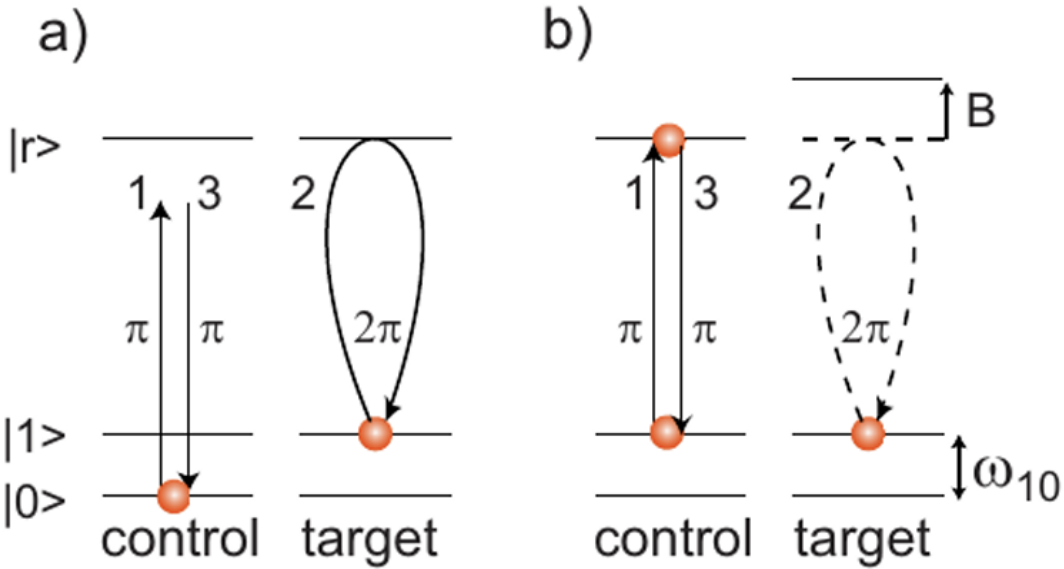
$$|1\rangle \leftrightarrow |r\rangle\,, \qquad H_{rr} = V_{rr}\,|rr\rangle\langle rr|\,, \qquad V_{rr} \gg \Omega.$$

双激发被 blockade 后，脉冲序列可实现 CZ 型相位门。

当前前沿

光镊重排给出可编程连接，原子损失又可转化为可探测的 erasure 信息。公开结果中，448 个中性原子已用于实现容错架构要素，四轮表面码表征给出 $2.14(13)\times$ below-threshold 表现，并演示最多 96 个 $d = 4$ logical qubit 同时活动。另有 6100 原子光镊阵列显示该平台的规模潜力，但这不是完整门模型计算机。

Bluvstein et al., Nature 2025；Manetsch et al., Nature 2025。


a)
|r>
1
3
2
π
π
2π
|1>
|0>
control
target
b)
B
1
3
2
π
π
2π
ω10
control
target

其他路线

平台	先进路线	公开尖端指标示例	主要瓶颈
超导	transmon + 可调耦合器 + 表面码	$d = 7$ surface-code memory，$p_L \simeq 1.43 \times 10^{-3}$/cycle	退相干、串扰、泄漏、布线
离子	QCCD、电子控制、smooth gate	商用系统 $p_{2q} \simeq 7.9 \times 10^{-4}$；两离子实验 $> 99.99\%$	门速、搬运、并行度
中性原子	光镊重排、Rydberg 门、erasure conversion	448 原子 QEC 架构；最多 96 个 logical qubit 活动	Rydberg 误差、损失、重装载
硅自旋	CMOS 兼容量子点、交换门	300 mm foundry 单元中单/两比特控制均超过 99%	均匀性、控制线、互连
光子/拓扑	cluster state、fusion；Majorana 方向仍在验证	更偏长期容错架构，还未形成通用可编程领先指标	损耗、确定性门、验证

Steinacker et al., Nature 2025；Google Willow、Quantinuum Helios、neutral-atom QEC 公开结果。

量子纠错与容错计算

量子纠错的一般问题

编码是把逻辑 Hilbert 空间嵌入物理 Hilbert 空间：

$$V : \mathcal{H}_L \hookrightarrow \mathcal{H}_P, \qquad \rho_L \mapsto V\rho_L V^\dagger.$$

噪声信道为

$$\mathcal{E}(\rho) = \sum_a E_a \rho E_a^\dagger.$$

目标是找恢复信道 $\mathcal{R}$，使得在 code subspace 上

$$(\mathcal{R} \circ \mathcal{E})(V\rho_L V^\dagger) = V\rho_L V^\dagger, \qquad \forall \rho_L.$$

记 code projector

$$P = VV^\dagger.$$

syndrome measurement 应该知道发生了什么错误，但不能知道逻辑态 ρ_L。

Knill–Laflamme 条件

错误集合 $\{E_a\}$ 可纠正，当且仅当存在矩阵 α_{ab} 使

$$PE_a^\dagger E_b P = \alpha_{ab} P, \qquad \forall a, b.$$

等价地，对任意逻辑基 $|i_L\rangle, |j_L\rangle$：

$$\langle i_L | E_a^\dagger E_b | j_L \rangle = \alpha_{ab} \delta_{ij}.$$

解释：

1. $i \neq j$ 时为 0：不同逻辑态出错后仍保持正交，能被恢复。
2. $i = j$ 时不依赖 i：错误 syndrome 的分布不携带逻辑态信息。

三比特 bit-flip code

编码：

$$|0_L\rangle = |000\rangle\,, \qquad |1_L\rangle = |111\rangle\,.$$

可纠正错误集合

$$\{I, X_1, X_2, X_3\}.$$

用稳定子

$$g_1 = Z_1Z_2, \qquad g_2 = Z_2Z_3$$

读取 syndrome：

error	Z_1Z_2	Z_2Z_3	correction
I	$+$	$+$	I
X_1	$-$	$+$	X_1
X_2	$-$	$-$	X_2
X_3	$+$	$-$	X_3

测量 Z_1Z_2, Z_2Z_3 只比较相邻比特是否相同，不区分 $\alpha\,|000\rangle + \beta\,|111\rangle$ 中的 α, β。

三比特 code 如何改进错误概率

假设每个物理比特独立 bit-flip，概率 p。三比特重复码能纠正 0 个或 1 个错误，因此成功概率

$$P_{\text{succ}} = (1-p)^3 + 3p(1-p)^2.$$

失败概率

$$\begin{aligned} P_{\text{fail}} &= 1 - P_{\text{succ}} \\ &= 3p^2(1-p) + p^3 = 3p^2 - 2p^3. \end{aligned}$$

对小 p，

$$P_{\text{fail}} = O(p^2),$$

线性项消失。

量子测量的作用

如果错误是相干的 $|\psi\rangle \mapsto |\psi\rangle + \eta X_1 |\psi\rangle$，syndrome 测量会把它投影到无错误或 X_1 错误子空间，再做离散修正。

phase-flip code

phase flip 是 Z 错误。因为

$$HZH = X, \qquad HXH = Z,$$

可把 bit-flip code 换到 X 基：

$$|0_L\rangle = |+++\rangle, \qquad |1_L\rangle = |---\rangle.$$

稳定子变为

$$g_1 = X_1X_2, \qquad g_2 = X_2X_3.$$

它能纠正单个 Z_i 错误。syndrome 表与 bit-flip code 相同，只是把

$$X_i \leftrightarrow Z_i, \qquad Z_iZ_j \leftrightarrow X_iX_j.$$

要点

量子纠错必须同时处理 bit 和 phase；只保护计算基布居远远不够。

Shor 九比特码

Shor code 把 phase-flip code 和 bit-flip code 级联：

$$|0_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)^{\otimes 3},$$

$$|1_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3}.$$

结构：

1. 每个三比特 block 内用 Z_iZ_j 检测 bit flip；
2. 三个 block 之间用相对相位检测 phase flip；
3. 任意单比特 Pauli 错误 X, Y, Z 都可纠正，因为 $Y = \mathrm{i}XZ$。

任意单比特错误

一般错误 $E = aI + bX + cY + dZ$ 是 Pauli 错误的线性组合；若 I, X, Y, Z 都能纠正，E 也能纠正。

稳定子码的一般语言

稳定子群 S 是 Pauli 群的交换子群。code space 定义为所有稳定子的 $+1$ 公共本征空间：

$$\mathcal{C} = \{|\psi\rangle : g|\psi\rangle = |\psi\rangle\,,\ \forall g \in S\}.$$

若有 r 个独立稳定子，编码量子比特数为

$$k = n - r.$$

错误 E 的 syndrome 由

$$g_j E = (-1)^{s_j} E g_j, \qquad s_j \in \{0, 1\}$$

给出。测量 g_j 得到 $(-1)^{s_j}$，然后根据 syndrome 选择恢复 Pauli。

逻辑算符

逻辑 Pauli 必须与所有稳定子对易，但不能属于稳定子群本身：

$$\bar{P} \in N(S) \setminus S.$$

距离和可纠错错误数

稳定子码记作

$$[[n, k, d]].$$

距离 d 是能在 code space 内产生非平凡逻辑作用的最小 Pauli 权重：

$$d = \min\{\mathrm{wt}(P) : P \in N(S) \setminus S\}.$$

能够纠正任意

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

个物理量子比特错误。原因是若两个权重不超过 t 的错误 E_a, E_b 不可区分，则

$$E_a^\dagger E_b$$

重量不超过 $2t < d$，不能是非平凡逻辑算符；因此要么给出不同 syndrome，要么只差稳定子。

容错计算的基本要求

如果纠错电路本身会把一个物理错误扩散成多个错误，code 可能立刻失效。因此容错操作要求错误传播受控。

1. **容错制备**：制备 logical $|0_L\rangle, |+_L\rangle$ 时不能把单错误变成高权重错误。
2. **容错门**：最好 transversal，即每个物理门只连接不同 code block 的对应比特。
3. **容错测量**：syndrome 提取需要防止 ancilla 错误反向传播到数据比特。

阈值定理的定性表述：若物理错误率低于某个阈值，并且噪声足够局域、独立，则通过级联编码或拓扑码可以把逻辑错误率压到任意低，代价是多项式或准多项式资源开销。

纠错真的降低错误率吗

以单 qubit depolarizing channel 为例：

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

不纠错时，infidelity 一阶随 p 增长。
若用能纠正任意单 qubit 错误的 9 qubit code，并假设每个物理 qubit 独立错误，则所有零错误和单错误都可纠正：

$$P_{\le 1} = (1-p)^9 + 9p(1-p)^8.$$

逻辑失败从二阶开始：

$$1 - P_{\le 1} = O(p^2).$$

代价

错误率阶数降低，代价是更多 qubit、更深 syndrome 电路和更复杂的容错门。

容错阈值和大规模量子计算

阈值定理的定性表述：

Threshold theorem

若物理门错误率低于某个平台/编码/噪声模型对应的阈值，并且错误足够局域、相关性可控，则通过量子纠错和容错门，可以把逻辑错误率压到任意低；资源开销随目标精度多项式增长。

容错计算需要：

- 重复 syndrome measurement；
- fault-tolerant Clifford gates；
- 非 Clifford 资源，例如 magic state distillation；
- 足够低的泄漏、串扰和相关错误。

要点

这就是为什么物理 qubit 数量多不是决定量子计算能否实用的唯一要素。

复杂度视角：量子计算不是万能指数加速

常见复杂度类：

$$P \subseteq BPP \subseteq BQP \subseteq PSPACE.$$

- Shor 算法说明 factoring 和 discrete log 在 BQP 中。
- Grover 对无结构搜索只给二次加速，而且这是最优的。
- 一般 NP-complete 问题是否能被量子计算多项式求解，目前没有证据表明可以。

参考文献 I

M. Lukin, *Physics 160 Lecture Notes*, notes typeset by E. Rosenfeld and M. Bhaskar, Harvard University, 2021.

M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Edition, Cambridge University Press, 2010.

X. Yuan, *Lecture Notes on Quantum Information Technology*, Peking University, 2025.

J. Preskill, *Lecture Notes for Physics 229: Quantum Information and Computation*, California Institute of Technology.

N. D. Mermin, *Quantum Computer Science: An Introduction*, Cambridge University Press, 2007.

D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society A* **439**, 553–558, 1992.

D. R. Simon, "On the power of quantum computation," *SIAM Journal on Computing* **26**, 1474–1483, 1997.

P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *FOCS*, 1994.

L. K. Grover, "A fast quantum mechanical algorithm for database search," *STOC*, 1996.

C. H. Bennett et al., "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters* **70**, 1895–1899, 1993.

C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters* **69**, 2881–2884, 1992.

R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Physical Review Letters* **86**, 5188–5191, 2001.

B. Hensen et al., "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres," *Nature* **526**, 682–686, 2015.

参考文献 II

C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175–179, 1984.

A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters* **67**, 661–663, 1991.

M.-D. Choi, "Completely positive linear maps on complex matrices," *Linear Algebra and its Applications* **10**, 285–290, 1975.

K. Kraus, *States, Effects, and Operations: Fundamental Notions of Quantum Theory*, Springer, 1983.

A. Uhlmann, "The transition probability in the state space of a *-algebra," *Reports on Mathematical Physics* **9**, 273–279, 1976.

E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Physical Review A* **55**, 900–911, 1997.

D. Gottesman, *Stabilizer Codes and Quantum Error Correction*, PhD thesis, Caltech, 1997.