量子信息手写笔记（整理版）

Contents

1 基、基变换与酉矩阵

1.1 基向量与基变换矩阵

两组基向量分别为 $\{|e_1\rangle,\dots,|e_n\rangle\}$ 与 $\{|f_1\rangle,\dots,|f_n\rangle\}$。把基向量按列排成矩阵：

$$E=\big(|e_1\rangle\ |e_2\rangle\ \cdots\ |e_n\rangle\big),\quad F=\big(|f_1\rangle\ |f_2\rangle\ \cdots\ |f_n\rangle\big).$$

定义基变换矩阵

$$U_{ij}=\langle e_i|f_j\rangle.$$

新基向量在旧基下展开为

$$|f_j\rangle=\sum_i U_{ij}|e_i\rangle.$$

矩阵形式写作

$$F=E\,U.$$

对任意态 $|\psi\rangle$，在旧基与新基下分别展开：

$$|\psi\rangle=\sum_i c_i|e_i\rangle=\sum_j c'_j|f_j\rangle,$$

其中

$$\vec{c}=\begin{pmatrix}c_1\\ \vdots\\ c_n\end{pmatrix},\qquad \vec{c}\,'=\begin{pmatrix}c'_1\\ \vdots\\ c'_n\end{pmatrix}$$

为展开系数组成的列向量。两者满足

$$\vec{c}\,'=U^\dagger\vec{c},\qquad \vec{c}=U\vec{c}\,'.$$

若 E,F 为正交归一基，则 U 为酉矩阵（$U^\dagger U=I$）。

1.2 算符的基变换

矩阵元定义（以旧基 E 为例）：

$$A^{(E)}_{ij}=\langle e_i|A|e_j\rangle.$$

算符在新基下的矩阵表示为

$$A^{(F)}=U^\dagger A^{(E)}U.$$

2 本征方程与对角化

$$A|\phi\rangle=\lambda|\phi\rangle,\qquad (A-\lambda I)|\phi\rangle=0.$$

非平凡解要求

$$\det(A-\lambda I)=0$$

从而求得本征值 λ，再代回求本征向量。

厄米矩阵要点　若 $A=A^\dagger$，则本征值全为实数，本征向量可取正交归一基；因此 A 可被酉对角化：$A=U\Lambda U^\dagger$，其中 U 的列向量就是按同一顺序排列的本征向量，$\Lambda=\mathrm{diag}(\lambda_1,\lambda_2,\dots)$ 为对应本征值的对角矩阵。

3 单比特态与 Bloch 球

任意纯态可写成

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle,$$

其中 $\theta \in [0,\pi]$ 为极角，$\varphi \in [0,2\pi]$ 为方位角。纯态对应 Bloch 球面上的点。

4 密度矩阵

$$\rho = |\psi\rangle\langle\psi|.$$

基本性质：$\rho^\dagger = \rho$，$\rho \geq 0$，$\mathrm{tr}(\rho) = 1$。

纯态与混态 纯态满足 $\rho^2 = \rho$，$\mathrm{tr}(\rho^2) = 1$；混态满足 $\mathrm{tr}(\rho^2) < 1$。一般混态可写成

$$\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|, \quad p_k \geq 0,\ \sum_k p_k = 1,$$

并可酉对角化为

$$\rho = U\,\mathrm{diag}(p_1, p_2, \ldots)\,U^\dagger.$$

5 Bell 态与最大纠缠

四个 Bell 态：

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \qquad |\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).$$

它们都是最大纠缠态。

5.1 对 Φ^+ 施加单比特门

在第一比特上作用（超密编码常用）：

操作	结果
I	$\|\Phi^+\rangle$
X	$\|\Psi^+\rangle$
Z	$\|\Phi^-\rangle$
iY (XZ)	$\|\Psi^-\rangle$

6 量子超密编码

预共享 Bell 态 $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$。按时间顺序：

1. t_0：Alice 与 Bob 共享 $|\Phi^+\rangle$（Alice 持第 1 比特，Bob 持第 2 比特）。
2. t_1：Alice 将 2 比特信息编码为本地操作

   $$00 \to I, \quad 01 \to X, \quad 10 \to Z, \quad 11 \to XZ\ (= iY),$$

   并把她的量子比特发送给 Bob。
3. t_2：Bob 进行 Bell 测量：先对第 1 比特施 CNOT（第 1 控第 2），再对第 1 比特施 H，最后在计算基测量两比特。
4. t_3：测量结果 $\{00, 01, 10, 11\}$ 分别对应 $\{|\Phi^+\rangle, |\Psi^+\rangle, |\Phi^-\rangle, |\Psi^-\rangle\}$，解码得到 Alice 的 2 比特信息。

结论：1 个量子比特 + 1 对纠缠可传 2 比特经典信息。

7 量子隐形传态

预共享 Bell 对，待传态为 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$。按时间顺序：

1. t_0：Alice 与 Bob 共享 Bell 对（Alice 持第 2 比特，Bob 持第 3 比特），Alice 还有待传态第 1 比特 $|\psi\rangle$。
2. t_1：Alice 对第 1、2 比特执行 CNOT（第 1 控第 2），再对第 1 比特施 H。
3. t_2：Alice 在计算基测量第 1、2 比特，得到 $(M_1, M_2) \in \{0,1\}^2$，并通过经典信道告知 Bob。
4. t_3：Bob 对第 3 比特施加纠正

$$X^{M_2} Z^{M_1},$$

得到原态 $|\psi\rangle$。

该过程不违反不可克隆与超光速通信（经典信道不可省）。

8 发展史与里程碑（背诵）

- 1992：Bennett 与 Wiesner 提出量子超密编码（量子密集编码）。
- 1993：Bennett 等提出量子隐形传态方案。
- 1996：首个超密编码实验（光子偏振编码）。
- 2004：原子系综中的超密编码实验。
- 2008：连续变量超密编码实验。
- 2012：超导量子比特超密编码实验。
- 2017：高维纠缠的超密编码（利用高维系统传更多信息）。
- 2010：自由空间 16 km 量子隐形传态实验。

9 实验装置与关键技术（背诵）

- **纠缠源：**需要高保真度 Bell 态；常见平台有光子偏振、原子系综、超导量子比特等。
- **Bell 态制备：**从 $|00\rangle$ 出发，$H \otimes I$ + CNOT 可制备 $|\Phi^+\rangle$。
- **Bell 基测量：**标准实现为 CNOT（第 1 控第 2）+ H（第 1 比特）+ 计算基测量；完全区分 4 个 Bell 态在实验上有技术难度。
- **经典信道：**超密编码需要传送 1 个量子比特；隐形传态需要传 2 个经典比特；经典信道限制整体速度，不可超光速。
- **退相干与损耗：**纠缠在传输/存储中易退相干，探测效率与信道损耗会降低保真度。

10 计算类背诵要点（导论/作业常考）

- **CNOT 作用：**$|ab\rangle \mapsto |a,\, b \oplus a\rangle$。
- **Bell 测量映射：** $|\Phi^+\rangle \to |00\rangle$，$|\Psi^+\rangle \to |01\rangle$，$|\Phi^-\rangle \to |10\rangle$，$|\Psi^-\rangle \to |11\rangle$（经 CNOT+H 后）。
- **超密编码映射：** $I \to |\Phi^+\rangle$，$X \to |\Psi^+\rangle$，$Z \to |\Phi^-\rangle$，$XZ(=iY) \to |\Psi^-\rangle$。
- **隐形传态纠正：**Bob 按 (M_1, M_2) 施加 $X^{M_2} Z^{M_1}$。
- **资源消耗：**超密编码与隐形传态均消耗 1 对纠缠；隐形传态还需 2 个经典比特。
- **互为对偶：**超密编码“量子 $\to$ 经典”，隐形传态“经典 $\to$ 量子”。

11 张量积与纠缠（背诵）

- 复合系统空间为张量积：$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$。

- 基向量：$\{|i\rangle \otimes |j\rangle\}$ 构成正交归一基。
- 内积规则：$\langle v_1 \otimes w_1 | v_2 \otimes w_2 \rangle = \langle v_1 | v_2 \rangle \langle w_1 | w_2 \rangle$。
- 可分态：$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$；否则为纠缠态。
- Bell 态是最大纠缠态，其子系统约化密度矩阵为最大混合态 $\frac{I}{2}$。

12 密度矩阵与偏迹（背诵）

- $\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|$，满足 $\rho^\dagger = \rho$，$\rho \geq 0$，$\mathrm{tr}(\rho) = 1$。
- 纯态：$\rho^2 = \rho$，$\mathrm{tr}(\rho^2) = 1$；混态：$\mathrm{tr}(\rho^2) < 1$。
- 约化密度矩阵：$\rho_A = \mathrm{tr}_B(\rho_{AB})$，保留子系统 A 的全部统计信息。
- 期望值：$\langle A \rangle = \mathrm{tr}(\rho_A A)$。
- 酉变换下不变量：$\mathrm{tr}(U\rho U^\dagger) = \mathrm{tr}(\rho)$。

13 贝尔不等式与量子相关（背诵）

- CHSH 经典上界：$\langle \hat{B} \rangle \leq 2$。
- Tsirelson 上界：$\langle \hat{B} \rangle \leq 2\sqrt{2}$（量子相关性强于经典）。
- 实验违反 CHSH 说明局域隐变量理论与量子力学不相容。

14 不可克隆定理（背诵）

- 不存在对任意未知态都成立的克隆变换：$U|\psi\rangle|0\rangle \neq |\psi\rangle|\psi\rangle$。
- 原因来自线性性；若能克隆两态，则对任意叠加态会矛盾。
- 含义：未知量子态不能复制，QKD 的安全性基础之一。

15 量子密钥分发 QKD（背诵）

- QKD 只分发密钥，不直接传输消息（如 BB84/E91 思想）。
- 任何窃听测量会引入扰动与错误率，可被检测。
- 需要**认证的经典信道**完成基筛选、纠错与隐私放大。
- 安全性根源：测量扰动与不可克隆定理。

16 量子计算类型与平台（背诵）

- 两类量子计算：**通用门电路量子计算**与 **量子退火/绝热计算**（Ising/QUBO 优化）。
- 量子线路模型：初始化 $\rightarrow$ 量子门序列 $\rightarrow$ 测量，整体可逆演化。
- 通用门集：任意单比特酉门 + CNOT（常用 $\{H, S, T, \mathrm{CNOT}\}$）。
- 典型算法：Shor（分解）、Grover（搜索）、QFT（量子傅里叶变换）。
- 平台概览：超导量子比特、离子阱、光子、核磁共振、金刚石 NV 色心、拓扑量子计算等。

17 量子通信与网络（背诵）

- 典型任务：量子隐形传态、超密编码、QKD、量子中继。
- 纠缠与经典信道共同完成通信；纠缠本身不传递可控信息。
- 代表性网络：DARPA 量子网络、欧洲 SECOQC、日本东京量子网络、中国天地一体化量子通信网络。

18 常见量子门（简表）

单比特门:

$$X=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix},$$

$$S=\begin{pmatrix}1&0\\0&i\end{pmatrix},\quad T=\begin{pmatrix}1&0\\0&e^{i\pi/4}\end{pmatrix},\quad R_\alpha(\theta)=e^{-i\theta\sigma_\alpha/2}\ (\alpha=x,y,z).$$

双比特门：CNOT 定义为

$$|ab\rangle\mapsto|a,\,b\oplus a\rangle,$$

矩阵表示为 $\mathrm{CNOT}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$。常用通用门集：$\{H,S,T,\mathrm{CNOT}\}$。