量子信息基础

第七章：量子测量

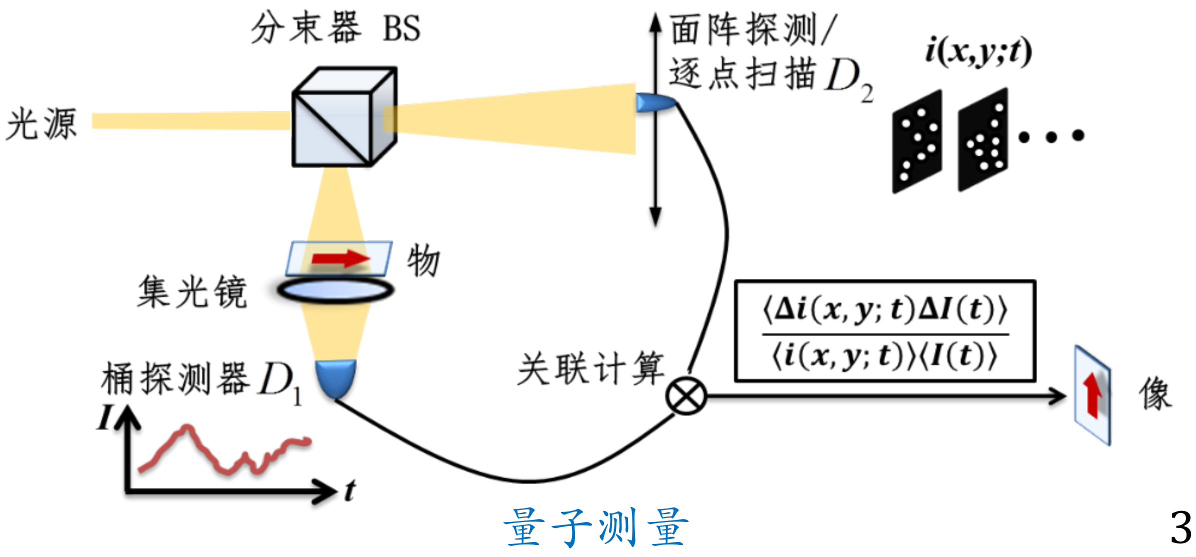
金潮渊
浙江大学信息与电子工程学院

浙江大学

C7-4 距离度量和量子纠错

课程回顾

- 量子成像技术是通过纠缠光子系统和混沌热辐射的非平庸二阶或高阶相干测量，复制物像，是物像空间的点对点成像关联的结果。主要介绍了两类鬼成像。包括利用了偶光子态非局域点对点关联和热光的二阶关联。
- 量子成像具有三个奇异特性：1.突破衍射极限；2.以非局域方式复制物像关系；3.抗扰动。都来源于多光子干涉。
- 利用鬼成像可以验证Popper的假想实验，Popper的预测结果与实验相同，也与量子力学的预测相同。产生佯谬的根源在于他将单粒子的测不准原理直接套用在双粒子系统上。



汉明距离(经典)

- 在信息论中，汉明距离(Hamming Distance)是一种衡量两个字符串差异的度量，它表示两个等长字符串在相同位置上不同字符的数量。

- 计算方式：对于两个等长的二进制字符串，汉明距离可以通过将它们进行异或运算，并统计结果中为1的个数来计算得出。例如，字符串“010111”和“110011”之间的汉明距离为2，因为这两个字符串有2个位置上的字符不同（第1和第4个位置）。

- 汉明距离在信息论、编码理论、密码学等领域都有广泛的应用。例如，在数字通信中，发送端将数据以某种结构格式发送到接收端，接收端通过计算汉明距离来确定收到的数据与期望的数据之间的区别，从而进行纠错操作或判断传输是否成功。此外，汉明距离也用于图像处理中的模板匹配和数字识别，通过计算两幅图像中对应位置为1的累计个数来衡量它们的相似度。

迹距离(经典)

- 怎样才能有效定义包含经典概率的信息之间的距离度量呢？比如，如果我们知道字母在一串词语中的出现频率，可否定义距离的概念？

- $\{p_x\}$和$\{q_x\}$同为定义在集合x上的概率分布，那么可以引入$\{p_x\}$和$\{q_x\}$之间的迹距离(trace distance)

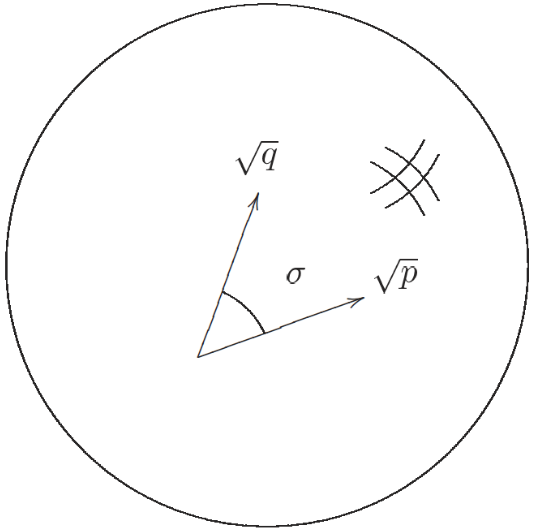
$$D(p_x, q_x) \equiv \frac{1}{2}\sum_x |p_x - q_x|$$

- 迹距离具有对称性，而且满足三角不等式

$$D(p_x, q_x) = D(q_x, p_x) \qquad \text{对称性}$$

$$D(p_x, q_x) \le D(p_x, r_x) + D(r_x, q_x) \qquad \text{三角不等式}$$

保真度(经典)



$F(p,q)=\sqrt{p}.\sqrt{q}=\cos(\sigma)$

- 另一种针对经典概率分布的距离度量，称为保真度(Fidelity)，一般定义为

$$F(p_x,q_x)\equiv\sum_x\sqrt{p_x q_x}$$

- 当$\{p_x\}$和$\{q_x\}$完全相等时，保真度等于1，代表信息没有失真

$$F(p_x,q_x)=\sum_x p_x=1$$

- 由于$\{p_x\}$和$\{q_x\}$都是归一化的概率，$\sqrt{p_x}$和$\sqrt{q_x}$可以想象为半径为1的球面上的点，而保真度是它们的内积。

迹距离(量子)

- 对于两个量子态的密度矩阵算符ρ和σ，引入ρ和σ之间的迹距离(trace distance)概念

$$D(\rho,\sigma) \equiv \frac{1}{2}\mathrm{tr}|\rho-\sigma|$$

- 假设ρ和σ可对易，那么他们有共同的本征函数系

$$\rho=\sum_i r_i|i\rangle\langle i| \qquad \sigma=\sum_i s_i|i\rangle\langle i|$$

以正交归一本征函数系为例

$$D(\rho,\sigma)=\frac{1}{2}\mathrm{tr}\sum_i|(r_i-s_i)|i\rangle\langle i||=D(r_i,s_i)$$

这样量子态之间的迹距离回归到本征值之间的迹距离，即经典迹距离。

迹距离(量子)

例1. 假定有两个量子态

$$\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| \qquad \sigma = \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|$$

他们之间的迹距离

$$D(\rho,\sigma) = \frac{1}{2} tr\left|\sum_i |r_i - s_i||i\rangle\langle i|\right| = \frac{1}{2}\left(\left|\frac{3}{4} - \frac{2}{3}\right| + \left|\frac{1}{4} - \frac{1}{3}\right|\right) = \frac{1}{12}$$

保真度(量子)

- 对于两个量子态的密度矩阵算符ρ和σ，引入ρ和σ之间的保真度(fidelity)概念

$$F(\rho,\sigma) \equiv \mathrm{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}$$

这个定义看起来对两个量子态不对称！但实际上是对称的。

- 假设ρ和σ可对易，那么他们有共同的本征函数系

$$\rho = \sum_i r_i |i\rangle\langle i| \qquad \sigma = \sum_i s_i |i\rangle\langle i|$$

以正交归一本征函数系为例

$$F(\rho,\sigma) \equiv \mathrm{tr}\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}} = \mathrm{tr}\sqrt{\sum_i r_i s_i |i\rangle\langle i|} = \mathrm{tr}\left(\sum_i \sqrt{r_i s_i}|i\rangle\langle i|\right) = \sum_i \sqrt{r_i s_i} = F(r_i, s_i)$$

这样量子态之间的保真度回归到本征值之间的保真度，即经典保真度。

保真度(量子)

例2. 假定有纯态$|\psi\rangle$和混态ρ，求他们之间的保真度

$$F(|\psi\rangle,\rho)=\mathrm{tr}\sqrt{\langle\psi|\rho|\psi\rangle|\psi\rangle\langle\psi|}=\sqrt{\langle\psi|\rho|\psi\rangle}$$

假定有纯态$|\psi\rangle$和纯态$|\phi\rangle$，求他们之间的保真度

$$F(|\psi\rangle,\rho)=\sqrt{\langle\psi|\rho|\psi\rangle}$$

令$\rho=|\phi\rangle\langle\phi|$

$$F(|\psi\rangle,|\phi\rangle)=|\langle\psi|\rho|\phi\rangle|$$

有时，纯态间的保真度定义为

$$F(|\psi\rangle,|\phi\rangle)=|\langle\psi|\rho|\phi\rangle|^2$$

量子误差

- 由于量子位、量子门和量子存储器受环境和别的量子器件的相互作用影响，肯定会发生不希望的量子纠缠，这些纠缠造成所考虑信息的退相干。在任何量子信息计算或存储过程中，总会有一定的概率出现失误。这就是量子误差。纠正误差的基本办法是：当存在发生误差机制的时侯，通过附加某种冗余信息，能够正确地解读出所要的信息。

- 从误差发生的部位来区分，误差的种类分为：
  - 存储误差(memory errors)
  - 运算误差(operation errors)

- 只有 当人们了解了怎样纠正误差之后，做一些与传递过程及时间相关的修改，人们就能纠正操作运行中的动态型误差。即量子纠错。

经典纠错

- 纠正误差的主要方法是基于冗余码(redundent code)的办法。比如，用3个比特位联合起来，共同表示“0”位和“1”位（逻辑比特）。即

$$0_{\mathrm{L}} = 000 \qquad 1_{\mathrm{L}} = 111$$

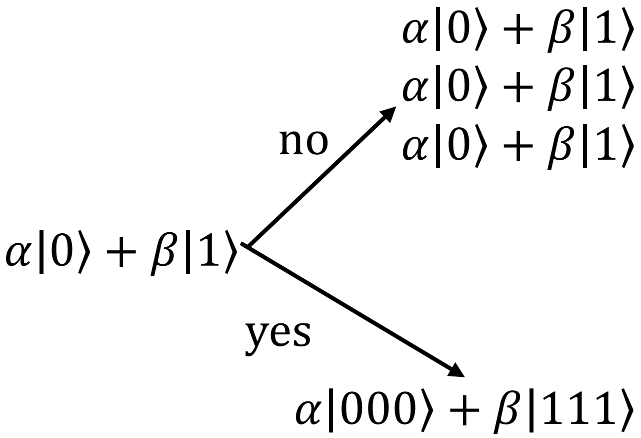
于是每个逻辑比特，实际上是由3个比特联合构成。任1逻辑比特的信息，在存储τ时间之后，无误差的概率为$\left(1-P(\tau)\right)^3$。发生1比特误差，比如原先是000，后来误成100或010或001中的任一种，其概率为$3P(\tau)\left(1-P(\tau)\right)^2$。发生2比特误差，比如原先是000，后来110或011或101中的任一种，其概率为$3P(\tau)^2\left(1-P(\tau)\right)$。发生3比特误差的概率为$3P(\tau)^3$。这时原先是000，后来是111。

- 经典纠错由如下测量所组成：假如3个比特全在同一状态上，就不做操作；假如它们在不同态上，我们就采用多数表决的原则去翻转、纠正那个处于少数的不同 状态的比特。现在来看纠正后失误的概率。纠正以后的r 时刻，我们得到维持在正确状态的概率为

$$P_c(\tau) = \left(1-P(\tau)\right)^3 + 3P(\tau)\left(1-P(\tau)\right)^2 = 1 - 3P(\tau)^2 - 2P(\tau)^3$$

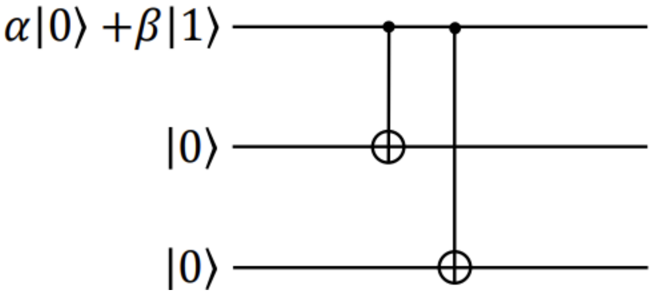
如果$P_c(\tau) > 1 - P(\tau)$，则$P(\tau) < 1/2$。

量子逻辑比特



- 对于量子纠错，设置重复量子比特是不可能的（量子不可克隆原理）。但是，我们可以利用量子纠缠来构造量子逻辑比特

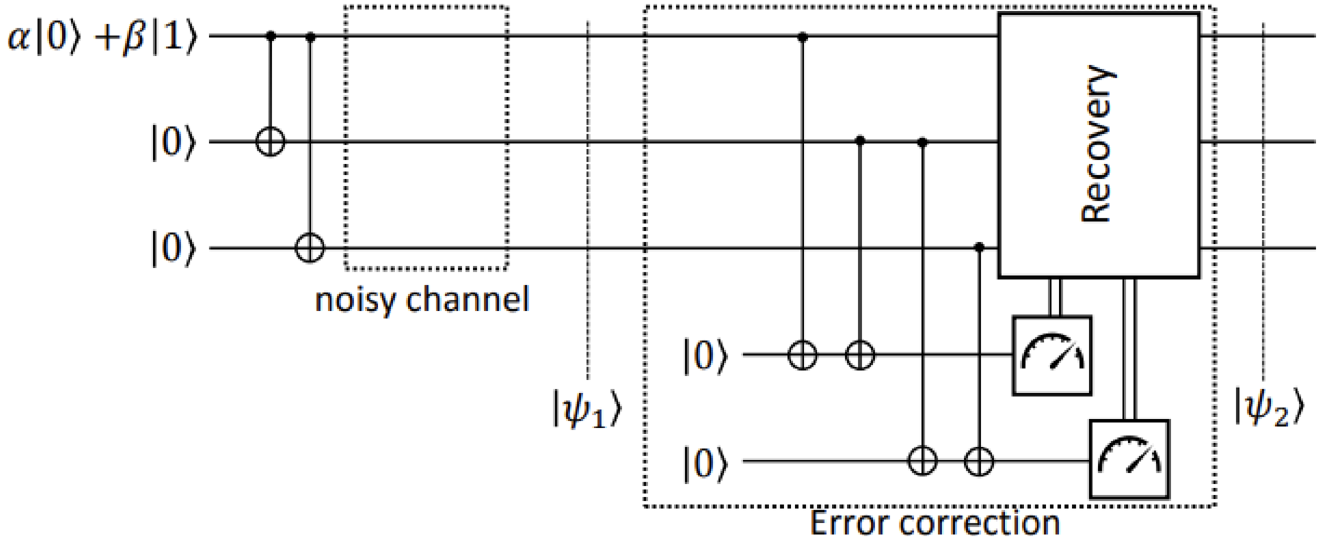
$$|0\rangle \longrightarrow |0_\mathrm{L}\rangle \equiv |000\rangle \qquad |1\rangle \longrightarrow |1_\mathrm{L}\rangle \equiv |111\rangle$$



- 如左图所示，我们可以利用简单排列CNOT门产生量子逻辑比特。

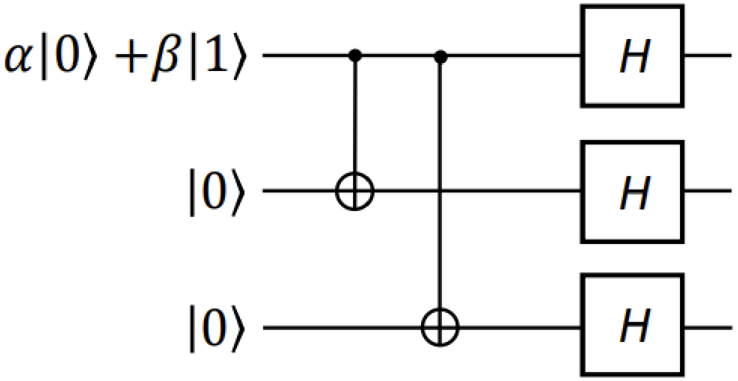
量子纠错

- 我们可以使用下面的量子回路和算法来实现自旋翻转的量子纠错



Bit-flip	$\lvert\psi_1\rangle$	M_1	M_2	Recovery	$\lvert\psi_2\rangle$
-	$\alpha\lvert 000\rangle + \beta\lvert 111\rangle$	0	0	$I \otimes I \otimes I$	$\alpha\lvert 000\rangle + \beta\lvert 111\rangle$
1	$\alpha\lvert 100\rangle + \beta\lvert 011\rangle$	1	0	$X \otimes I \otimes I$	$\alpha\lvert 000\rangle + \beta\lvert 111\rangle$
2	$\alpha\lvert 010\rangle + \beta\lvert 101\rangle$	1	1	$I \otimes X \otimes I$	$\alpha\lvert 000\rangle + \beta\lvert 111\rangle$
3	$\alpha\lvert 001\rangle + \beta\lvert 110\rangle$	0	1	$I \otimes I \otimes X$	$\alpha\lvert 000\rangle + \beta\lvert 111\rangle$

相位翻转



- 如左图所示，我们可以利用简单排列CNOT门和H门产生相位翻转的量子逻辑比特。

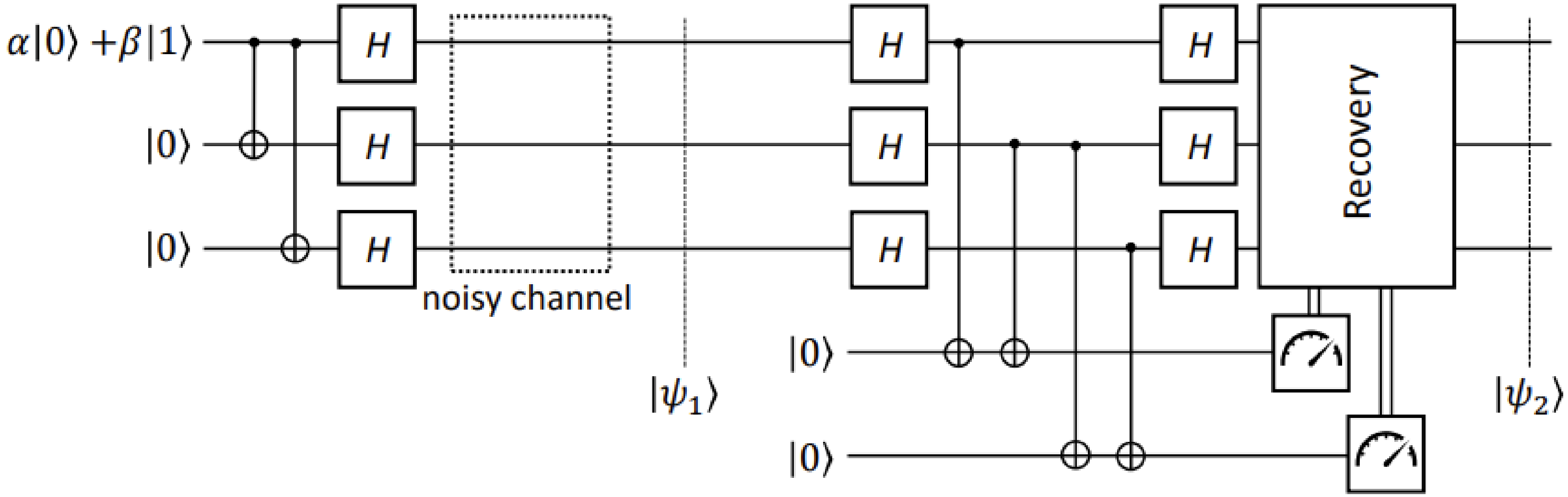
$$|0\rangle \longrightarrow |+_{\mathrm{L}}\rangle \equiv |{+}{+}{+}\rangle \qquad |1\rangle \longrightarrow |-_{\mathrm{L}}\rangle \equiv |{-}{-}{-}\rangle$$

- 其中

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

量子纠错(相位翻转)

- 我们可以使用下面的量子回路和算法来实现相位翻转的量子纠错

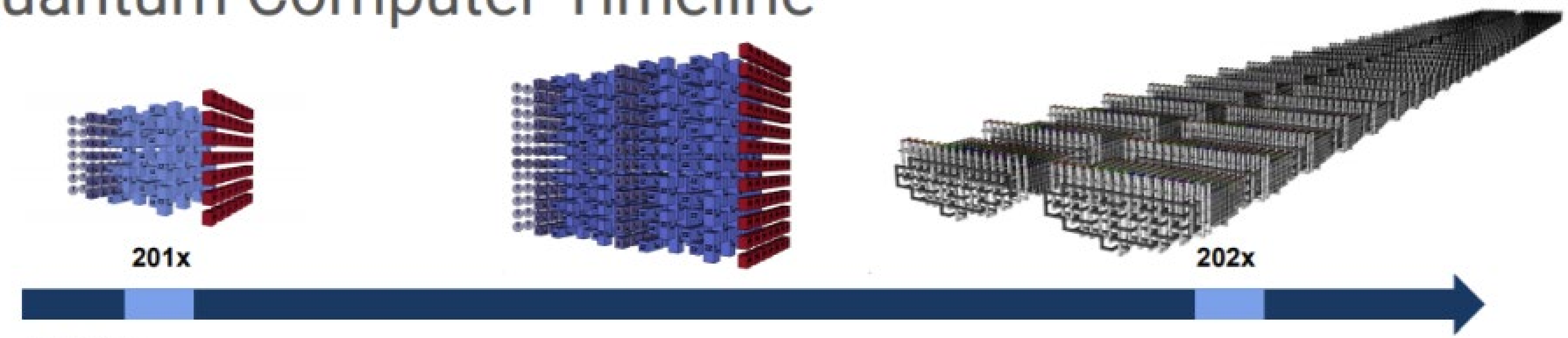


Ph-flip	$\|\psi_1\rangle$	M_1	M_2	Recovery	$\|\psi_2\rangle$
-	$\alpha\|+++\rangle+\beta\|---\rangle$	0	0	$I\otimes I\otimes I$	$\alpha\|+++\rangle+\beta\|---\rangle$
1	$\alpha\|-++\rangle+\beta\|+--\rangle$	1	0	$Z\otimes I\otimes I$	$\alpha\|+++\rangle+\beta\|---\rangle$
2	$\alpha\|+-+\rangle+\beta\|-+-\rangle$	1	1	$I\otimes Z\otimes I$	$\alpha\|+++\rangle+\beta\|---\rangle$
3	$\alpha\|++-\rangle+\beta\|--+\rangle$	0	1	$I\otimes I\otimes Z$	$\alpha\|+++\rangle+\beta\|---\rangle$

量子容错计算

- 量子优越性、专用量子模拟机、容错通用量子计算是量子计算发展的三个主要阶段

Quantum Computer Timeline



Quantum supremacy

Beyond classical computing capability demonstrated for a select computational problem

Pre-error corrected quantum processors

Early application wins expected for

- Simulation of Quantum Systems
- Optimization
- Sampling
- Quantum Neural Network

Error corrected quantum computer

Growing list of quantum algorithms for wide variety of applications with proven speedups

- Unstructured Search
- Factoring
- Semi-definite Programming
- Solving Linear Systems
- ...

参考文献

- 符合测量和延迟选择的内容主要参考：

  - Michael A. Nielsen and Isaac L. Chuang, Quantum Computation and Quantum Information (10th anniversary edition), Cambridge University Press (2016)。第9-10章。
  - 张永德，量子信息物理原理，科学出版社。第12章。
  - John Preskill, Quantum Computing (CST Part II), Lecture 13: Quantum Error Correction.