中国科学院大学课程讲义

量子信息与量子密码

中国科学院大学网络空间安全学院

密码学与信息安全基础教研室

授课教师：杨理

2020 年 11 月 21 日

前言

随着实验技术的进步，人类已能够独立操纵单个量子系统，量子科学和技术的发展于是成为我们这个时代科学技术进步伟大洪流的一个重要组成部分，量子信息、量子计算和量子密码等领域的发展已成为发达国家高新技术竞争的一个热点。

在量子信息科学的研究中，把量子态序列视为消息，对量子态序列提出信息论问题，是人类在信息概念上的巨大飞跃，是基于自然界基本定律对信息概念的自然推广，是量子信息科学的基石。经过四十年的努力，量子信息论已经基本建立起来（如：Holevo 定理（1964，1973），Schumacher 定理（1995），HSW 定理（1998），等等），这些工作与 C.Shannon 1948 年关于信息论的经典论文相对应。目前看来，实用量子信息系统的出现已无悬念，信息安全和保密领域所面临的一个新的课题是：如何保障量子信息系统的安全。深刻的分析表明，从根本上解决这个问题需要建立起涵盖量子信息系统和经典系统的新型密码学理论，这些工作与 C.Shannon 1949 年关于密码学的奠基性论文和后来几十年密码学的发展相对应。

量子密钥分配、量子掷币、量子承诺和 OT，及其它以经典消息为保护对象的量子算法，如某些量子秘密共享和量子公钥算法，这些工作的共同特点是利用量子物理学手段实现经典消息的密码学目标。这些工作可看作是一种密码技术上的新手段、新途径，不构成密码学研究的核心内容，我们称之为“狭义量子密码学”。由于经典信息是量子信息的一个子集（即计算基态的集合），建立在量子消息空间和量子密钥空间上、基于量子信息论和量子计算复杂性理论的密码学，才是涵盖经典密码学和各类量子密码协议的一个完整理论，我们称之为“广义量子密码学”或“量子信息密码学”。显然，面向经典消息的现代密码学和前述“狭义量子密码学”将作为“量子信息密码学”这个普遍理论的两个退化极限而存在。

从计算机理论来看，首先 Church-Turing 论题断言算法可计算函数类等于 Turing 机可计算函数类。大约半个世纪前又有人提出了强 Church-Turing 论题，即任何算法过程都可以用 Turing 机进行有效模拟。1980 年代英国物理学家 David Deutsch 试图借助物理学定律给这两个假设一个可信的基础。尽管他的努力失败了，但以他名字命名的量子算法及其后续发展对强 Church-Turing 论题构成了挑战，其中最有代表性的成果就是 Shor 的因子分解量子算法。此外，著名的 Grover 搜索算法也是 Deutsch 算法思想发展的结果。

这份讲义是依据 2005 年以来我在国科大及其前身中科院研究生院开设量子信息相关课程时所讲授的内容编写的，参考了国内外的一些教材和专著（见参考书目），并补充了该学科的若干研究前沿，包括我们自己的一些工作。本讲义从线性代数和量子力学预备知识讲起，介绍了量子通信、量子密码和早期量子算法，以及量子密码协议和量子安全性理论等内容；在量子计算方面主要讲授量子计算模型和量子算法，以及量子计算机物理实现的原理；最后介绍了量子纠错码和容错量子计算理论，以及量子信息论的基础内容。2017 年以来，我的研究生谢惠琴、刘慧、杨碧瑶、宋雅琪、刘霞、高文华、孙泽宇等同学参与了本讲义的编写、录入和编辑工作，特此致谢!

杨 理

2021 年 3 月 20 日

目录

第 1 章 线性代数与量子力学基础

§1.1 线性代数

1.1.1 矩阵的分解与直积

极式分解与奇异值分解是十分有用的工具，利用它们可以将一般的线性算子转化为酉算子和半正定算子的乘积。不加证明地给出下列定理：

定理 1.1.1（奇异值分解）设 A 是$m \times n$矩阵，$Rank(A) = r$，总可以找到一个 n 阶酉阵 U 和一个 m 阶酉阵 V 以及对角阵$s_0 = \begin{pmatrix} s_1 & & 0 \\ & \ddots & \\ 0 & & s_r \end{pmatrix}$，$s_1 \geq \cdots \geq s_r > 0$，使得表达式 A=VSU 成立。其中$S = \begin{pmatrix} s_0 & 0 \\ 0 & 0 \end{pmatrix}$.

上述定理即为矩阵 A 的奇异值分解，其中数$s_1, \cdots, s_r (> 0)$称为矩阵 A 的奇异值（即$A^\dagger A$的特征值的算术根）。

定理 1.1.2（极式分解）令 A 是向量空间 V 上的线性算子，则存在酉算子 U 和半正定算子 J 和 K 使得

$$A = UJ = KU, \tag{1.1.1}$$

其中 J 和 K 是唯一满足这些方程的半正定算子，定义为$J \equiv \sqrt{A^\dagger A}$和$K \equiv \sqrt{AA^\dagger}$。如果 A 可逆，则 U 是唯一的。$A = UJ$为 A 的左极式分解，$A = KU$为 A 的右极式分解。

推论 1.1.1（奇异值分解）令 A 是一方阵，则必存在酉矩阵 U、V 和一个非负对角阵 D 使得

$$\mathrm{A} = \mathrm{UDV}, \tag{1.1.2}$$

其中 D 的对角元称为 A 的奇异值。

（奇异值分解不只适用于方阵，具体应用定理 1.2.4 Schmidt 分解定理的证明）

定义 1.1.1（直积）给定矩阵 A 和 B，它们的直积（张量积）定义如下：

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix}. \tag{1.1.3}$$

例 1.1.1

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} \otimes \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 1 \times 2 \\ 1 \times 3 \\ 2 \times 2 \\ 2 \times 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 4 \\ 6 \end{bmatrix}, \tag{1.1.4}$$

$$\mathrm{X}\otimes\mathrm{Y}=\begin{bmatrix}0\cdot\mathrm{Y} & 1\cdot\mathrm{Y}\\ 1\cdot\mathrm{Y} & 0\cdot\mathrm{Y}\end{bmatrix}=\begin{bmatrix}0 & 0 & 0 & -\mathrm{i}\\ 0 & 0 & \mathrm{i} & 0\\ 0 & -\mathrm{i} & 0 & 0\\ \mathrm{i} & 0 & 0 & 0\end{bmatrix}. \tag{1.1.5}$$

直积具有如下性质：

1.$0\otimes A=A\otimes 0=0$;

2.$(A_1+A_2)\otimes B=A_1\otimes B+A_2\otimes B, A\otimes(B_1+B_2)=A\otimes B_1+A\otimes B_2$;

3.$(\alpha A)\otimes(\beta B)=\alpha\beta(A\otimes B)$;

4.$(A\otimes B)\otimes C=A\otimes(B\otimes C)$;

5.$(A_1\otimes B_1)(A_2\otimes B_2)=(A_1A_2)\otimes(B_1B_2)$;

6.$(A\otimes B)^{-1}=A^{-1}\otimes B^{-1}$;

7.$(A\otimes B)^T=A^T\otimes B^T$;

8.两个上(下)三角阵的直积是上(下)三角阵;

9.两酉阵的直积是酉阵；

10.$det(A\otimes B)=(detA)^n\otimes(detB)^m\quad A\in\mathbf{C}^{mm}, B\in\mathbf{C}^{nn}$;

11.$tr(A\otimes B)=(trA)(trB)$;

12.$rank(A\otimes B)=rank(A)rank(B)$;

13.$A^2=A, B^2=B\Rightarrow(A\otimes B)^2=A\otimes B$.

下对性质 12 进行证明，其余留给读者练习。

证明对 A、B 进行奇异值分解，有

$$A=V_AS_AU_A, B=V_BS_BU_B$$

故，$A\otimes B=(V_A\otimes V_B)(S_A\otimes S_B)(U_A\otimes U_B)\equiv VSU$，且$rankS=(rankS_A)(rankS_B)$.

由于与可逆矩阵相乘不改变矩阵的秩，得

$$\begin{aligned}rank(A\otimes B)&=rankS\\&=(rankS_A)(rankS_B)\\&=(rankV_AS_AU_A)(rankV_BS_BU_B)\\&=(rankA)(rankB).\end{aligned}$$

1.1.2 矩阵的酉对角化

定义 1.1.2（酉变换）保持内积不变的变换，即

$$(Ux,Uy)=(x,y). \tag{1.1.6}$$

定义 1.1.3（酉矩阵）酉变换在标准正交基下的矩阵。

定理 1.1.3 矩阵 A 可以酉相似于对角矩阵的充分必要条件是$AA^{\dagger}=A^{\dagger}A$（即 A 是正规矩阵）。

证明（必要性）A 酉相似于对角阵→ $AA^{\dagger}=A^{\dagger}A$.

设 T 为酉矩阵，则$T^{-1}=T^{\dagger}$,

$$TAT^{-1}=\begin{bmatrix}\lambda_1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & \lambda_n\end{bmatrix},$$

则有

$$(T^{-1})^{\dagger}A^{\dagger}T^{\dagger}=TA^{\dagger}T^{-1}=\begin{bmatrix}\lambda_1^{*} & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & \lambda_n^{*}\end{bmatrix},$$

$$AA^{\dagger}=T^{-1}\begin{bmatrix}\lambda_1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & \lambda_n\end{bmatrix}TT^{-1}\begin{bmatrix}\lambda_1^{*} & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & \lambda_n^{*}\end{bmatrix}T$$

$$=T^{-1}\begin{bmatrix}\lambda_1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & \lambda_n\end{bmatrix}\begin{bmatrix}\lambda_1^{*} & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & \lambda_n^{*}\end{bmatrix}T=A^{\dagger}A.$$

（充分性）$AA^{\dagger}=A^{\dagger}A$ →A 酉相似于对角阵。（递归构造证明）

当$i=1$时，显然结论成立；

假设$i=n-1$时结论成立，当$i=n$时，取 A 的某一特征值λ_n和其对应的归一化特征向量X_n，有$AX_n=\lambda_n X_n$，$X_n^{\dagger}X_n$=1.

补充$X_1,X_2,\ldots,X_{n-1}$与X_n构成一组标准正交基，则存在酉矩阵 S 使得矩阵 A 在新基下为

$$A'=\begin{bmatrix}A_{n-1} & O\\ C & \lambda_n\end{bmatrix},$$

（使S^{-1}的第j列是第j个基矢量，即有$SAS^{-1}=A'$）。

由此得

$$AA^{\dagger}=S^{-1}\begin{bmatrix}A_{n-1}A_{n-1}^{\dagger} & A_{n-1}C^{\dagger}\\ CA_{n-1}^{\dagger} & CC^{\dagger}+\lambda_{\mathrm{n}}\lambda_n^{*}\end{bmatrix}S,$$

$$A^{\dagger}A=S^{-1}\begin{bmatrix}A_{n-1}^{\dagger}A_{n-1}+C^{\dagger}C & C^{\dagger}\lambda_n\\ \lambda_n^{*}C & \lambda_n^{*}\lambda_n\end{bmatrix}S,$$

由于$AA^{\dagger}=A^{\dagger}A$，可得$CC^{\dagger}+\lambda_{\mathrm{n}}\lambda_n^{*}=\lambda_n^{*}\lambda_n$，故$C=O,A_{n-1}A_{n-1}^{\dagger}=A_{n-1}^{\dagger}A_{n-1}$，即$A_{n-1}$是正规矩阵，因此知存在酉阵 P 使得

$$PA_{n-1}P^{-1}=\begin{bmatrix}\lambda_1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & \lambda_n\end{bmatrix}.$$

令$Q=\begin{bmatrix}P & 0\\ 0 & 1\end{bmatrix}$，于是

$$QSAS^{-1}Q^{-1}=\begin{bmatrix}P & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}A_{n-1} & 0\\ 0 & \lambda_n\end{bmatrix}\begin{bmatrix}P^{-1} & 0\\ 0 & 1\end{bmatrix}=\begin{bmatrix}PA_{n-1}P^{-1} & 0\\ 0 & \lambda_n\end{bmatrix}=\begin{bmatrix}\lambda_1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & \lambda_n\end{bmatrix},$$

由于 S、Q 为酉阵，因此$T=QS$也为酉阵，故存在酉阵$T=QS$使得

$$TAT^{-1}=\begin{bmatrix}\lambda_1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & \lambda_n\end{bmatrix},$$

结论得证。

设 A 是 Hilbert 空间 V 上的线性算子，则存在唯一的线性算子$A^\dagger$满足对任意的$|v\rangle, |w\rangle \in V$成立：

$$(|v\rangle, A|w\rangle)=(A^\dagger|v\rangle, |w\rangle), \tag{1.1.7}$$

这个算子称为A的伴随或Hermitian共轭。若$|v\rangle$是一个向量，定义$|v\rangle^\dagger \equiv \langle v|$，从而有$(A|v\rangle)^\dagger = \langle v|A^\dagger$。从矩阵表示的角度来说，一个算子取伴随，等价于它的矩阵表示取共轭转置，即$A^\dagger \equiv (A^*)^T$。如果一个算子的伴随等于自身，则称为厄米算子。

厄米算子的一个重要的例子是投影算子。假设W是一个d维向量空间V的k 维子空间，利用 Gram-Schmidt 正交化过程可以构造一组 V 标准正交基$|1\rangle, \cdots, |d\rangle$，使得$|1\rangle, \cdots, |k\rangle$恰为 W 的标准正交基。定义:

$$P \equiv \sum_{i=1}^{k} |i\rangle\langle i| \tag{1.1.8}$$

为到子空间 W 的投影算子，显然 P 是厄米的，$P^\dagger = P$。P 的正交补算子为$Q \equiv I - P$，Q 为到由$|k+1\rangle, \cdots, |d\rangle$张成的向量空间的投影算子。

一个算子 A 称为正规的，若$AA^\dagger = A^\dagger A$。显然厄米算子一定是正规的。关于正规算子有如下重要的定理:

定理 1.1.4（谱分解定理）向量空间 V 上的任意正规算子 M，在 V 的某个标准正交基下可对角化。反之，任意可对角化的算子都是正规的。

证明采用对空间 V 维数 d 的归纳法证明。d=1 的情况是平凡的。令λ是 M 的一个特征值，P 是到λ特征空间的投影，Q 是到正交补的投影，于是$M=(P+Q)M(P+Q)=PMP+PMQ+QMP+QMQ$。显然$MP=\lambda P$，故$QMP=0$。令$|v\rangle$为$\lambda$特征空间中的元素，则由 M 的正规性，$MM^\dagger|v\rangle = M^\dagger M|v\rangle = \lambda M^\dagger|v\rangle$，可得$QM^\dagger P=0$, 即$PMQ=0$，于是$M=PMP+QMQ$。由$QM=QM(P+Q)=QMQ$，$QM^\dagger = QM^\dagger(P+Q)=QM^\dagger Q$有：

$$\begin{aligned} QMQQM^{\dagger} &= QMOM^{\dagger}Q \\ &= QMM^{\dagger}Q \\ &= QM^{\dagger}MQ \\ &= QM^{\dagger}QMQ \\ &= QM^{\dagger}QQMQ, \end{aligned} \tag{1.1.9}$$

故 QMQ 是正规的。

由归纳假设，QMQ 对子空间 Q 的某个标准正交基是可对角化的，而 PM 已经是对 P 的标准正交基对角化的，可知$M = PMP + QMQ$相对全空间的某个标准正交基可对角化。

定理 1.4.5（同时酉对角化）两个可交换的正规矩阵可以同时酉对角化。

证明 (1)当$AB = BA$时，A,B 至少有一个共同的特征向量。设$AX = \lambda_1 X$，构造$[X, BX, B^2X, \cdots]$，为$\mathbf{C}_n$的子空间，B 为该子空间的线性变换，则存在X_1，使得$BX_1 = \mu_1 X_1$，同时有$AX_1 = \lambda_1 X_1$。

(2)类似地，补充向量$Y_2, \cdots, Y_n$，与X_1构成一组标准正交基。

$$SAS^{-1} = \begin{bmatrix} \lambda_1 & F \\ 0 & A_{n-1} \end{bmatrix}, \qquad SBS^{-1} = \begin{bmatrix} \mu_1 & G \\ 0 & B_{n-1} \end{bmatrix}$$

由$AA^{\dagger} = A^{\dagger}A$，$BB^{\dagger} = B^{\dagger}B$可推出 F,G=0，从而

$$SAS^{-1} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & A_{n-1} \end{bmatrix}, \qquad SBS^{-1} = \begin{bmatrix} \mu_1 & 0 \\ 0 & B_{n-1} \end{bmatrix}$$

且A_{n-1}，B_{n-1}为可交换的正规矩阵。

(3)由此可逐步得到标准正交基$\{X_1, \cdots, X_n\}$，在这组基下，A，B 可对角化为：

$$UAU^{-1} = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}, \qquad UBU^{-1} = \begin{bmatrix} \mu_1 & & \\ & \ddots & \\ & & \mu \end{bmatrix}.$$

定理 1.4.6 设 A 和 B 是厄米矩阵，当且仅当存在一组标准正交基，使 A 和 B 在这组基下同时对角的，有$[A, B] = 0$，即 A 和 B 可对易。

上述定理说明了两个厄米阵可对易的充分条件（关于矩阵对易的定义详见下节）。

1.1.3 Gram-Schmidt 正交化

内积$(\cdot,\cdot)$是向量空间上的函数，以向量空间中的两个向量作为输入并输出一个复数。例如$|v\rangle$与$|w\rangle$的内积为$(|v\rangle, |w\rangle)$。这不是标准的量子力学记号，标准的量子力学记号为$\langle v|w\rangle$，$\langle v|$表示向量$|v\rangle$的对偶向量。

定义 1.1.4（内积）一个函数从$V \times V$到$\mathbf{C}$的函数$(\cdot,\cdot)$称为内积或标量积，如果：

(1)$(\cdot,\cdot)$关于第二个输入线性：$(|v\rangle, \sum_i \lambda_i |w_i\rangle) = \sum_i \lambda_i (|v\rangle, |w_i\rangle)$;

(2)$(|v\rangle, |w\rangle) = (|w\rangle, |v\rangle)^*$;

(3)$(|v\rangle,|v\rangle)\geq 0$，等号成立当且仅当$|v\rangle=0$.

一个定义了内积的向量空间称为内积空间。

若向量$|v\rangle$和$|w\rangle$的内积等于零，则称它们是正交的。向量$|v\rangle$的范数定义为

$$\| v \| \equiv \sqrt{\langle v|v\rangle}. \tag{1.1.10}$$

若$\| v \|=1$，则称$|v\rangle$为单位向量，也称$|v\rangle$是归一化的。一个具有指标集 i 的向量集$|i\rangle$称为正交归一的，如果每个向量是归一化的，且不同的向量正交，即$\langle i|j\rangle=\delta_{ij}$.

假设$|w_1\rangle,|w_2\rangle,\cdots,|w_d\rangle$是内积空间 V 的一组基，可以利用 Gram-Schmidt 正交化方法将其逐渐生成一组标准正交基：取$|v_1\rangle\equiv\frac{|w_1\rangle}{\||w_1\rangle\|}$，对$1\leq k\leq d-1$，令

$$|v_{k+1}\rangle\equiv\frac{|w_{k+1}\rangle-\sum_{i=1}^{k}\langle v_i|w_{k+1}\rangle|v_i\rangle}{\||w_{k+1}\rangle-\sum_{i=1}^{k}\langle v_i|w_{k+1}\rangle|v_i\rangle\|}. \tag{1.1.11}$$

可以验证$|v_1\rangle,\cdots,|v_d\rangle$即为 V 的一组标准正交基。

向量空间中两个向量的内积也可采取矩阵表示。设向量$|w\rangle$和$|v\rangle$相对于标准正交基的表示分别为$|w\rangle=\sum_i w_i|i\rangle$及$|v\rangle=\sum_j v_j|j\rangle$.由于$\langle i|j\rangle=\delta_{ij}$，有

$$\begin{aligned}\langle v|w\rangle &= (\textstyle\sum_i v_i|i\rangle,\sum_j w_j|j\rangle)=\sum_{ij}v_i^*w_j\delta_{ij}=\sum_i v_i^*w_i\\ &= \begin{bmatrix}v_1^* & \cdots & v_n^*\end{bmatrix}\begin{bmatrix}w_1\\ \vdots\\ w_n\end{bmatrix}\end{aligned}\quad , \tag{1.1.12}$$

所以，两个向量的内积等于这两个向量在相同的标准正交基下的矩阵表示之间的内积。

线性算子除了有矩阵表示外，还有外积表示。

定义 1.1.5（外积）设$|v\rangle$和$|w\rangle$分别是内积空间 V 和 W 的向量，定义 V 到 W 的线性算子（外积）$|w\rangle\langle v|$如下：

$$(|w\rangle\langle v|)(|v'\rangle)\equiv|w\rangle\langle v|v'\rangle=\langle v|v'\rangle|w\rangle. \tag{1.1.13}$$

外积算子的线性组合可类似地定义为线性算子，如$\sum_i a_i|w_i\rangle\langle v_i|$作用在向量$|v'\rangle$后得到$\sum_i a_i|w_i\rangle\langle v_i|v'\rangle$.

外积的概念可用来推导一个重要的结果：正交向量的完备性关系。设$|i\rangle$是向量空间 V 的一组标准正交基，所以任意向量$|v\rangle$可写为$|v\rangle=\sum_i v_i|i\rangle$，注意到$\langle i|v\rangle=v_i$，从而

$$(\textstyle\sum_i|i\rangle\langle i|)|v\rangle=\sum_i|i\rangle\langle i|v\rangle=\sum_i v_i|i\rangle=|v\rangle, \tag{1.1.14}$$

由$|v\rangle$的任意性得：

$$\textstyle\sum_i|i\rangle\langle i|=I, \tag{1.1.15}$$

（1.1.15）被称为完备性关系，之后将反复用到这一公式。

前文已经描述矢量的外积$\sum_i a_i\,|w_i\rangle\langle v_i|$是一个线性算子。现在反过来，利用完备性关系导出任意算子的外积表示。设$A: V \to W$是线性算子，$|v_i\rangle$、$|w_j\rangle$分别是 V 和 W 的标准正交基，由完备性关系得：

$$\begin{aligned} A &= I_W A I_V \\ &= \sum_{ij} |w_j\rangle\langle w_j|A|v_i\rangle\langle v_i|, \\ &= \sum_{ij} \langle w_j|A|v_i\rangle |w_j\rangle\langle v_i| \end{aligned} \tag{1.1.16}$$

上式即为 A 的外积表示。I_W、I_V分别为 W 和 V 上的单位算子，$\langle w_j|A|v_i\rangle$为复数。

利用完备性关系还可以证明 Cauchy-Schwarz 不等式：Hilbert 空间中任意两个向量$|v\rangle$和$|w\rangle$满足：

$$|\langle v|w\rangle|^2 \le \langle v|v\rangle\langle w|w\rangle. \tag{1.1.17}$$

证明基于 Gram-Schmidt 方法构造向量空间的一组标准正交基$\{|i\rangle\}$时，取这组基的第一个成员为$|w\rangle/\sqrt{\langle w|w\rangle}$，利用完备条件$\sum_i |i\rangle\langle i| = I$，只保留第一项，可得

$$\begin{aligned} \langle v|v\rangle\langle w|w\rangle &= \sum_i \langle v|i\rangle\langle i|v\rangle\langle w|w\rangle \\ &\ge \frac{\langle v|w\rangle\langle w|v\rangle}{\langle w|w\rangle}\langle w|w\rangle \\ &= \langle v|w\rangle\langle w|v\rangle \\ &= |\langle v|w\rangle|^2, \end{aligned} \tag{1.1.18}$$

可以看出，当且仅当$|v\rangle$和$|w\rangle$线性相关时，上式取等号。

另一种证明方法：对于任意复数λ，显然有

$$(\langle\psi| - \lambda^*\langle\varphi|)(|\psi\rangle - \lambda|\varphi\rangle) \ge 0,$$

即，$\langle\psi|\psi\rangle + \lambda^*\lambda\langle\varphi|\varphi\rangle - \lambda\langle\psi|\varphi\rangle - \lambda^*\langle\varphi|\psi\rangle \ge 0$.取$\lambda = \langle\varphi|\psi\rangle/\langle\varphi|\varphi\rangle$，即得

$$\langle\psi|\psi\rangle\langle\varphi|\varphi\rangle - \langle\psi|\varphi\rangle\langle\varphi|\psi\rangle > 0.$$

1.1.4 算子函数

定义 1.1.6（算子函数）设$A = \sum_a a\,|a\rangle\langle a|$是正规算子 A 的一个谱分解，定义算子函数:

$$f(A) = \sum_a f(a)|a\rangle\langle a|. \tag{1.1.19}$$

一组非零向量$|v_1\rangle, |v_2\rangle, \cdots, |v_n\rangle$称为线性相关的，如果存在不全为零的复数$a_1, \cdots, a_n$，使得

$$a_1|v_1\rangle + a_2|v_2\rangle + \cdots + a_n|v_n\rangle = 0. \tag{1.1.20}$$

否则称为线性无关。

向量空间 V 到向量空间 W 的一个线性算子 A 为向量空间 V 到 W 的映射，且满足线性，即：

$$A(\sum_i a_i\,|v_i\rangle) = \sum_i a_i\,A(|v_i\rangle). \tag{1.1.21}$$

线性算子具有矩阵表示。确定了 n 维线性空间的一组基后，空间中的任一向量可由这组基线性表达，表达的系数即对应 n 维复向量空间$\mathbb{C}^n$中的一个向量。所以任意 n 维复线性空间中的向量与$\mathbb{C}^n$中的向量一一对应。而一个$m \times n$维的复数域上矩阵 A，通过矩阵乘法可以将$\mathbb{C}^n$中的向量映射为$\mathbb{C}^m$中的向量。所以给定一个$m \times n$维的复矩阵，自然对应一个从 n 维线性空间到 m 维线性空间的线性算子。另一方面，对于一个线性算子，也可以对应一个矩阵：设$A: V \to W$是向量空间 V 到 W 的线性算子。$|v_1\rangle, |v_2\rangle, \cdots, |v_m\rangle$是 V 的一组基，$|w_1\rangle, |w_2\rangle, \cdots, |w_n\rangle$是 W 的一组基，则对任意的 j,$1 \le j \le m$，存在复数$A_{1j}, \cdots, A_{nj}$使得：

$$A\big|v_j\big\rangle = \sum_i A_{ij}\,|w_i\rangle. \tag{1.1.22}$$

由A_{ij}作为矩阵元构成的矩阵称为算子 A 的矩阵表示。一个算子与它的矩阵表示是完全等价的，我们之后不作特别区分。

一个重要的矩阵函数是矩阵的迹：

$$tr(A) \equiv \sum_i A_{ii}. \tag{1.1.23}$$

矩阵的迹具有如下性质：

$$tr(AB) = tr(BA); \tag{1.1.24a}$$

$$tr(A+B) = tr(A) + tr(B); \tag{1.1.24b}$$

$$tr(\lambda A) = \lambda tr(A). \tag{1.1.24c}$$

矩阵的迹在酉相似变换$A \to UAU^\dagger$下不变:

$$tr(UAU^\dagger) = tr(U^\dagger UA) = tr(A). \tag{1.1.25}$$

迹在酉相似变换下的不变性保证算子的迹是与基的选取无关的。

下面的等式是一个常用的结果：

$$tr(A|\psi\rangle\langle\psi|) = \sum_i \langle i|A|\psi\rangle\langle\psi|i\rangle. \tag{1.1.26}$$

§1.2 量子力学基础

1.2.1 量子力学基本假设

量子力学的第一个假设为波函数假设，即系统状态为$|\psi\rangle$，坐标表象$\psi(r,t)$，对于孤立系统，波函数为完全描述，并有几率波解释。

波函数的引入必然导致态叠加原理和纠缠态问题，而这正是量子物理全部神秘和神奇之源。量子信息理论主要涉及由有限维复向量空间上的线性变换所描述的“简易量子力学”，态叠加原理和纠缠态问题却更加凸现出来，量子力学的神秘和神奇丝毫不减。

量子力学的第二个假设为算符假设，即力学量可用线性厄密算符表示。一对共轭力学量算符的不可对易性是量子力学的基本特征。

基本算符：$r, p \equiv -i\hbar\nabla$，由此可构造：

$$\hat{T} = \frac{\hat{p}^2}{2m} = -\frac{\hbar^2}{2m}\Delta, \hat{V} = V(r),$$

$$\hat{L} = r \times \hat{p} = -i\hbar \mathrm{r} \times \nabla, \hat{E} = i\hbar\frac{\partial}{\partial t},$$

……

量子力学的第三个假设为测量假设，即对力学可观测量的测量使系统随机落入该力学量的一个本征态$|\varphi_m\rangle$，概率为$|\langle\varphi_m|\psi\rangle|^2$，平均值为$\overline{\Omega}_\psi = \int \psi^*(r)\Omega\psi(\mathrm{r})\mathrm{dr}$，用 Dirac 符号写为$\overline{\Omega} = \langle\Omega\rangle_\psi = \langle\psi|\Omega|\psi\rangle$，不需要指出具体在哪个基上展开。

大量处于相同的量子态的系统构成量子系综，而量子态上的平均值是在量子系综上的平均值。两个力学量可同时观测的充分必要条件是两力学量算符可对易，即$\left[\hat{A}, \hat{B}\right] = 0$，这种情况下两算符有共同本征函数系因此可以进行同时测量，测量后系统进入两力学量的一个共同本征态。

量子力学的第四个假设为态演化假设，即薛定谔绘景下量子态演化所遵循的方程是薛定谔方程：$i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = \hat{H}(p, q, t)|\psi(t)\rangle$. 其中$\hat{H}(p, q, t)$为系统的哈密顿算符。

量子力学的第五个假设为全同性假设，即全同粒子体系的波函数对于任意两粒子的交换是对称的（玻色子情形）或是反对称的（费米子情形），即自然界存在的态$|\psi\rangle$必须是所有交换算符的本征态：$\left|P_{ij}\right|\psi\rangle = \pm|\psi\rangle, (i, j = 1,2, \ldots, N)$.

1.2.2 狄拉克（Dirac）符号

线性空间是线性代数的基本概念。在量子力学中，向量空间中的一个向量采用标准符号：$|\psi\rangle$，有时也被叫做右矢，它的对偶向量则称为左矢：$\langle\psi|$，两个向量$|\psi\rangle$与$|\varphi\rangle$之间的内积记为$\langle\psi|\varphi\rangle$，这种记法被称为狄拉克符号。

狄拉克采用抽象的态矢量符号，以普遍的、与基的选取无关的方式表达量子体系的状态在态空间中的演化，更凸显了物理本质。狄拉克给出了量子力学的第三种表述形式（第四种表述：费曼的量子最小作用量原理），统一了波动力学和矩阵力学，在考虑连续谱时，物理的态空间已经超出了数学上的希尔伯特空间。

定义 1.2.1（右矢、左矢、标量积）

右矢：$|A\rangle$，如$|r\rangle, |p\rangle, |\psi(t)\rangle, \ldots$

左矢：$\langle A| = (|A\rangle)^\dagger \Longrightarrow (\langle A|)^\dagger = |A\rangle$.

标量积：$\langle B|A\rangle$，即对由态矢$|A\rangle$描述的物理系统测量，发现该系统处于状态$|B\rangle$的几率幅，且有$\langle B|A\rangle = \langle A|B\rangle^*$.

为了能在态矢空间进行定量计算，需要选取一组特定的态矢作为基矢，以展开任意态矢。

定义 1.2.2（对易式、反对易式）A、B 为厄密算符，则有

对易式：

$$[\mathrm{A},\mathrm{B}]=\mathrm{AB}-\mathrm{BA} \tag{1.2.1}$$

反对易式：

$$\{\mathrm{A},\mathrm{B}\}=\mathrm{AB}+\mathrm{BA} \tag{1.2.2}$$

设 A、B 为厄密算符，且$\langle\psi|AB|\psi\rangle=x+iy$，有$\langle\psi|[AB]|\psi\rangle=2iy,\langle\psi|\{AB\}|\psi\rangle=2x$.于是有$|\langle\psi|[AB]|\psi\rangle|^2+|\langle\psi|\{AB\}|\psi\rangle|^2=4|\langle\psi|AB|\psi\rangle|^2$.根据 Cauchy-Schwarz 不等式

$$|\langle\psi|AB|\psi\rangle|^2\leq\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle$$

可得$|\langle\psi|[AB]|\psi\rangle|^2\leq 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle$.

1.2.3 量子测量

量子测量是由测量算子集合$\{M_m\}$描述。这些算子是作用在被测量的态空间上，指标 m 对应可能的测量输出结果。若量子体系在测量前一刻的态是$|\psi\rangle$，那么输出 m 的几率为：

$$p(m)=\langle\psi|M_m^\dagger M_m|\psi\rangle. \tag{1.2.3}$$

系统测后态为：

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}. \tag{1.2.4}$$

由于各可能输出的几率和必须为 1，得完备性方程：

$$\sum_m M_m^\dagger M_m=I. \tag{1.2.5}$$

上述是对最一般的测量进行描述，有一类特殊的测量称为投影测量，投影测量由一个可观测量 M，即作用在被观测体系的态空间上的厄密算子描述。观测量 M 为厄密算子，所以可谱分解：

$$M=\sum_m m\,P_m, \tag{1.2.6}$$

其中$P_m=|m\rangle\langle m|$是 M 对于本征值 m 的特征子空间的投影算子。测量可能的输出对应本征值 m.若测量态为$|\psi\rangle$，则得到结果 m 的几率为：

$$p(m)=\langle\psi|P_m|\psi\rangle. \tag{1.2.7}$$

测后态则为：

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}}. \tag{1.2.8}$$

在量子力学中，可观测量对应一个物理量。当对可观测量 M 进行测量时，M 的本征值即对应可能得到的结果，并且态矢在测量后发生坍缩，投影到了相应的特征空间中。当计算测量可观测量 M 时，得到的测量结果的平均值：

$$\begin{aligned} E(M) &= \sum_m m\, p(m) \\ &= \sum_m m\, \langle\psi|P_m|\psi\rangle \\ &= \langle\psi|(\sum_m mP_m)|\psi\rangle \\ &= \langle\psi|M|\psi\rangle \end{aligned} \tag{1.2.9}$$

由此可知对态矢$|\psi\rangle$测量可观测量 M（或者说测量相应的力学量 M）时得到的均值为$\langle\psi|M|\psi\rangle$.

除此之外还有广义测量和 POVM 测量。广义测量是指在大系统上进行正交投影测量时，在子系统上所观察到的测量，是前面给出的测量形式理论的具体实现，POVM 测量是指一组能对单位算符做分解的非负的厄米算符。

一般的量子测量不仅描述测量结果的概率分布，还对测量之后的态进行刻画，但有时并不关心测后的态而只在意测量结果的分布，对于这类情况用 POVM 测量作为工具进行分析将更加方便。假设作用在态$|\psi\rangle$上的测量由测量算子$\{M_m\}$描述。则测量结果为 m 的几率为(1.2.3)。定义：

$$E_m \equiv M_m^\dagger M_m, \tag{1.2.10}$$

则E_m为半正定算子且$\sum_m E_m = I$。态矢$|\psi\rangle$测量输出 m 的几率$p(m) = \langle\psi|E_m|\psi\rangle$。所以$E_m$即完全确定了测量输出的几率分布。算子$E_m$称为 POVM 元。算子集合$\{E_m\}$称为 POVM。事实上，任何一组对单位算子做分解的半正定算子对应于一个 POVM 测量。

下面定理描述了 POVM 测量与投影测量的关系：

定理 1.2.1（Neumark 定理）任何给定的 POVM 都可以通过将态空间扩展到某一更大的态空间，并在其上实行正交投影的方法实现。

Neumark 定表明，在大系统上作正交投影测量，从子系统上来看即为 POVM 测量。反之，子空间上的任意 POVM 测量（对应算子 I 的任意半正定分解）也可通过在某一大空间作正交投影测量实现。

1.2.4 密度算符

到目前所提到的形如$|\psi\rangle$的态矢，是 Hilbert 空间中的向量，它完全刻画了系统。这样的态称为纯态。但有时，量子系统所处的状态可能不完全已知。更准确地说，量子系统可能处于状态集$\{|\psi_i\rangle\}$中的一个，其中处于状态$|\psi_i\rangle$的几率为p_i。这时称系统所处的状态为纯态系综$\{p_i, |\psi_i\rangle\}$。密度算子是描述这样不完全已知的态的有力工具。对于纯态系综$\{p_i, |\psi_i\rangle\}$，定义相应的密度算子为:

$$\rho \equiv \sum p_i |\psi_i\rangle\langle\psi_i|. \tag{1.2.11}$$

从定义可以看出它为态空间上的半正定算子。密度算子有时也称为密度矩阵。在前一节中介绍的几个量子力学基本假设，都可以用密度算子的语言重新描述，且这种描述与用态矢的语言描述是等价的。首先，对于假设一，有相应的如下假设：任意一个孤立的量子系统是一个有着内积的复向量空间，系统完全由密度算子描述。密度算子为作用在态空间上的半正定算子。如果量子系统以几率p_i处于状态ρ_i，则系统的密度算子为$\sum_i p_i\, \rho_i$。而量子力学的第二个基本假设表明一个闭的量子系统的演化是由一个酉算子 U 来刻画。若系统最初以几率p_i

处于状态$|\psi_i\rangle$，则演化后的系统将以几率p_i处于状态$U|\psi_i\rangle$。因此，密度算子的演化按照如下方程：

$$\rho = \sum_i p_i\,|\psi_i\rangle\langle\psi_i|$$

$$\xrightarrow{U} \sum_i p_i\,U|\psi_i\rangle\langle\psi_i|U^\dagger$$

$$= U\rho U^\dagger. \tag{1.2.12}$$

量子力学关于测量的基本假设同样可以用密度算子的语言来描述。假设测量算子为$\{M_m\}$，若初态为$|\psi_i\rangle$，则测量输出为 m 的几率是

$$p(m|i) = \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = tr(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|). \tag{1.2.13}$$

由全概率公式，测量输出为 m 的几率为

$$\begin{aligned} p(m) &= \textstyle\sum_i p\,(m|i)p_i \\ &= \textstyle\sum_i p_i\,tr(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|) \\ &= tr(M_m^\dagger M_m\rho). \end{aligned} \tag{1.2.14}$$

现在计算测量输出为 m 时系统在测量之后的密度算子。若初态为$|\psi_i\rangle$，则得到 m 结果的测量后的状态为

$$|\psi_i^m\rangle = \frac{M_m|\psi_i\rangle}{\sqrt{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle}}, \tag{1.2.15}$$

所以测量输出 m 之后的系综由态矢$|\psi_i^m\rangle$构成，相应的几率为$p(i|m)$。写成密度算子为：

$$\rho_m = \textstyle\sum_i p\,(i|m)|\psi_i^m\rangle\langle\psi_i^m| = \sum_i p\,(i|m)\frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle}. \tag{1.2.16}$$

由概率论的知识$p(i|m) = p(m,i)/p(m) = p(m|i)p_i/p(m)$，从而：

$$\begin{aligned} \rho_m &= \textstyle\sum_i p_i\frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{tr(M_m^\dagger M_m\rho)} \\ &= \frac{M_m\rho M_m^\dagger}{tr(M_m^\dagger M_m\rho)}. \end{aligned} \tag{1.2.17}$$

所以用密度算子的语言来描述测量如下：量子测量由算子集合$\{M_m\}$刻画，这些算子是作用在被测量的态空间上的，指标 m 对应于可能的测量输出。若测量前的状态为ρ，则测量结果为 m 的几率是：

$$p(m) = tr(M_m^\dagger M_m\rho), \tag{1.2.18}$$

且测量后的系统状态为:

$$\frac{M_m\rho M_m^\dagger}{tr(M_m^\dagger M_m\rho)}, \tag{1.2.19}$$

其中测量算子满足完备性条件：

$$\sum_m M_m^\dagger M_m = I. \tag{1.2.20}$$

量子力学关于复合系统的基本假设同样可以由密度算子的语言来描述：复合物理体系的态空间是子系统态空间的张量积。用$1,\cdots,n$标记子系统，若系统 i 处于态ρ_i，则整个系统的联合态为$\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$。

这一小节的开头提到，一个系统的状态若是 Hilbert 空间的某个态矢$|\psi\rangle$，则被称为纯态。此时的密度算子为$\rho = |\psi\rangle\langle\psi|$。否则$\rho$则称为混合态，它可以理解为对$\rho$对应系综中各纯态的混合。因为密度算子为半正定算子，所以可对它进行谱分解$\rho = \sum_i \lambda_i |i\rangle\langle i|$，简单计算得$\rho^2 = \sum_i \lambda_i^2 |i\rangle\langle i|$，所以$tr(\rho) = \sum_i \lambda_i$，$tr(\rho^2) = \sum_i \lambda_i^2$.

若ρ为纯态，则其中一个λ_i为 1，其他为零。因而$tr(\rho) = tr(\rho^2) = 1$；若为混合态，则$\lambda_i$至少有两个非零，所以$tr(\rho^2) < 1$.因此可以根据$tr(\rho^2)$是否等于 1 来判断系统是处于纯态还是混合态。

当看到给定一个纯态系综，便可以得到它的密度算子。那么一个一般的线性算子，在满足什么条件时存在系综以它为密度矩阵呢？有下面定理：

定理 1.2.2（密度算子）一个算子ρ是描述某个系综$\{p_i, |\psi_i\rangle\}$的密度算子当且仅当它满足以下条件：

(1)（迹条件）ρ的迹为 1；

(2)（正定性条件）ρ是半正定算子。

证明设$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$是密度算子，则

$$tr(\rho) = \sum_i p_i \, tr(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i = 1, \tag{1.2.21}$$

所以$tr(\rho) = 1$.

假设$|\varphi\rangle$是态空间的任意态矢，则

$$\begin{aligned} \langle\varphi|\rho|\varphi\rangle &= \sum_i p_i \langle\varphi|\psi_i\rangle\langle\psi_i|\varphi\rangle \\ &= \sum_i p_i |\langle\varphi|\psi_i\rangle|^2 \\ &\geq 0 \end{aligned}, \tag{1.2.22}$$

所以密度算子是半正定的。

反之，假设ρ是迹为 1 的半正定算子，则它有谱分解：

$$\rho = \sum_j \lambda_j |j\rangle\langle j|, \tag{1.2.23}$$

其中$|j\rangle$是互相正交，λ_j是ρ的非负实本征值。由于ρ的迹为 1，所以$\sum_j \lambda_j = 1$。所以系综$\{\lambda_j, |j\rangle\}$对于的密度算子即为ρ.

事实上，一个密度算子可以对应不同的系综。如考虑密度算子:

$$\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|. \tag{1.2.24}$$

令：

$$|a\rangle \equiv \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle; \tag{1.2.25a}$$

$$|b\rangle \equiv \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle. \tag{1.2.25b}$$

简单计算即可发现

$$\rho = \frac{1}{2}|a\rangle\langle a| + \frac{1}{2}|b\rangle\langle b| = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|. \tag{1.2.26}$$

一个自然的问题是哪些系综可以对应同一个密度算子。为了方便，采用记号$|\widetilde{\psi}_i\rangle$表示非归一化的向量。若密度算子为$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$，令$|\widetilde{\psi}_i\rangle = \sqrt{p_i}|\psi_i\rangle$，则称向量$|\widetilde{\psi}_i\rangle$生成密度算子$\rho \equiv \sum_i |\widetilde{\psi}_i\rangle\langle\widetilde{\psi}_i|$.

下面定理说明什么情况下向量集合$|\widetilde{\psi}_i\rangle$和$|\widetilde{\varphi}_j\rangle$生成相同的密度算子。

定理 1.2.3（密度算子的系综的酉自由度）向量集合$|\widetilde{\psi}_i\rangle$和$|\widetilde{\varphi}_j\rangle$生成相同的密度算子当且仅当

$$|\widetilde{\psi}_i\rangle = \sum_j u_{ij} |\widetilde{\varphi}_j\rangle, \tag{1.2.27}$$

其中u_{ij}是酉矩阵的矩阵元，对于指标 i 和 j（通过适当填充零向量使得两个向量集有相同的大小）。

证明若存在酉阵 u 使得$|\widetilde{\psi}_i\rangle = \sum_j u_{ij} |\widetilde{\varphi}_j\rangle$，则

$$\begin{aligned} \sum_i |\widetilde{\psi}_i\rangle\langle\widetilde{\psi}_i| &= \sum_{ijk} u_{ij} u^*_{ik} |\widetilde{\varphi}_j\rangle\langle\widetilde{\varphi}_k| \\ &= \sum_{jk} (\sum_i u^\dagger_{ki} u_{ij}) |\widetilde{\varphi}_j\rangle\langle\widetilde{\varphi}_k| \\ &= \sum_{jk} \delta_{kj} |\widetilde{\varphi}_j\rangle\langle\widetilde{\varphi}_k| \\ &= \sum_j |\widetilde{\varphi}_j\rangle\langle\widetilde{\varphi}_j|, \end{aligned} \tag{1.2.28}$$

所以$|\widetilde{\psi}_i\rangle$和$|\widetilde{\varphi}_j\rangle$生成相同的算子。

反之，若

$$A = \sum_i |\widetilde{\psi}_i\rangle\langle\widetilde{\psi}_i| = \sum_j |\widetilde{\varphi}_j\rangle\langle\widetilde{\varphi}_j|. \tag{1.2.29}$$

设$A = \sum_k \lambda_k |k\rangle\langle k|$为 A 的谱分解，满足$\lambda_k$全为正数。令$|\widetilde{k}\rangle \equiv \sqrt{\lambda_k}|k\rangle$.

先证$|\widetilde{k}\rangle$与$|\widetilde{\psi}_i\rangle$相差一个酉阵。

设$|\psi\rangle$是任意与$|\widetilde{k}\rangle$张成的空间正交的向量，则对任意 k 有$\langle\psi|\widetilde{k}\rangle\langle\widetilde{k}|\psi\rangle = 0$，因此

$$0 = \langle\psi|A|\psi\rangle = \sum_i \langle\psi|\widetilde{\psi}_i\rangle\langle\widetilde{\psi}_i|\psi\rangle = \sum_i |\langle\psi|\widetilde{\psi}_i\rangle|^2, \tag{1.2.30}$$

所以对所有的 i 及所有与$|\widetilde{k}\rangle$张成的空间正交的向量$|\psi\rangle$有$\langle\psi|\widetilde{\psi}_i\rangle = 0$.因此$|\widetilde{\psi}_i\rangle$可以表示为$|\widetilde{k}\rangle$的线性组合，设$|\widetilde{\psi}_i\rangle = \sum_k c_{ik} |\widetilde{k}\rangle$.

由于$A=\sum_k|\widetilde{k}\rangle\langle\widetilde{k}|=\sum_i|\widetilde{\psi}_i\rangle\langle\widetilde{\psi}_i|$，所以

$$\sum_k|\widetilde{k}\rangle\langle\widetilde{k}|=\sum_{kl}(\sum_i c_{ik}\,c*_{il})|\widetilde{k}\rangle\langle\widetilde{l}|. \tag{1.2.31}$$

根据算子$|\widetilde{k}\rangle\langle\widetilde{l}|$的线性无关性，可以得到$\sum_i c_{ik}\,c*_{il}=\delta_{kl}$.所以对矩阵 c 加入额外的列可得到酉阵 v 满足$|\widetilde{\psi}_i\rangle=\sum_k v_{ik}|\widetilde{k}\rangle$（其中在集合$|\widetilde{k}\rangle$中补充若干个零向量）。同理，可以找到酉阵 w 使得$|\widetilde{\varphi}_j\rangle=\sum_k w_{jk}|\widetilde{k}\rangle$。因此，$|\widetilde{\psi}_i\rangle=\sum_j u_{ij}|\widetilde{\varphi}_j\rangle$，其中$u=vw^{\dagger}$是酉阵。

由此定理可以看出对于归一化的态矢$|\psi_i\rangle$，$|\varphi_j\rangle$和概率分布p_i，q_j，$\rho=\sum_i p_i|\psi_i\rangle\langle\psi_i|=\sum_j q_j|\varphi\rangle\langle\varphi|$当且仅当存在酉阵 u 使得：

$$\sqrt{p_i}|\psi_i\rangle=\sum_j u_{ij}\sqrt{q_j}|\varphi_j\rangle, \tag{1.2.32}$$

所以定理 1.2.3 刻画了能够生成给定密度算子的系综的自由度。

1.2.5 复合体系

以两个系统构成的复合系统为例，若子系统A,B的基矢分别为$\{|i\rangle_A\}$和$\{|\mu\rangle_B\}$，则$\{|i\rangle_A\otimes|\mu\rangle_B\}$为复合系统 A+B 的一组完备基。A+B 中的任意量子态可表为;

$$|\psi\rangle_{AB}=\sum_{i\mu}a_{i\mu}|i\rangle_A|\mu\rangle_B,\quad \sum_{iv}|a_{i\mu}|^2=1. \tag{1.2.33}$$

相应的，有$\rho_{AB}=|\psi\rangle_{AB}\langle\psi|=\sum_{i\mu jv}a^*_{jv}a_{i\mu}|i\rangle_A|\mu\rangle_{BA}\langle j|_B\langle v|$，这里$|\psi\rangle_{AB}$是纯态，因而$\rho_{AB}$是一个纯态的密度算子。

约化密度算子是用来刻画复合系统的子系统的概念。假设有物理系统 A 和 B，系统处在状态ρ^{AB}.系统 A 的约化密度算子定义为：

$$\rho^A\equiv tr_B(\rho^{AB}), \tag{1.2.34}$$

其中tr_B是算子映射，称为 B 系统上的偏迹。偏迹的定义为：

$$tr_B(|a_1\rangle\langle a_2|\otimes|b_1\rangle\langle b_2|)\equiv|a_1\rangle\langle a_2|tr(|b_1\rangle\langle b_2|), \tag{1.2.35}$$

其中$|a_1\rangle$和$|a_2\rangle$是 A 系统态空间的向量，$|b_1\rangle$和$|b_2\rangle$是 B 系统态空间中的向量。等式右边的迹运算则是通常的定义在系统 B 上的迹运算，所以$tr(|b_1\rangle\langle b_2|)=\langle b_2|b_1\rangle$.对于 AB 上的任意一个一般的算子，利用偏迹的线性即可按照(1.3.24)式求解。

例如 Bell 态$(|00\rangle+|11\rangle)/\sqrt{2}$，它的密度算子为：

$$\begin{aligned}\rho &=\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00|+\langle 11|}{\sqrt{2}}\right)\\ &=\frac{|00\rangle\langle 00|+|11\rangle\langle 00|+|00\rangle\langle 11|+|11\rangle\langle 11|}{2},\end{aligned} \tag{1.2.36}$$

将第二个量子比特取偏迹得到第一个量子比特的约化密度算子：

$$\begin{aligned}\rho^1 &= tr_2(\rho)\\ &= \frac{tr_2(|00\rangle\langle 00|)+tr_2(|11\rangle\langle 00|)+tr_2(|00\rangle\langle 11|)+tr_2(|11\rangle\langle 11|)}{2}\\ &= \frac{|0\rangle\langle 0|\langle 0|0\rangle+|1\rangle\langle 0|\langle 0|1\rangle+|0\rangle\langle 1|\langle 1|0\rangle+|1\rangle\langle 1|\langle 1|1\rangle}{2}\\ &= \frac{|0\rangle\langle 0|+|1\rangle\langle 1|}{2}\\ &= \frac{I}{2}\end{aligned}. \tag{1.2.37}$$

由于$tr((I/2)^2) = 1/2 < 1$，ρ^1是混合态。在这个例子中，两个量子比特的联合系统处于纯态，也就是被完全了解。而第一个量子比特却处于混合态，对这个状态没有完全的了解。这种联合态完全已知，子系统却处于混合态的现象是纠缠现象的另一个特点。

Schmidt 分解和纯化是也研究复合系统的有力工具。

定理 1.2.4（Schmidt 分解）假设$|\psi\rangle$是复合系统 AB 的一个纯态，则存在 A 系统的正交归一的态矢$|i_A\rangle$和 B 系统的正交归一的态矢$|i_B\rangle$使得：

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle, \tag{1.2.38}$$

其中λ_i是非负实数并满足$\sum_i \lambda_i^2 = 1$，称为 Schmidt 系数。

这是一个十分有用的结果。设$|\psi\rangle$是复合系统 AB 的纯态，则由 Schmidt 分解$\rho^A = tr_B(|\psi\rangle\langle\psi|) = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|$, $\rho^B = tr_A(|\psi\rangle\langle\psi|) = \sum_i \lambda_i^2 |i_B\rangle\langle i_B|$.所以$\rho^A$的本征值和$\rho^B$的本征值是完全一样的，都为$\lambda_i^2$.量子系统的许多性质是由约化密度算子的本征值决定的。对于处于纯态的复合系统，两个子系统的这类性质是一样的。例如两个量子比特的纯态$(|00\rangle + |01\rangle + |11\rangle)/\sqrt{3}$，看起来没有明显的对称性，但计算$tr((\rho^A)^2)$和$tr((\rho^B)^2)$都等于$\frac{7}{9}$。下面来具体证明定理。

证明假设系统 A 和 B 有相同的维数，$|j\rangle$和$|k\rangle$分别是系统 A 和 B 的固定的标准正交基。对 A 和 B 维数不同的情景（如 A 的维数比 B 小），只需取 A 的一组标准正交基再补充若干个零向量仍记为$|j\rangle$，证明类似。$|\psi\rangle$可以写为：

$$|\psi\rangle = \sum_{jk} a_{jk} |j\rangle|k\rangle, \tag{1.2.39}$$

其中a_{jk}为某些复数，设a_{jk}作为矩阵元构成矩阵a，由奇异值分解有$a = udv$，其中 d 是有非负实对角元的对角阵，u 和 v 是酉阵。因此：

$$|\psi\rangle = \sum_{ijk} u_{ji}\, d_{ii} v_{ik} |j\rangle|k\rangle. \tag{1.2.40}$$

定义$|i_A\rangle \equiv \sum_j u_{ji} |j\rangle$，$|i_B\rangle \equiv \sum_k v_{ik} |k\rangle$，$\lambda_i \equiv d_{ii}$则

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle. \tag{1.2.41}$$

因为 u 和 v 的酉性，$|i_A\rangle$和$|i_B\rangle$分别构成标准正交基。

基矢$|i_A\rangle$和$|i_B\rangle$分别称为 A 和 B 的 Schmidt 基。非零λ_i的个数称为态矢$|\psi\rangle$的 Schmidt 数。关于 Schmidt 数有一个重要的结论：复合系统 AB 的态矢$|\psi\rangle$是直积态当且仅当它的 Schmidt 数为 1，也即当且仅当ρ^A(因而ρ^B) 是纯态。这将作为习题留给读者证明。

学习量子计算与量子信息的另一个有力工具为纯化。假设ρ^A是量子系统 A 的一个状态，可引入另一个系统 R，并且定义联合系统 AR 的纯态$|AR\rangle$使得$\rho^A = tr_R(|AR\rangle\langle AR|)$。即当只看系统 A 时纯态$|AR\rangle$约化为$\rho^A$。这个过程称为纯化，这仅仅是一个数学上的过程，以便联系纯态和混合态。称系统 R 为参考系统，它是一个虚构的系统，没有直接的物理意义。

为了证明任意态都可以纯化，直接解释如何构造系统 R 和纯态$|AR\rangle$。假设ρ^A的谱分解为$\rho^A = \sum_i p_i |i^A\rangle\langle i^A|$，引进系统 R，R 和 A 有相同的态空间，有一组正交基$|i^R\rangle$。并定义复合系统上的纯态:

$$|AR\rangle \equiv \sum_i \sqrt{p_i}\,|i^A\rangle|i^R\rangle, \tag{1.2.42}$$

则对应系统 A 的约化密度矩阵为：

$$\begin{aligned} tr_R(|AR\rangle\langle AR|) &= \sum_{ij} \sqrt{p_i p_j}\,|i^A\rangle\langle j^A| tr(|i^R\rangle\langle j^R|) \\ &= \sum_{ij} \sqrt{p_i p_j}\,|i^A\rangle\langle j^A|\delta_{ij} \\ &= \sum_i p_i\,|i^A\rangle\langle i^A| \\ &= \rho^A \end{aligned}, \tag{1.2.43}$$

因此$|AR\rangle$是ρ^A的纯化。

注意 Schmidt 分解与纯化之间的关系：纯化过程中定义的纯态$|AR\rangle$对应系统 A 的 Schmidt 基正是混合态ρ^A对角化时的基矢。Schmidt 系数则是ρ^A对角化时相应本征值的平方根。

1.2.6 Bell 不等式

在学习量子计算和量子信息的过程中，理解量子力学非同寻常的非经典的性质是至关重要的。量子力学与经典世界之间的差别究竟在哪里？本节讨论的 Bell 不等式是反映量子与经典物理本质差别的一个重要例子。

在生活中，当谈及某一对象，总认为这个对象的物理性质的存在性是独立于观察者的，即测量仅仅是揭示这些物理性质。例如，一个足球的位置是它具有的一个性质。但随着量子力学的发展，出现了与经典观点非常不同的观点。该观点认为，还未被观察的粒子不具有独立于测量的物理性质。相反，物理性质是在系统上进行观察所造成的结果。例如，一个量子比特在被观测前不具有“在 z 方向自旋σ_z” 或“在 x 方向自旋σ_x”这样的确定性质。这两个性质是在进行了适当的测量后才可以给出。量子力学给出一套规则，给定态矢空间，能够确定的只是测量σ_x或σ_z时可能的测量结果及几率。

许多物理学家拒绝这种观点，最著名的反对者是 Einstein。他在与 Boris Podolsky 和 Nathen Rosen 合著的著名的 EPR 论文中提出了一个思想实验，爱因斯坦相信这个实验说明了量子力学并非完整的理论。EPR 主要讨论他们所称的实在的元素(elemet of reality)。他们认为这样的实在元素必须在任何完整的物理学理论中得到表示。他们的目的是通过指出实在的元素没有被包含在量子力学中，来证明量子力学不是完整的物理学理论。

例如考虑分别属于 Alice 和 Bob 的量子比特组成的纠缠对：

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{1.2.44}$$

假定 Alice 和 Bob 彼此距离很远，Alice 沿 v 轴进行自旋测量，即她进行算子$\vec{v}\cdot\vec{\sigma}$的测量。无论 Alice 得到的结果是+1 还是-1，她都可以确切地预测 Bob 若也沿 v 轴测量自旋，将得到相反的结果。原因如下：假设$|a\rangle$和$|b\rangle$是$\vec{v}\cdot\vec{\sigma}$的本征矢，则存在复数α、β、γ和δ满足

$$|0\rangle = \alpha|a\rangle + \beta|b\rangle; \tag{1.2.45a}$$

$$|1\rangle = \gamma|a\rangle + \delta|b\rangle. \tag{1.2.45b}$$

于是得到：

$$\frac{|01\rangle-|10\rangle}{\sqrt{2}} = (\alpha\delta-\beta\gamma)\frac{|ab\rangle-|ba\rangle}{\sqrt{2}}. \tag{1.2.46}$$

由于$\alpha\delta-\beta\gamma$是酉矩阵$\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}$的行列式，所以等于一个相位因子。因此略去一个全局相位，有：

$$\frac{|01\rangle-|10\rangle}{\sqrt{2}} = \frac{|ab\rangle-|ba\rangle}{\sqrt{2}}. \tag{1.2.47}$$

所以若对两个粒子都进行$\vec{v}\cdot\vec{\sigma}$的测量，则第一个粒子的测量结果意味着第二个粒子得到相反的结果。按照 EPR 准则，量子比特沿 v 轴的自旋必对应一个实在的要素，并且应该在任何完整的物理学理论中被表示。然而量子力学仅仅说明测量$\vec{v}\cdot\vec{\sigma}$得到各结果的概率，因而量子力学是不完整的。

EPR 论文发表近三十年后，人们提出了一项测试实验，用于检验 EPR 准则是否正确。结果是自然通过实验否定了这样的观点，而与量子力学相吻合。Bell 不等式是检验这项实验的关键。为了得到不等式，先暂时忘掉量子力学的知识，应用直观进行分析。想象一个思想实验，Charlie 制备两个粒子，他如何制备粒子不重要，重要的是他可以重复实验。他制备好粒子后，分别发给 Alice 和 Bob。Alice 一收到粒子就对其进行测量。她有两台不同的设备，故她可从两种不同的测量中选择一种，这两种测量的属性分别记为P_Q和P_R。Alice 收到粒子后通过随机掷币来确定进行哪一种测量。设 Q、R 分别为测量P_Q和P_R得到的值。为简化，不妨设测量结果只有+1 和-1。同样，Bob 通过随机掷币决定测量两个属性P_S和P_T的哪一个，得到客观存在的 S 或 T 值，S、T 取+1 或-1。Alice 与 Bob 绝对精准地在同一时间进行测量，或用相对论的语言来说，以没有因果联系的方式进行测量。所以，Alice 的测量不可能干扰 Bob 的测量结果，因为物理性的影响传播的速度不能超过光速。注意到：

$$QS+RS+RT-QT = (Q+R)S+(R-Q)T. \tag{1.2.48}$$

因为$R,Q=\pm1$，所以$(Q+R)S=0$或$(R-Q)T=0$。因此无论 Q、R、S 和 T 的取值情况如何，都有$QS+RS+RT-QT=\pm2$。设测量前系统处于$Q=q$，$R=r$，$S=s$和$T=t$的概率是$p(q,r,s,t)$。则$QS+RS+RT-QT$的均值为：

$$\begin{aligned} E(QS+RS+RT-QT) &= \textstyle\sum_{qrst} p\,(q,r,s,t)(qs+rs+rt-qt)\\ &\le \textstyle\sum_{qrst} p\,(q,r,s,t)\times 2\\ &= 2 \end{aligned}, \tag{1.2.49}$$

又因为

$$\begin{aligned} E(QS+RS+RT-QT) &= \sum_{qrst} p\,(q,r,s,t)qs + \sum_{qrst} p\,(q,r,s,t)rs \\ &+ \sum_{qrst} p\,(q,r,s,t)rt - \sum_{qrst} p\,(q,r,s,t)qt\,, \\ &= E(QS)+E(RS)+E(RT)-E(QT) \end{aligned} \tag{1.2.50}$$

比较式(1.2.49)和式(1.2.50)得到 Bell 不等式：

$$E(QS)+E(RS)+E(RT)-E(QT) \leq 2. \tag{1.2.51}$$

(1.2.51)式也常被称为 CHSH 不等式，是诸多 Bell 不等式中的一个。重复多次实验，Alice 和 Bob 可以通过对样本取平均得到不等式左边的值，从而检验在真实的实验中，该不等式是否成立。

接下来，再从量子力学的角度分析这个过程。进行如下的量子力学实验，Charlie 制备一个双量子比特的状态：

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \tag{1.2.52}$$

并把第一个粒子传给 Alice，第二个粒子传给 Bob。他们进行测量的可观察量如下：

$$\begin{aligned} Q &= Z_1, & S &= \frac{-Z_2 - X_2}{\sqrt{2}} \\ R &= X_1, & T &= \frac{Z_2 - X_2}{\sqrt{2}} \end{aligned}, \tag{1.2.53}$$

简单计算可得到这些可观测量的平均值：

$$< QS >= \frac{1}{\sqrt{2}}, \tag{1.2.54a}$$

$$< RS >= \frac{1}{\sqrt{2}}, \tag{1.2.54b}$$

$$< RT >= \frac{1}{\sqrt{2}}, \tag{1.2.54c}$$

$$< QT >= -\frac{1}{\sqrt{2}}. \tag{1.2.54d}$$

于是

$$E(QS)+E(RS)+E(RT)-E(QT) = 2\sqrt{2}. \tag{1.2.55}$$

量子力学得到的结果与 Bell 不等式矛盾。幸运的是，可以通过实验来判断哪个才是正确的。事实上，实验的结果支持量子力学的语言，而违背了 Bell 不等式。这意味着在推导 Bell 不等式的过程中至少有一个是错的。推导 Bell 不等式的过程中有两个假设：

（1）物理性质P_Q、P_R、P_S和P_T具有独立于观测的值 Q,R,S,T 的假设，称为实在性假设；

（2）Alice 的测量不影响 Bob 测量结果的假设，称为定域性假设。

这两个假设合称定域实在性假设。实验表明 Bell 不等式被破坏，所以两个假设至少有一个是不合理的。当然它们在直观上看是合理的，符合日常的生活经验。Bell 不等式说明了关于世界如何运行的直觉有时可能是错的。

第 2 章 量子通信与量子密码

§2.1 量子通信

2.1.1 Super-dense Coding

用四个 Bell 基$|\boldsymbol{\Phi}^+\rangle$、$|\boldsymbol{\Phi}^-\rangle$、$|\boldsymbol{\Psi}^+\rangle$、$|\boldsymbol{\Psi}^-\rangle$来进行 Super-dense Coding。Alice 和 Bob 共享一个处于 Bell 态$|\boldsymbol{\Phi}^+\rangle$的 EPR 对，Alice 对手中的粒子做下述四个操作之一：

$$\boldsymbol{X_1}|\boldsymbol{\Phi}^+\rangle = |\boldsymbol{\Psi}^+\rangle,\ \boldsymbol{Z_1}|\boldsymbol{\Phi}^+\rangle = |\boldsymbol{\Phi}^-\rangle$$

$$\boldsymbol{Y_1}|\boldsymbol{\Phi}^+\rangle = |\boldsymbol{\Psi}^-\rangle,\ \boldsymbol{I_1}|\boldsymbol{\Phi}^+\rangle = |\boldsymbol{\Phi}^+\rangle \tag{2.1.1}$$

然后将粒子发给 Bob，如果 Bob 可以进行 Bell 基测量，则可以确知 Alice 所做的操作，于是实现了一个粒子传递 2 比特经典信息的任务。将此功能称为 Super-dense Coding。

2.1.2 量子 Teleportation

如果只通过定域量子操作和经典信号传递（LOCC）即可将$|\boldsymbol{\Psi}\rangle$变为$|\boldsymbol{\Phi}\rangle$，则称$|\boldsymbol{\Psi}\rangle$LOCC 可归约为$|\boldsymbol{\Phi}\rangle$，记为

$$|\boldsymbol{\Psi}\rangle \xrightarrow{\boldsymbol{LOCC}} |\boldsymbol{\Phi}\rangle \tag{2.1.2}$$

若$|\boldsymbol{\Psi}\rangle \xrightarrow{\boldsymbol{LOCC}} |\boldsymbol{\Phi}\rangle$且$|\boldsymbol{\Phi}\rangle \xrightarrow{\boldsymbol{LOCC}} |\boldsymbol{\Psi}\rangle$，则称$|\boldsymbol{\Psi}\rangle$与$|\boldsymbol{\Phi}\rangle$是 LOCC 等价的，记为

$$|\boldsymbol{\Psi}\rangle \xleftrightarrow{\boldsymbol{LOCC}} |\boldsymbol{\Phi}\rangle \tag{2.1.3}$$

如果$|\boldsymbol{\Psi}\rangle$与$|\boldsymbol{\Phi}\rangle$只相差一个定域酉变换，则称$|\boldsymbol{\Psi}\rangle$与$|\boldsymbol{\Phi}\rangle$是 LU 等价的。 Bennett et al. 证明，对于纯态，LU 等价与 LOCC 等价是相同的。从 LOCC 的观点来看 Teleportation：

$$\begin{aligned}|\boldsymbol{\Psi}^-\rangle_{12}|\boldsymbol{\varphi}\rangle_3 &= \frac{\boldsymbol{1}}{\sqrt{\boldsymbol{2}}}(|\boldsymbol{0}\rangle_1|\boldsymbol{1}\rangle_2 - |\boldsymbol{1}\rangle_1|\boldsymbol{0}\rangle_2)(\boldsymbol{\alpha}|\boldsymbol{0}\rangle_3 + \boldsymbol{\beta}|\boldsymbol{1}\rangle_3)\\ &= \frac{\boldsymbol{1}}{\boldsymbol{2}}[(\boldsymbol{\alpha}|\boldsymbol{1}\rangle_1 + \boldsymbol{\beta}|\boldsymbol{0}\rangle_1)|\boldsymbol{\Phi}^+\rangle_{23} + (\boldsymbol{\alpha}|\boldsymbol{1}\rangle_1 - \boldsymbol{\beta}|\boldsymbol{0}\rangle_1)|\boldsymbol{\Phi}^-\rangle_{23}\\ &\quad +(-\boldsymbol{\alpha}|\boldsymbol{0}\rangle_1 - \boldsymbol{\beta}|\boldsymbol{1}\rangle_1)|\boldsymbol{\Psi}^+\rangle_{23} + (\boldsymbol{\alpha}|\boldsymbol{0}\rangle_1 - \boldsymbol{\beta}|\boldsymbol{1}\rangle_1)|\boldsymbol{\Psi}^-\rangle_{23}]\end{aligned} \tag{2.1.4}$$

Alice 测量手中的 2,3 粒子处于哪一 Bell 态，告诉 Bob，Bob 对粒子 1 进行操作(X,Y,Z,I)，以使粒子 1 处于相应态。

2.1.3 量子纠缠交换

纠缠交换（ Entanglement Swapping ）方案：通过 LOCC 使从未谋面、也未进行直接量子通信的 Bob 和 Charlie 共享纠缠态。

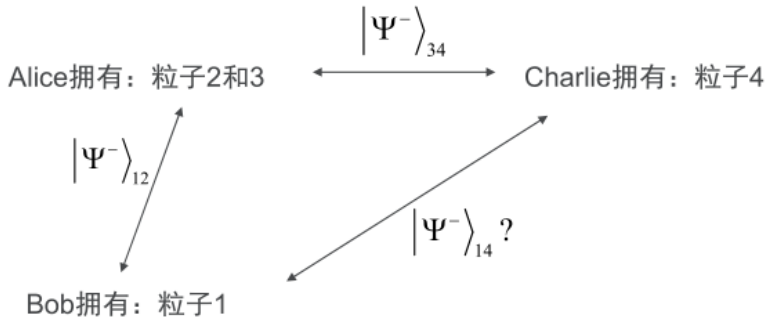


图 2.1-1 共享纠缠态示意图

初态为：

$$|\Psi_{1234}\rangle = \frac{1}{2}(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2)(|0\rangle_3|1\rangle_4 - |1\rangle_3|0\rangle_4) \quad (2.1.5)$$

将其表示为按$|\Phi^{\pm}\rangle_{23}$和$|\Psi^{\pm}\rangle_{23}$展开的形式：

$$\begin{aligned}|\Phi\rangle_{1234} = \frac{1}{2}[&|0\rangle_1\frac{1}{\sqrt{2}}(|\Psi^+\rangle_{23} - |\Psi^-\rangle_{23})|1\rangle_4 \\ &-|0\rangle_1\frac{1}{\sqrt{2}}(|\Phi^+\rangle_{23} - |\Phi^-\rangle_{23})|0\rangle_4 \\ &-|1\rangle_1\tfrac{1}{\sqrt{2}}(|\Phi^+\rangle_{23} + |\Phi^-\rangle_{23})|1\rangle_4 + \\ &|1\rangle_1\frac{1}{\sqrt{2}}(|\Psi^+\rangle_{23} + |\Psi^-\rangle_{23})|0\rangle_4] \\ &= \frac{1}{2}(-|\Phi^+\rangle_{23}|\Phi^+\rangle_{14} + |\Phi^-\rangle_{23}|\Phi^-\rangle_{14} \\ &+|\Psi^+\rangle_{23}|\Psi^+\rangle_{14} - |\Psi^-\rangle_{23}|\Psi^-\rangle_{14})\end{aligned} \quad (2.1.6)$$

进行下述步骤：

1、Alice 通过定域操作测量粒子 2、3；

2、Alice 用经典信道通知 Bob 和 Charlie 测量结果；

3、 Bob 和 Charlie 通过定域操作（I,X,Y,Z)共享$|\Psi^-\rangle_{14}$。

§2.2 量子密码协议

狭义量子密码学是指用量子技术实现经典密码学的目标，包含量子密钥分配协议、量子比特承诺协议、量子不经意传输协议等。将量子力学与传统密码学相结合始于 1969 年，Wiesner 首先提出了量子钞票的概念[1]，但当时并未发表。1984 年 Bennett 和 Brassard 基于 Wiesner 思想并加以发展，提出了著名的量子密钥分配协议 BB84 协议和量子掷币协议[2]，其中量子密钥分配 BB84 协议在之后被证明是无条件安全的[3-6]。之后量子密码受到广泛关注，各量子密码研究分支都得到了快速发展。

2.2.1 量子密钥分配协议

量子密码的发展有其自身发现问题、解决问题的过程，某些部分可能与传统密码无关。例如量子密钥分配（Quantum key distribution，QKD）系统的光子数分束攻击问题的解决，

以及近来一些关于 QKD 系统的侧信道攻击和对抗问题的研究。虽然量子密码有许多内容，但它之所以现在能受到众多密码学家的重视，主要还是因为 QKD。

QKD 实现了一个密码学家的理想：异地同步的（真）随机数生成器。基于密码学现有结果完善 QKD 系统，包括 QKD 经典信道的认证问题（经典信道无条件安全的消息认证和身份鉴别），经典数据的后处理方法（数据协调和保密增强），基于密码算法的 QKD 网络构建方案，等等。

量子密钥分配协议是为了依靠不可靠的信道为通信双方建立共享的安全密钥。实现 QKD 协议需要两个信道：一个量子信道，可以容忍不违背物理学原理的任何攻击；一个经典信道，是公开的抗干扰（unjammable）信道（广播信道或认证信道）,采用认证信道时，需要有初始的认证密钥。根据测量塌缩原理，主要窃听者对光子进行测量就会破坏部分信息，从而被通信双方发现；而不可克隆定理保证了窃听者无法在信道中复制量子信号，其安全性由量子力学基本原理保证。

Key		1				0	1				0
A basis	⊗	⊕	⊕	⊗	⊕	⊗	⊗	⊕	⊗	⊗	⊕
A bit value	0	1	0	1	1	0	1	0	0	0	0
A sends	$\|45^0\rangle$	$\|H\rangle$	$\|V\rangle$	$\|135^0\rangle$	$\|H\rangle$	$\|45^0\rangle$	$\|135^0\rangle$	$\|V\rangle$	$\|45^0\rangle$	$\|45^0\rangle$	$\|V\rangle$
B basis	⊗	⊕	⊗	⊕	⊕	⊗	⊗	⊗	⊕	⊕	⊕
B bit	0	1	0	0	1	0	1	1	0	1	0
Same basis?	y	y	n	n	y	y	y	n	n	n	y
A keeps	0	1			1	0	1				0
B keeps	0	1			1	0	1				0
Test Eve	y	n			y	n	n				n

图 2.2-1QKD(BB84)协议执行过程举例

执行过程大致讲解：Alice 随机生成一串长度为n的二进制随机串，想将其发送给 Bob，则他随机选择发送基对其进行发送。Bob 随机选择测量基对来自 Alice 的粒子进行测量，若 Bob 所选择的的测量基与 Alice 所选择的发送基完全相同，则 Bob 能够得到 Alice 的长度为n的随机串。然而，Bob 所选择的的测量基与 Alice 所选择的发送基完全相同的概率为$1/2^n$。一按概率计算，Bob 只有一半测量基与 Alice 的发送基相同。Alice 和 Bob 通过公开信道比较他们所使用的基，留下使用相同基时所对应的比特得到裸密钥。为测量潜在的窃听，Alice 和 Bob 从裸密钥中拿出一部分进行核对，如果完全相同，说明中间没有窃听，如果有不同的比特，说明存在窃听。

QKD 的 BB84 协议可看作是一个独特的远程同步的（真）随机数生成器：

1) 用于认证的密钥看作种子；

2) 双信道，交互式；

3) 单向变换（算子）：正交编码→共轭编码；

4) 具有无条件安全性。

就经典密码学而言，远离的两个相同的 PRBG 由同一个种子控制，可以异地同步地生成相同的伪随机序列，但所生成序列的熵至多等于该种子的熵，绝对不会增大，而由 BB84

协议生成的（真）随机序列的熵会大于种子的熵，那么熵是从哪来的？下面从熵的角度分析BB84 协议。

对于 Eve 和 Bob 而言，Alice 发送的是混合态$\rho = \frac{1}{2}I$，有

$$S(\rho) \equiv -tr(\rho log\rho) = -\sum_x \lambda_x log\lambda_x = 1 \quad (2.2.1)$$

BB84 协议所采用的共轭编码$I(A,E) > 1 - 0.2198$，有测量基（密钥）的人能以概率 1 得到该比特，Breidbart 攻击使敌手以 0.85 概率得到该比特。共轭编码的意义不在于强的加密，而在于当被攻击的量子位多时能确认攻击并放弃数据，以及当被攻击的量子位少时能有效地消除攻击效果。BB84 协议具有如下优势：

- 优势提取：Alice 保留 Bob 选基正确的位，从而使保留的序列对于 Bob 而言熵大幅减小，但对于 Eve 而言熵不变；
- 信息协调：使 Bob 的熵趋于零，Eve 的熵有所减小但不趋于零；
- 保密度放大：保密度(privacy)=1-I(A,E)，Bob 的熵保持为零，由于序列长度减小，Eve 的总熵减小，但每比特的熵趋于 1。

安全性是量子密钥分配关注的重点，包括理论安全性和实际安全性。1996 年 Mayers 最初证明了 QKD 协议的无条件安全性[3]，他根据量子力学基本原理，利用信息论计算出窃听者可以得到的关于密钥的最大信息量，但是证明过程比较复杂。其证明思想被 Lo 所发展[4]，提出了基于纠缠提纯的安全性证明，但是其证明需要量子计算机来完成。2000 年 Shor 和 Preskil 提出了比较简单的安全性证明方法[5]，在其证明中只需计算已校验的比特翻转错误便可确定总的错误概率，由此产生的密钥的安全性仍可由量子不可克隆定理和测不准原理保证。之后 Renner[6] 提出了基于信息论的 BB84 协议的普适安全证明，证明了量子密钥的绝对安全性实质上可以由信息量的一系列关系来表征。

虽然 QKD 理论安全性已经得到证明，但是实际系统所采用的设备总不是完美的，使得系统存在一些安全隐患。实际 QKD 系统的攻防问题主要集中在五部分：光源、编码、信道、解码、探测。

（1）光源：在理想模型中，光源应该是理想的单光子源，但是目前为止，实用高效的单光子源还没有实现，大多数 BB84 协议实验都是用典型平均光子数为 0.1 或者更大的相位随机弱相干脉冲（WPCs），这些状态可以很容易的用标准半导体激光器和校准衰减器制备。主要缺点是：WPCs 的光子数服从泊松分布，一些信号在相同的量子态可能包含了不止一个光子，很容易受到光子数分束（PNS）攻击[7-9]。在 PNS 攻击中，Eve 的最佳策略为：拦截所有单光子脉冲，窃听所有多光子脉冲，她只分走多光子脉冲中的一个光子，将剩余 n-1 个光子转发给 Bob，保存该单光子态直到 Alice 和 Bob 在公开经典信道上讨论编码基为止。通过对公开的经典信道的窃听，Eve 得知编码基后按照其对手中单光子测量得到密钥。为抵抗 PNS 攻击，多采用诱骗态的 QKD 协议[10-13]，目前该方法在实际中得到广泛的应用[14-17]，京沪干线项目中也采用了诱骗态的协议。一般系统中采用多个激光器作为量子态的发送装置，不同的激光器编码不同的信息，这些激光器的参数和制造工艺可能不完全相同，存在侧信道攻击。Nauerth 等分析了自由攻击 QKD 系统在时间、频谱、强度等维度上的信息泄露[18]。

（2）编码：在实际系统中，编码设备可能存在某种缺陷，使得发送端实际发送的量子态并非理想的 BB84 协议中的四态。Fung 等[19]最早提出在往返式的 QKD 系统中，窃听者可以通过改变光脉冲到达相位调制器的时间改变发送的量子态，从而获得更多信息，即相位重映射攻击。实际系统中发送者用相位调制器来调制光源发射光子的相位，相位调制器由电信号控制，电信号大体分为上升沿、稳定期和下降沿。量子信号在正常状态时在稳定区入射，此时相位为 BB84 协议中的四态；在往返式系统中，窃听者能够控制光脉冲入射到发送方的时间，使得光脉冲在上升沿阶段进行调制，此时光脉冲的实际相位变为。窃听者可优化的值，利用截取- 重发攻击对量子态进行 POVM 测量，使得其引入的误码率最小。2010 年 Lo 小组在商用 QKD 系统中实现了该攻击[20]。

（3）信道：关于只针对信道的攻击方案较少，2013 年 Yang 等[21]提出了针对有损有噪信道的 BB84 协议的一种个体攻击?——耗散攻击。其主要原理是，任何光信号都可以利用偏振分束器分解到两个正交的方向 a，b 上，若沿方向 a 对此信号进行耗散，其 a 方向分量就会减小，从而改变原信号的强度和方向。Eve 只需随机在四态（Breidbart 基）所处 4 个方向上选取一个进行耗散以保证“0”“1” 数量平衡即可。这样虽然总体密钥是均匀分布的，但是对于攻击者而言每个比特为 0、为 1 的概率不同，她可以以一定优势得到量子密钥。

（4）解码：在 QKD 系统中，Bob 随机的选择两个基来测量 Alice 的量子态，而这种随机选择过程可以分为主动选择和被动选择两种模式。就目前的分析看来，人们尚没有发现主动选基过程中的缺陷及窃听者的攻击方案。但是对被动选基系统而言，研究表明，窃听者在某些情况下可以控制 Bob 测量基的选择。2011 年 Li 等[22]就提出被动选基系统中所使用的 BS 可能存在波长相关性，所以窃听者可以通过发送不同波长的光脉冲来控制 Bob 的基选择过程，进而可以确定性的预测 Bob 探测器的响应。随后该小组在 2012 年将该方法扩展到了连续变量 QKD 系统中，从而实现了对连续变量 QKD 的攻击[23]。

（5）探测：在实际 QKD 系统中，由于探测器的不完美，窃听者能够控制接收端探测器的响应或输出结果，从而获取部分或全部信息而不被发现。伪态攻击、时移攻击、致盲攻击都是此类攻击。

2006 年 Makarov 等[24]提出利用 QKD 系统中所使用的两个单光子探测器在效率上的不匹配，使得窃听者有可能控制接收端探测器的响应，即伪态攻击。2008 年他们对 SARG04、相位-时间编码、DPSK 和 Ekert 协议进行了伪态攻击[25]。伪态攻击是一种截取-重发类攻击，Eve 复制 Bob 的装置，截取 Alice 发送的态后随机选择测量基进行测量，然后制备处于相反基下的相反值的态发送给 Bob 且控制参数为其测量值。控制参数即利用了两个探测器效曲线的不匹配性使得只有其中一个探测器响应。令探测器 0 响应的参数记为 t0，只令探测器 1 响应的参数记为 t1。例如，若 Eve 测到，她发送给 Bob 并使得控制参数为 t0。虽然这会使得 Bob 检测到的效率变低，但是 Eve 可以通过调节光强来弥补。

时移攻击同样利用两探测器的差异，理论上 Bob 所用的两个探测器的性能应该完全一样，但是实际系统中由于制造工艺等原因两个探测器总会有微小差别使得其探测效率-时间曲线并非完全吻合。一旦曲线不吻合，就存在某时间段使得只有一个探测器响应。Eve 通过控制光脉冲到达 Bob 的时间来控制探测器的响应。比如 Eve 想让探测器 0 发生响应，那么她就可以通过调节光路的长度让光脉冲在只有探测 0 响应的时间到达 Bob 端。在此攻击中 Eve 不需要进行截取- 重发攻击，故不需要接收和制备量子态的装置。Zhao 等[26]利用探测器的效率不匹配在实验上实现了时移攻击，他们所攻击的商业 QKD 系统中有内置的时间校

准装置，理想情况下两探测器响应时间差是恒定的，但是偶尔会有更大的效率不匹配，根据实验，达到最大效率不匹配的概率为 4%。对于伪态攻击和时移攻击，窃听者仅能获得部分信息，而致盲攻击可以获得全部信息。大部分的单光子探测器的核心是雪崩光电二极管（APD），APD 的工作区分为线性模式和盖革模式。当加载在 APD 的反偏电压小于雪崩电压时，APD 处于线性区，只有强光才能产生较大的光电流达到阈值电流，从而计数；当加载在 APD 的反偏电压大于雪崩电压时，单光子有一定概率被 APD 吸收产生电子空穴对并在反偏电压的加速下产生雪崩效应，从而计数。反偏电压通过电阻加载在 APD 上，如果 APD 产生光电流会使电阻拉低偏置电压。致盲攻击指的是 Eve 向 Bob 发送一定功率的连续激光，使得加载到 APD 上的偏置电压降低处于线性模式。然后 Eve 采用截取-重发攻击，将他测量到的结果重新制备强光信号后发给 Bob，使得 Bob 端光电流达到阈值电流并响应。只要 Eve 仔细的设计光功率的强度，Bob 端的测量结果与她完全一致。2009 年 Makarov 等[27]提出可以利用较强光致盲被动淬灭单光子探测器从而攻击 QKD 协议。2010 年该组又指出致盲攻击对于门控单光子探测器同样适用[28、29]。Lydersen 等利用探测器的这一漏洞对 Id Quantique 公司的 Clavis2 商用系统和 MagiQ 公司的 QPN5505 商用系统成功的实施了致盲攻击[30]，完全获得了信息而没有被发现。

QKD 在实验方面的进展如下：

BB84 协议的提出是在 1984 年，关于它的第一个实验的执行是在 1989 年，该实验装置较为简陋，通信的距离仅有 30 厘米，但其基本原理有较为重大的意义。

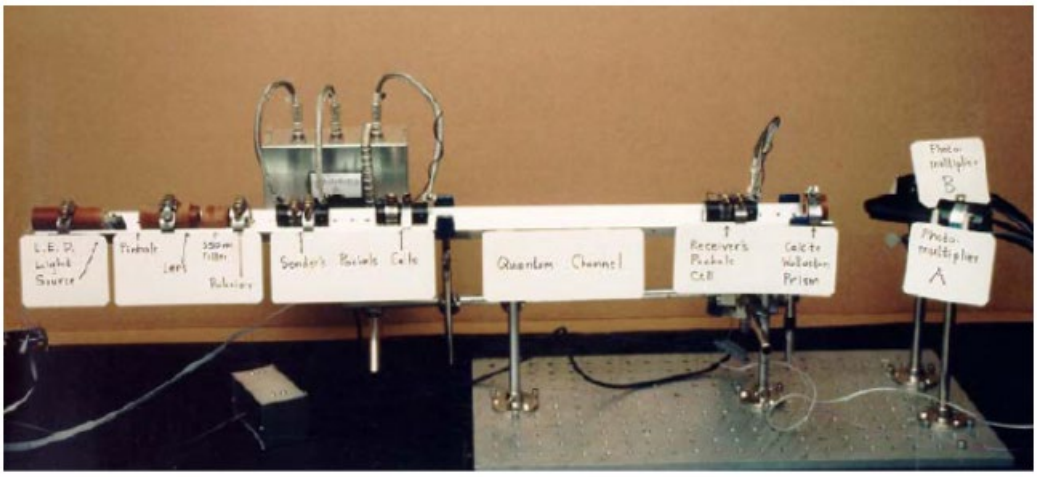


图 2.2-2 BB84 协议的第一个实验装置

十年之后，美国的 Los Alamos 实验室做了通信距离为 48 千米的 QKD 实验装置，即使用 48 签名长的光纤使得两方之间的通信距离达到 48 千米。

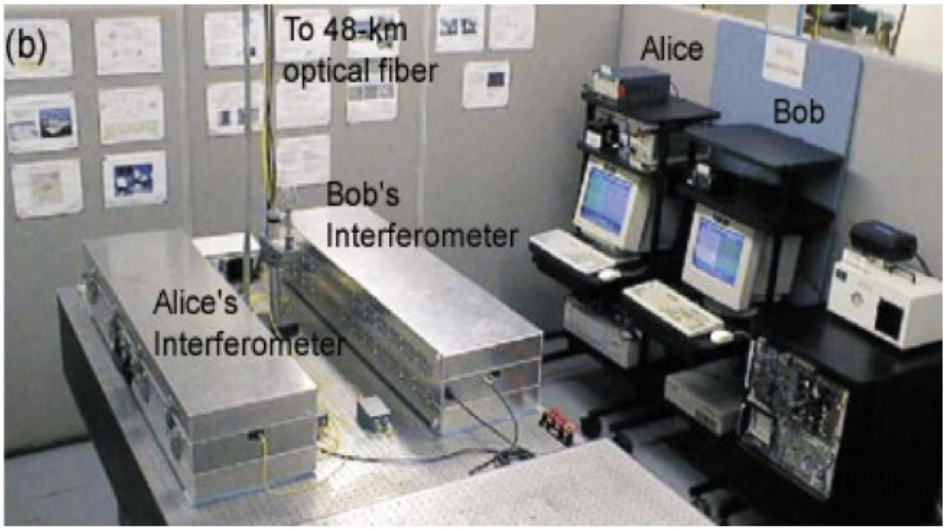


图 2.2-3 Los Alamos 实验室实验装置

2002 年初，在阿尔卑斯山选择海拔分别为 2950 米和 2244 米的两个点，海拔在 1000 米以上使得信道所受大气的影响较小。实现量子密钥分配在自由空间的传输距离达到 23.4 千米。

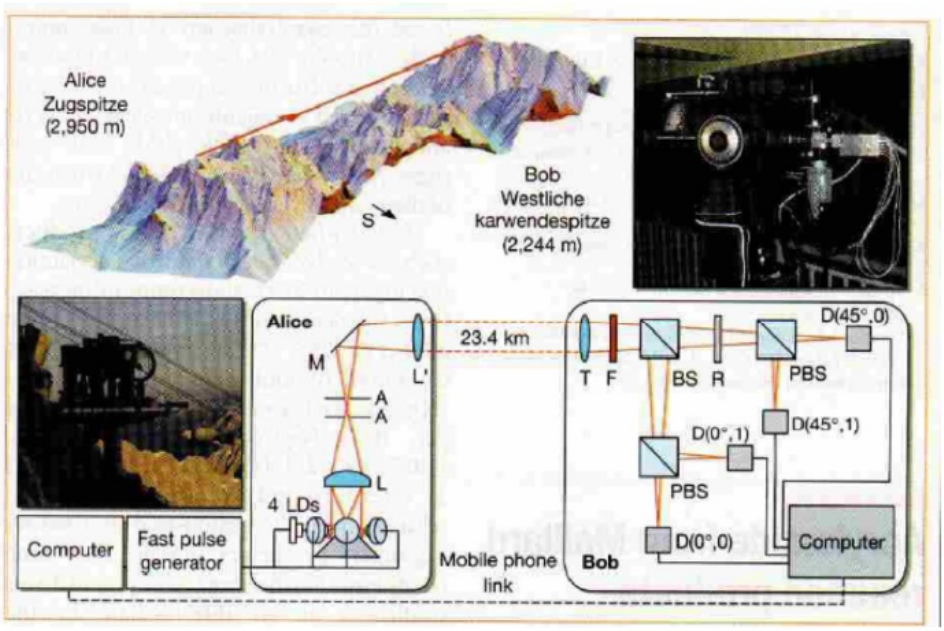


图 2.2-4 自由空间 QKD 实验装置

2003 年，美国国家标准与技术研究院和波士顿大学的科研人员研制出单脉冲光探测器，为开发安全量子通信和密码系统提供了关键技术。美国在 2005 年建成了 DARPA 量子网络，其连接节点有 3 个，分别为美国 BBN 公司、哈佛大学和波士顿大学，延伸长度为 10 公里。

欧洲联合了来自 12 个欧盟国家的 41 个伙伴小组成立了 SECOQC 量子通信网络，并于 2008 年 10 月在维也纳现场演示了一个基于商业网络的安全量子通信网络，该系统包含 6 个节点，其组网方式为在每个节点试用多个不同类型量子密钥分发的收发系统并利用可信中继

进行联网。2009 年瑞士日内瓦大学、西瑞士应用科学大学以及 ID Quantique 公司组建 SwissQuantum 量子网络测试平台，对量子密码网络长时间运行的稳定性进行测试，测试结果表明这项技术已经成熟可靠。2013 年，日本国家情报通信研究机构通过洲际合作，在东京构建了东京 QKD 网络。

此后，一些实用化的小规模光纤量子通信网络先后在国际上建成。全球信息产业巨头 IBM、Philips、AT&T、Bell 实验室等对量子通信技术投入大量研发资本，开展量子通信技术的研发和产业化。瑞士 ID Quantique、美国 MagiQ Technologies 以及澳大利亚 QuintessenceLabs 等公司已有量子密码相关产品。其中，瑞士 ID Quantique 的量子密码产品已在多个领域得以应用，例如，为瑞士两家私人银行(Hyposwiss、NotenStein)分别构建了量子保密通信专线，以及 2010 年南非世界杯期，用 QKD 终端建成了一条实验性的量子加密通信线路，用于保护世界杯期间的新闻报道的通信安全。由此可见，QKD 技术在实际中的应用比较成熟。

2004 年，郭光灿课题组在国际上首次成功分析实际光纤量子密码系统不稳定的原因，并使用法拉第反射镜的迈克尔逊干涉方案实现了国际上第一个城际量子密码实验，量子线路长度 125 公里，创下了当时的世界纪录。

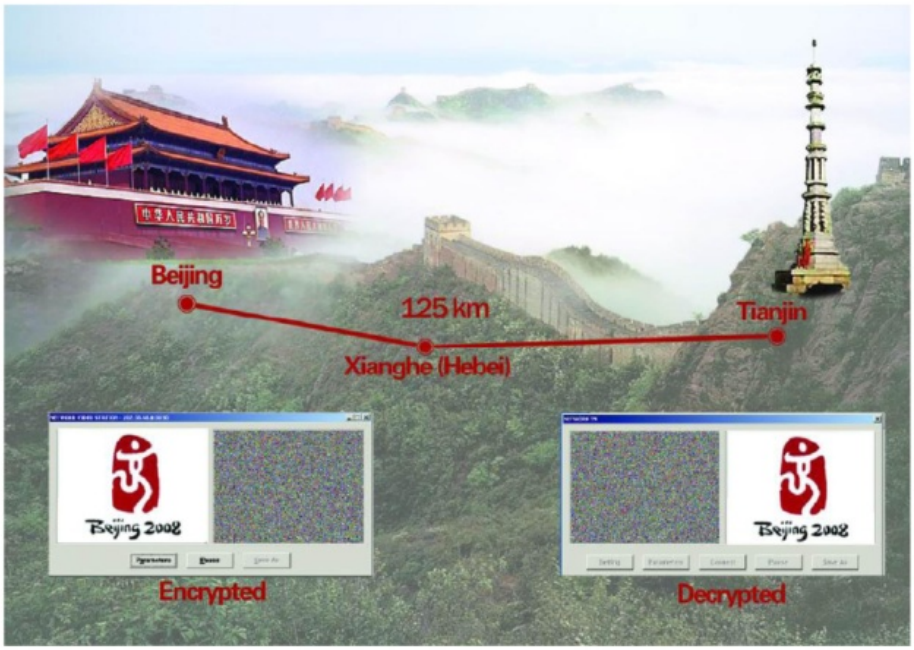


图 2.2-5 中国科大 QKD 光纤实验 125km

2007 年，中科大潘建伟团队以及美国洛斯阿拉莫斯国家实验室—美国国家标准与技术研究院联合实验组同时实现超过 100 公里的诱骗态光纤量子密钥系统。2008 年，潘建伟团队基于诱骗态方案，实现了国际上首个全通型量子通信网络。2013 年，潘建伟团队和加拿大的 Tittel 小组分别在国际上首次实验实现了测量器件无关的量子密钥分发，解决了单光子探测系统易被黑客攻击的安全隐患。2014 年，潘建伟团队首次实现了测量器件无关的量子纠缠验证，大大提高了实际系统中纠缠检验的正确性。同年，该团队成功将量子密钥分发系统的安全距离扩展至 200 公里，创下新的世界纪录。

2.2.2 量子比特承诺（QBC）和量子不经意传输协议（QOT）

(1)比特承诺协议与不经意传输协议

不经意传输（Oblivious Transfer，缩写为 OT）协议和比特承诺（Bit Commitment，缩写为 BC）协议是密码学的安全基础协议，经常出现在安全多方计算和零知识证明等各类密码协议之中。在现代密码学中，OT 协议和 BC 协议是基于二次剩余或离散对数等数学难题构造的，Shor 量子算法的提出使得此类构造不再具有安全性。

比特承诺协议是一个双方协议，分为两个阶段：承诺阶段和公开阶段。在承诺阶段，发送者给出对一个确定消息或数据的承诺，以保证自己确实拥有该数据而又不泄露它；在公开阶段，发送者给出该消息（数据）和承诺阶段的相关信息，接收者可以由此验证。比特承诺协议的安全性要满足隐藏性和绑定性两个要求：

（i）隐藏性：在承诺阶段完成对 b 的承诺后，接收者不能获得 b 的信息；

（ii）绑定性：在公开阶段，发送者不能使接收者接受一个不同于 b 的消息b'。

承诺阶段:

a) Alice 和 Bob 协定两个安全参数 m 和 n;

b) Alice 选择一个随机比特$b \in \{0,1\}$作为承诺值，根据承诺值生成 m 串随机序列，每串序列包含 n 比特，表示为$a^{(i)} \equiv \left(a_1^{(i)} a_2^{(i)} \ldots a_n^{(i)}\right) \in \{0,1\}^n, i = 1,2, \ldots., m$，每个序列满足等式$a_1^{(i)} \oplus a_2^{(i)} \oplus \ldots \oplus a_n^{(i)} = b$;

c) Bob 也生成 m 穿随机序列，每串序列包含 n 比特，表示为$b^{(i)} \equiv \left(b_1^{(i)} b_2^{(i)} \ldots b_n^{(i)}\right) \in \{0,1\}^n$;

d) Alice 和 Bob 通过执行一个逐比特比对方案使得 Bob 拥有一部分证据，在这一步中，Bob 可以逐一对比$b_j^{(i)}$和$a_j^{(i)}$，从而知道$b_j^{(i)} = a_j^{(i)}$，$b_j^{(i)} \neq a_j^{(i)}$,或者得不到任何信息（⊥），通过逐比特的比对，将 Bob 确定 Alice 该比特的概率记为p，Alice 知道 Bob 确定她的比特的概率为q，要求$0 \leq q < p < 1$.

公开阶段:

1) Alice 公开承诺值 b 和 m 个序列$a_1^{(i)} a_2^{(i)} \ldots a_n^{(i)}$， i = 1, 2, ..., m;

2) Bob 验证$a_1^{(i)} \oplus a_2^{(i)} \oplus \ldots \oplus a_n^{(i)} = b$是否成立，验证 Alice 公开的每比特$a_j^{(i)}$是否与他确定知道的值相同。若一致则承认 Alice 的承诺为 b，否则不承认。

不经意传输协议是一个双方协议（发送者，接收者）。发送者拥有 n 个秘密消息，接收者欲按照自己的意愿获取其中一（几）个消息。当协议结束后，接收者按照自己的选择得到了想要的那个（些）秘密，但却没有得到其余秘密的任何信息，同时发送者也不知道接收者选择的是哪个(些)秘密。1988 年 Crépeau 证明了 R-OT 和OT_1^2是等价的，可以互相构造[31]。协议需要满足以下条件：

（i）正确性：协议后，Bob 可以得到他想得到的量子比特；

（ii）发送者安全性：Bob 除了自己选择得到的以外不能得到另一量子比特的任何信息；

（iii）接收者安全性：无论发送者采取什么策略，她都不能得到有关接收者选择的任何信息。

1984 年，Bennett 和 Brassard 在文献[2]中不但提出了 BB84 密钥分配方案，还给出了一个掷币方案，然而此方案会受到 EPR 攻击，并不安全。1988 年 Crépeau 和 Kilian 提出第一个 QOT 协议[32]，这个协议和之后的 QOT 协议是基于 QBC 协议构造的。1991 年，Bennett 等人[33]基于 BB84 编码给出了 QBC 方案，并宣称它是无条件安全的。1992 年，Bennett 等提出了可实用化的 QOT 协议[34]，但是它的安全性建立在接收者 Bob 不可以延迟测量的基础上，否则他可以获得两条信息，破坏了隐藏性。1993 年 Brassard 等提出了一个 QBC 协议并对其安全性进行了证明[35]，这一证明曾被普遍接受。1994 年，Crépeau 用[BCJL]QBC 协议构造出 QOT 协议，在此协议中 Bob 可以延迟测量。1995 年，Yao 证明无条件安全的 QBC 协议可以用于构造无条件安全的 QOT 协议，如果 QBC 是安全的，那么基于它构造出的 QOT 也是安全的[36]。这些结论使得量子密码的前途非常光明，因为 Killian 证明了 OT 协议可以构造任何两方密码协议。但是，1996 年 Mayers 发现[BCJL] 协议是不安全的[27]。1997 年，Mayers 和 Lo,Chau 分别得出一致的结论：无条件安全的量子比特承诺是不可能的[38-40]，即著名的 no-go 定理。

No-go 定理并不排除存在计算安全的量子比特承诺。2000 年，Dumais 等人[41] 给出了一个基于计算假设的量子单向置换可以用于构造计算安全的比特承诺方案，并证明了所给方案是完全隐藏和统计安全的。2011 年，杨理等人[42]试图提出不受 no-go 定理限制的 QBC 方案，但由于 EPR 对的攻击会破坏方案的绑定性，只构造出了满足无条件绑定性或无条件隐藏性的一系列方案。

然而，量子不经意传输协议是否一定要建立在量子比特承诺之上呢？一些科研人员提出了不基于量子比特承诺的协议。2006 年，吕欣等根据 Kawachi 公钥算法提出了计算安全的量子不经意传输协议[43]。2006 年，何广平等提出了基于量子纠缠的不经意传输协议[44]。2008 年，I.-C. Chen 等提出了运用四态后选择的量子密钥分配协议[45]的量子不经意传输协议[46]。2010 年，提出了基于物理不可克隆方程的不经意传输协议[47]。2013 年，杨理提出了一个更简单的方案[48]，一个两态的 R-OT 协议，运用 Crépeau 的方法构造成OT_1^2协议，进而可通过经典协议改造方法得到承诺协议。

在实验方面，2004 年，G. Molina-Terriza 等基于 Ambainis[49]的协议进行了量子掷币实验，这是量子掷币的第一个实验[50]。2008 年，D. Fattal 等实验验证了无纠缠的欺骗敏感的量子不经意传输协议[51]。2012 年，Nelly Huei Ying Ng 等进行了噪声存储模型下的比特承诺协议的实验[52]。2013 年，T. Lunghi 等改进了 Kent 基于量子通信和狭义相对论的量子比特承诺协议[53] 并进行了实验[54]。随后潘建伟组也对 Kent12 协议进行了实验，两个代理间距离超过 20km[55]。

（2）半反直观量子比特承诺协议

BC 模型中承诺阶段的第 4 步调用了一个逐比特比对方案，下面先基于反直观 QKD 构造了一个两方比对方案，这个方案可以以一定概率实现逐比特的比对。然后根据 BC 模型和逐比特比对方案给出了一个半反直观量子比特承诺协议。

图 2.2-6 逐比特比对方案和半反直观 QBC 协议的装置图

1）基于反直观密码的逐比特比对方案

a) Alice 和 Bob 依照图 2.3-20 搭建设备，其中分束器 BS 为半透半反镜；

b) Alice 和 Bob 进行一个测试来确定时间参数，Bob 发送一串由$|H\rangle$和$|V\rangle$构成的量子态序列给 Alice，并且通过经典信道告诉 Alice 他发送的态，Alice 在合适的时间控制光开关 SW 使得三个探测器D_0, D_1, D_2分别响应，通过这个测试可以确定三个时间参数：量子态从光源 S 经过偏振分束器 PBS 到达光开关 SW 的时间Δt_0；量子态从光源 S 经过光延迟环 OL 到达光开关 SW 的时间Δt_1；量子态从光源 S 被 Alice 端法拉第镜 FM1 反射重新回到 Bob 端的时间Δt_2；

c) Alice 和 Bob 协定一系列时刻点$\mathrm{t}_1^{(\mathrm{i})}\mathrm{t}_2^{(\mathrm{i})}\ldots\mathrm{t}_\mathrm{n}^{(\mathrm{i})}$，其中$i = 1,2,\ldots m$.Bob 生成他需要对比的序列$\left(\mathrm{b}_1^{(\mathrm{i})}\mathrm{b}_2^{(\mathrm{i})}\ldots\mathrm{b}_\mathrm{n}^{(\mathrm{i})}\right) \in \{0,1\}^n$并在时刻$\mathrm{t}_\mathrm{j}^{(\mathrm{i})}$发送相应的量子态$|\psi_{b_j^{(i)}}\rangle$给 Alice，其中$|\psi_0\rangle = |H\rangle, |\psi_1\rangle = |V\rangle$；

d) Alice 生成她所要对比的序列$\left(\mathrm{a}_1^{(\mathrm{i})}\mathrm{a}_2^{(\mathrm{i})}\ldots\mathrm{a}_\mathrm{n}^{(\mathrm{i})}\right) \in \{0,1\}^n$并且依据该序列相应时间控制光开关 SW，当$a_\mathrm{j}^{(\mathrm{i})} = 0$时，在$\mathrm{t}_\mathrm{j}^{(\mathrm{i})} + \Delta t_0$控制光关；当$a_\mathrm{j}^{(\mathrm{i})} = 1$时，在$\mathrm{t}_\mathrm{j}^{(\mathrm{i})} + \Delta t_1$控制光开关；

e) Alice 和 Bob 分别记录探测器D_0, D_1, D_2的响应情况，得到三个序列：$\left(a_1^{(\mathrm{i})}a_2^{(\mathrm{i})}\ldots a_\mathrm{n}^{(\mathrm{i})}\right) \in \{0,1\}^n$，$\left(\beta_{01}^{(\mathrm{i})}\beta_{02}^{(\mathrm{i})}\ldots\beta_{0\mathrm{n}}^{(\mathrm{i})}\right) \in \{0,1\}^n$)，$\left(\beta_{11}^{(\mathrm{i})}\beta_{12}^{(\mathrm{i})}\ldots\beta_{1\mathrm{n}}^{(\mathrm{i})}\right) \in \{0,1\}^n$，其中$a_\mathrm{j}^{(\mathrm{i})}, \beta_{0\mathrm{j}}^{(\mathrm{i})}, \beta_{1\mathrm{j}}^{(\mathrm{i})} = 0$表示相应探测器没响应；$a_\mathrm{j}^{(\mathrm{i})}, \beta_{0\mathrm{j}}^{(\mathrm{i})}, \beta_{1\mathrm{j}}^{(\mathrm{i})} = 1$表示相应探测器响应了，注意，只要探测器没有在合适的时间响应即记为“0”，例如，如果 Bob 端探测器没有在时间$\mathrm{t}_\mathrm{j}^{(\mathrm{i})} + \Delta t_2$之前响应，则记为$\beta_{0\mathrm{j}}^{(\mathrm{i})} = \beta_{1\mathrm{j}}^{(\mathrm{i})} = 0$。

2）半反直观 QBC

承诺阶段:

a) Alice 和 Bob 如图 2.2-6 搭建设备，其中分束器 BS 为半透半反镜，协定两个安全参数 m 和 n；

b) Alice 选择一个随机比特$b \in \{0,1\}$作为承诺值，根据承诺值生成 m 串随机序列，每串序列包含 n 比特，表示为$a^{(i)} \equiv \left(a_1^{(\mathrm{i})} a_2^{(\mathrm{i})} \ldots a_{\mathrm{n}}^{(\mathrm{i})}\right) \in \{0,1\}^n, i = 1,2,\ldots.,m$，每个序列满足等式$a_1^{(\mathrm{i})} \oplus a_2^{(\mathrm{i})} \oplus \ldots \oplus a_{\mathrm{n}}^{(\mathrm{i})} = \mathrm{b}$;

c) Bob 也生成 m 穿随机序列，每串序列包含 n 比特，表示为$b^{(i)} \equiv \left(\mathrm{b}_1^{(\mathrm{i})} \mathrm{b}_2^{(\mathrm{i})} \ldots \mathrm{b}_{\mathrm{n}}^{(\mathrm{i})}\right) \in \{0,1\}^n$;

d) Alice 和 Bob 协定一系列时刻点$\mathrm{t}_1^{(\mathrm{i})} \mathrm{t}_2^{(\mathrm{i})} \ldots \mathrm{t}_{\mathrm{n}}^{(\mathrm{i})}$，和时间段$\Delta t_1, \Delta t_2, \Delta t_3$，Bob 在时刻$\mathrm{t}_{\mathrm{j}}^{(\mathrm{i})}$发送相应的量子态$|\psi_{b_j^{(i)}}\rangle$给 Alice，其中$|\psi_0\rangle = |H\rangle, |\psi_1\rangle = |V\rangle$；Alice 根据$a_{\mathrm{j}}^{(\mathrm{i})}$在相应的时间$\mathrm{t}_{\mathrm{j}}^{(\mathrm{i})} + \Delta \mathrm{t}_{aj}^{(\mathrm{i})}$控制光开关;

e) Alice 和 Bob 记录各探测器的是否响应和响应时间，Alice 验证对于每串序列探测器 D2 的响应数量是否约为 n/4，若比例不对，放弃执行协议。

公开阶段:

a) Alice 公开承诺值 b 和 m 个序列$a_1^{(\mathrm{i})} a_2^{(\mathrm{i})} \ldots a_{\mathrm{n}}^{(\mathrm{i})}, i = 1,2,\ldots.,m$;

b) Bob 验证$a_1^{(\mathrm{i})} \oplus a_2^{(\mathrm{i})} \oplus \ldots \oplus a_{\mathrm{n}}^{(\mathrm{i})} = \mathrm{b}$是否成立，验证 Alice 公开的每比特$a_{\mathrm{j}}^{(\mathrm{i})}$是否与他确定知道的值相同，若一致则承认 Alice 的承诺为 b，否则不承认。

3）半反直观量子比特承诺协议的安全性分析

下面将分析半反直观 QBC 协议中可能存在的攻击。由于比对方案和半反直观 QBC 协议都非常简单，可能存在的攻击种类很少。对于 Bob 而言，他可以改变装置或者发送非协议态来进行攻击；而 Alice 有两种攻击，截取攻击和截取/重发攻击。

Bob 的欺骗策略

在半反直观 QBC 协议中，量子态是有由 Bob 发送的，所以 Bob 可以通过发送非协议态和改变装置来攻击协议的隐藏性。 Bob 发送非协议态进行攻击时，他可以发送不同偏振方向的单光子态或者多光子态。当 Bob 发送不同偏振方向的单光子态例如$|+\rangle$或者$|-\rangle$时，这其实只影响了光子通过偏振分束器 PBS 的概率，并不能提高他知道 Alice 比特的概率 p，所以并不是个有效攻击。当 Bob 发送多光子态时，多光子经过协议装置后，到达探测器D_2的数量会多于 n/4，在半反直观 QBC 协议中 Alice 会验证探测器D_2响应的次数，显然发送多光子态会被 Alice 发现。

在 Bob 端装置中，对协议隐藏性有影响的只有分束器。Bob 可以不适用半透半反镜而采用具有其他参数的分束器，假设非协议分束器 BS'的透射率是 t'，这时探测器D_2响应的概率为 t'/2。不同参数的分束器会导致探测器D_2响应的比例不同，这种攻击同样会被 Alice 发现。

Alice 的欺骗策略

截取攻击。当 Alice 进行截取攻击时，概率 q 会变大，这样她有可能在更改承诺值时以更大的概率不被发现。接下来将分析这是否是一个有效攻击。Alice 可以在$t_j^{(i)}+\Delta t_0$和$t_j^{(i)}+\Delta t_1$时均控制光开关 SW，这样探测器D_2响应的数量会变多，以此来提高概率 q。然而，如果 Alice 在所有光子传输时都控制光开关，那么探测器D_2大约会响应 n/2 次，这种比例显然会被 Bob 发现，所以 Alice 应该只选取少量光子截取。

假设 Alice 选择n_0个光子截取，她在$b_j^{(i)}=a_j^{(i)}$和$b_j^{(i)}\neq a_j^{(i)}$两种情况下都截取。当$b_j^{(i)}\neq a_j^{(i)}$时，探测器D_2探测到的光子数为n_0，探测器D_0探测到的光子数为$n-n_0$。当$b_j^{(i)}=a_j^{(i)}$时，探测器D_2探测到的光子数为$n_0+(t_n-n_0)=t_n$；探测器D_1探测到的光子数为rt_n；探测器D_0探测到的光子数为r^2n，因此各个探测器的响应总数如下

$$N(\beta_{0j}^{(i)}=1)=\frac{1}{2}(n-n_0)+\frac{1}{2}r^2n=\frac{5}{8}n-\frac{1}{2}n_0; \tag{2.2.2a}$$

$$N(\beta_{1j}^{(i)}=1)=\frac{1}{2}rtn=\frac{1}{8}n; \tag{2.2.2b}$$

$$N(\alpha_j^{(i)}=1)=\frac{1}{2}n_0+\frac{1}{2}tn=\frac{1}{4}+\frac{1}{2}n_0. \tag{2.2.2c}$$

其中$N\left(\beta_{0j}^{(i)}=1\right)+N\left(\beta_{1j}^{(i)}=1\right)+N(\alpha_j^{(i)}=1)=n$。当$\alpha_j^{(i)}=1$时，Alice 知道 Bob 确认了她的比特，她是最佳策略是在$n-N(\alpha_j^{(i)}=1)$比特范围内更 1 比特，而在$n-N(\alpha_j^{(i)}=1)$比特中只有$N(\beta_{0j}^{(i)}=1)$比特是 Bob 真正不知道的，所以在截取攻击中，Alice 更改 1 比特而不被 Bob 发现的概率是

$$p'(Aalter)=\frac{N(\beta_{0j}^{(i)}=1)}{n-N(\alpha_j^{(i)}=1)}=\frac{5n-4n_0}{6n-4n_0} \tag{2.2.3}$$

即使 Alice 不做截取攻击，她更改 1 比特而不被 Bob 发现的概率是$p(Aalter)=5/6$.可以看出$p'(Aalter)<p(Aalter)$，也就是说会更大概率被 Bob 发现，所以这是个无效攻击。

截取/重发攻击。当 Alice 进行截取攻击时，概率$p(Aalter)$的分子和分母都增大了，所以使得 Alice 的攻击更大概率被 Bob 发现，是无效攻击。接下来分析一个类似的攻击，即截取/重发攻击。Alice 在$t_j^{(i)}+\Delta t_0$和$t_j^{(i)}+\Delta t_1$时均控制光开关 SW，测量完每个光子后，立即发送一个处于同偏振态的光子给 Bob。因为 Alice 截取并重发的所有光子以相同的概率被探测器D_0和D_1探测到，这样会破坏原协议中各探测器探测到个光子比例从而被 Bob 发现。因此，应该只选取少量光子截取/重发。

假设 Alice 选取n'_0个光子截取并重发。她在$b_j^{(i)}=a_j^{(i)}$和$b_j^{(i)}\neq a_j^{(i)}$两种情况下都截取/重发。当$b_j^{(i)}\neq a_j^{(i)}$时，探测器D_2探测到的光子数为n_0'，探测器D_1探测到的光子数为rn'_0，探测器D_0探测到的光子数为$n-n_0'+tn_0'$。当$b_j^{(i)}=a_j^{(i)}$时，探测器D_2探测到的光子数为tn；探测器D_1探测到的光子数为$rtn+rn_0'$；探测器D_0探测到的光子数为r^2n+tn_0'。因此各个探测器的响应总数如下

$$N'(\beta_{0j}^{(i)}=1)=\frac{1}{2}(n-n_0'+tn_0')+\frac{1}{2}(r^2n+tn_0')=\frac{5}{8}n; \tag{2.2.4a}$$

$$N'(\beta_{1j}^{(i)}=1)=\frac{1}{2}rn_0'+\frac{1}{2}(rtn+rn_0')==\frac{1}{8}n+\frac{1}{2}n_0'; \tag{2.2.4b}$$

$$N'(\alpha_j^{(i)}=1)=\frac{1}{2}n_0'+\frac{1}{2}tn=\frac{1}{4}n+\frac{1}{2}n_0'. \tag{2.2.4c}$$

由于 Alice 重发了n_0'个光子，所以各个探测器的响应总数为

$$N'\left(\beta_{0j}^{(i)}=1\right)+N'\left(\beta_{1j}^{(i)}=1\right)+N'\left(\alpha_j^{(i)}=1\right)=n+n_0', \tag{2.2.5}$$

在$N'(\alpha_j^{(i)}=1)$比特中，有n_0'比特是被 Alice 截取重发的，被截取的光子和重发光子是指标相同。对于那些n_0'比特，虽然 Alice 知道其对应的$\mathrm{b}_\mathrm{j}^{(\mathrm{i})}$值，但是不知道是被探测器$D_0$还是$D_1$接收的，所以 Alice 不知道 Bob 对这$n_0'$比特的判断。当 Alice 想要更改承诺值时，她的更改范围实际是$n-[N'(\alpha_j^{(i)}=1)-n_0']$。其中只有$N'(\beta_{0j}^{(i)}=1)$是 Bob 真正不知道的，Alice 更改这些比特不会被发现。所以在截取/重发攻击中，Alice 更改 1 比特而不被 Bob 发现的概率是

$$p''(Aalter)=\frac{N'(\beta_{0j}^{(i)}=1)}{n-[N'(\alpha_j^{(i)}=1)-n_0']}=\frac{5n}{6n+4n_0} \tag{2.2.6}$$

可以看出$p''(Aalter)<p(Aalter)$，也就是说会更大概率被 Bob 发现，所以说这也不是个有效的攻击。

No-go 定理攻击。No-go 定理的攻击模型描述如下，当 Alice 承诺 b 时，她制备

$$|b\rangle=\sum_i \alpha_i^{(b)}\left|e_i^{(b)}\right\rangle_A\otimes\left|\varphi_i^{(b)}\right\rangle_B \tag{2.2.7}$$

其中$\left\langle e_i^{(b)}\middle|e_j^{(b)}\right\rangle_A=\delta_{ij}$，$\left|\varphi_i^{(b)}\right\rangle_B$不一定是相互正交的。Alice 发送第二个量子寄存器给 Bob 作为一部分证据。为了保证 QBC 协议的隐藏性，其约化密度矩阵要相等或近似，即

$$Tr_A|0\rangle\langle 0|\equiv\rho_0^B\simeq\rho_1^B\equiv Tr_A|1\rangle\langle 1|. \tag{2.2.8}$$

当上式成立时，由 Schmidt 分解可知，Alice 可以利用一个本地酉变换将$|0\rangle$更改为$|1\rangle$且不被发现。

在半反直观 QBC 协议中，量子态是由 Bob 制备的，Alice 没有初始量子态。如果 Alice 想要利用 no-go 定理进行攻击，她需要在收到 Bob 发送的量子态后做一个受控酉变换，使得受控量子位和接收量子位纠缠。也就是说，当 Alice 承诺“0”时，整个系统的量子态是

$$|0\rangle=\frac{1}{2^{n-1}}\sum_{\alpha_1^{(i)}\oplus\ldots\oplus\alpha_n^{(i)}=0}\left|\alpha_1^{(i)}\ldots\alpha_n^{(i)}\right\rangle_A U_B\left(\alpha_1^{(i)}\ldots\alpha_n^{(i)}\right)\overset{j=1}{\overset{n}{\otimes}}\left|\psi_{b_j^{(i)}}\right\rangle_B.$$

$$=\frac{1}{2^{n-1}}\sum_{\alpha_1^{(i)}\oplus\ldots\oplus\alpha_n^{(i)}=0}\left|\alpha_1^{(i)}\ldots\alpha_n^{(i)}\right\rangle_A\left[U_B\left(\alpha_1^{(i)}\right)\left|\psi_{b_1^{(i)}}\right\rangle_B\otimes\ldots\otimes\left[U_B(\alpha_n^{(i)})\left|\psi_{b_n^{(i)}}\right\rangle_B\right]\right.$$

$$=\frac{1}{2^{n-1}}\sum_{\alpha_1^{(i)}\oplus\ldots\oplus\alpha_n^{(i)}=0}\left|\alpha_1^{(i)}\ldots\alpha_n^{(i)}\right\rangle_A\left|\psi'_{b_1^{(i)}}\right\rangle_B\otimes\ldots\otimes\left|\psi'_{b_1^{(i)}}\right\rangle_B$$

同理，当 Alice 承诺“1”时，整个系统的量子态是

$$|1\rangle = \frac{1}{2^{n-1}}\sum_{\alpha_1^{(i)}\oplus\ldots\oplus\alpha_n^{(i)}=1}\left|\alpha_1^{(i)}\ldots\alpha_n^{(i)}\right\rangle_A\left|\psi'_{b_1^{(i)}}\right\rangle_B\otimes\ldots\otimes\left|\psi'_{b_1^{(i)}}\right\rangle_B. \quad (2.2.9)$$

由于需要满足 QBC 协议的隐藏性，Alice 可以做一个本地酉变换将$|0\rangle$变为$|1\rangle$。然而有以下两个原因限制了这种攻击很难进行：

1) Alice 根据她的经典比特值在不同的时间点控制光开关 SW。这里 SW 是一个宏观的器件，Alice 的操作不能当做$\left|a_j^i\right\rangle_A$或者其他量子态，而是否存在纯量子的光开关以及微观粒子能够与宏观器件相纠缠一直是一个有争议的问题。所以系统的状态不是上式所表示的形式；

2) 假设存在纯微观的光开关，Alice 可以利用受控酉变换将自己的量子寄存器与 Bob 手中的量子比特做纠缠，no-go 定理攻击仍无法实现，原因是从光的粒子性来看反直观类的协议，有一半的粒子并未通过信道传送到 Alice 端，而是一直在 Bob 端，Alice 无法对 n 个量子态均做受控酉变换，从光的波动性来分析反直观类协议，光子由 a 和 b 两个模式以一定的几率幅构成，处于 b 模式下的光波通过信道传送到 Alice 端，但这只是部分而非全部， Alice 仍得不到处于 a 模式的部分光，她只能做到将自己的量子寄存器与 b 模式下的光相纠缠，而执行 no-go 定理攻击的前提是 Alice 承诺相关的全部比特和 Bob 手中的全部量子比特相纠缠，无论是从光的粒子性还是波动性来看，Alice 都无法执行这一攻击。

安全参数

分析了 Alice 的截取攻击以及截取/重发攻击都是无效攻击，而 Alice 直接在每个序列中更改 1 比特不被发现的概率为

$$p(Aalter) = \frac{1-p}{1-q} = \frac{5}{6} \quad (2.2.10)$$

所以在半反直观 QBC 协议中，Alice 更改其承诺值而不被发现的概率为$p(Aalter)^m$。如果限制攻击成功的概率为 10^{-6} 量级，我们发现当 m = 70 时，Alice 攻击绑定性成功的概率约为 2.8×10^{-6}。

在半反直观 QBC 协议中 Alice 会验证D_2探测到的光子数量，使得 Bob 无法发送非协议态或者使用非协议装置。而 Bob 猜对 Alice 比特$a_j^{(i)}$的概率为

p'= 7/8，因此 Bob 破坏协议隐藏性成功的优势是

$$\left|p(Bknows) - \frac{1}{2}\right| = \frac{1}{2} - \frac{(1-P_B^n)^m}{2} \quad (2.2.11)$$

当 m = 70，n = 130 时，Bob 破坏隐藏性的优势约为 1.0×10^{-6}。

如果限制协议双方攻击成功的概率在 10^{-6} 量级，那么 m = 70，n = 130 是对合适的安全参数。协议的安全参数可以根据具体的安全需求进行设置。

2.2.3 总结

通过对量子密码协议的进展进行调研，在未来的学习研究中，可尝试构造实用化的量子不经意传输协议和量子比特承诺协议，寻找超越 no-go 定理的无条件安全的量子比特承诺协议；对现有可信中继量子密钥分配系统进行安全性分析，提出更安全、简单的改进方案，构造可实用化的量子网络。

参考文献

[1] Wiesner S. Conjugate coding[J]. AcmSigact News, 1983, 15(1):78-88.

[2] Bennett, C., Brassard, G. Quantum cryptography: Public key distribution and coin tossing[C]. International Conference on Computers, Systems & Signal Processing, Bangalore, India. 1984.

[3] Mayers D. Quantum Key Distribution and String Oblivious Transfer in Noisy Channels[C]Advances in Cryptology: Proceedings of Crypto ’96. Berlin: Spriger Verlag, 1996:343—357.

[4] Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances[J]. Science, 1999,283(5410): 2050–2056.

[5] Shor P W, Preskill J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol[J]. Physical Review Letters, 2000, 85:441–444.

[6] RENATO RENNER. SECURITY OF QUANTUM KEY DISTRIBUTION[J]. International Journal of Quantum Information, 2011, 6(1):1-127.

[7] Brassard G, Lütkenhaus, Mor T, et al. Limitations on practical quantum cryptography[J]. Physical Reveiw Letters, 2000, 85:1330–1333.

[8] Dušek M, Haderka O, Hendrych M. Generalized beam-splitting attack in quantum cryptography with dim coherent states[J]. Optics communications, 1999, 169(1-6): 103-108.

[9] Liu W T, Sun S H, Liang L M, et al. Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution[J]. Physical Reveiw A, 2011, 83:042326.

[10] Hwang W Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication[J]. Physical Reveiw Letters, 2003, 91:057901.

[11] Wang X B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography[J]. Physical Reveiw Letters, 2005, 94:230503.

[12] Ma X F, Qi B, Zhao Y, et al. Practical decoy state for quantum key distribution[J]. Physical Review A, 2005, 72:012326.

[13] Cai Q Y, Tan Y G. Photon-number-resolving decoy-state quantum key distsribution[J]. Physical Reveiw A, 2006, 73:032305.

[14] Zhao Y, Qi B, Ma X F, et al. Experimental Quantum Key Distribution with Decoy States[J]. Physical Review Letters, 2006, 96:070502.

[15] Peng C Z, Zhang J, Yang D, et al. Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding[J]. Physical Reveiw Letters, 2007, 98:010505.

[16] Rosenberg D, Harrington J W, Rice P R, et al. Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber[J]. Physical Review Letters, 2007, 98:010503.

[17] Dixon A R, Yuan Z L, Dynes J F, et al. Gigahertz decoy quantum key distribution with 1Mbit/s secure key rate[J]. Optics Express, 2008, 16(23):18790–18979.

[18] Nauerth S, Fürst M, Schmitt-Manderbach T, et al. Information leakage via side channels in freespace BB84 quantum cryptography[J]. New Jouranl of Physics, 2009, 11:065001.

[19] Fung C H F, Qi B, Tamaki K, et al. Phase-remapping attack in practical quantum key distribution systems[J]. Physical Review A, 2007, 75:032314.

[20] Xu F H, Qi B, Lo H K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system[J]. New Journal of Physics, 2010, 12:113026.

[21] Li Yang, Bing Zhu. Dissipation attack on Bennett-Brassard 1984 protocol in practical quantum key distribution system. arXiv: 1305.5744, 2013.

[22] Li H W, Wang S, Huang J Z, et al. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources[J]. Physical Reveiw A, 2011, 84:062308.

[23] Huang J Z, Yin Z Q, Wang S, et al. Wavelength attack scheme on continuous variable quantum key distribution system using heterodyne protocol[J]. arXiv: quantum-ph/1206.6550, 2012.

[24] Makarov V, Anisimov A, Skaar J. Effects of detector efficiency mismatch on security of quantum cryptography[J]. Physical Review A, 2006, 74:022313.

[25] Makarov V, Skaar J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols [J]. Quantum Information and Computation, 2008, 8(6):0622—0635.

[26] Zhao Y, Fuang C H F, Qi B, et al. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems[J]. Physical Review A, 2008, 78:042333.

[27] Makarov V. Controlling passively quenched single photon detectors by bright light[J]. New Journal of Physics, 2009, 11:065003.

[28] Wiechers C, Lydersen L, Wittmann C, et al. After-gate attack on a quantum cryptosystem[J]. arXiv: quant-ph/1009.2683, 2010.

[29] Makarov V, Anisimov A, Sauge S. Quantum hacking: adding a commercial actively-quenched module to the list of single-photon detectors controllable by Eve[J]. arXiv:quant-ph/0809.3408, 2009.

[30] Lydersen L, Wiechers C, Wittmann C, et al. Hacking commercial quantum cryptography systems by tailored bright illumination[J]. Nature Photonics, 2010, 4:686.

[31] Cr*é*peau C. Equivalence Between Two Flavours of Oblivious Transfers[M]// Advances in Cryptology — CRYPTO ’87. Springer Berlin Heidelberg, 1987:350-354.

[32] Crépeau C, Kilian J. Achieving oblivious transfer using weakened security assumptions[C]// Foundations of Computer Science, 1988. Symposium on. IEEE, 1988:42 - 52.

[33] Brassard G, Crépeau C. Quantum bit commitment and coin tossing protocols[C]//Conference on the Theory and Application of Cryptography. Springer Berlin Heidelberg, 1990: 49-61.

[34] Bennett C H, Brassard G, Crépeau C, et al. Practical Quantum Oblivious Transfer[M]// Advances in Cryptology — CRYPTO '91. Springer Berlin Heidelberg, 1992:351-366.

[35] Brassard G, Crepeau C, Jozsa R, et al. A quantum bit commitment scheme provably unbreakable by both parties[C]// Symposium on Foundations of Computer Science. IEEE, 1993:362-371.

[36] A. C.-C. Yao, in Proceedings of the twenty-seventh annual ACM symposium on Theory of computing (ACM, Las Vegas, Nevada, USA, 1995), pp. 67

[37] D. Mayers. The Trouble with Quantum Bit Commitment, arXiv:quant-ph/9603015.1996.

[38] Mayers D. Unconditionally Secure Quantum Bit Commitment is Impossible[J]. Physical Review Letters, 1997, 78(17):3414.

[39] Lo H K, Chau H F. Is Quantum Bit Commitment Really Possible?[J]. Physical Review Letters, 1997, 78(17):3410-3413.

[40] G. Brassard et al. A brief review on the impossibility of quantum bit commitment. arXiv:quant-ph/9712023, 1997.

[41] Paul Dumais, Dominic Mayers, Louis Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. Advances in Cryptology—EUROCRYPT 2000. Springer Berlin Heidelberg (2000):300-315.

[42] Li Yang (CA), Chong Xiang, Bao Li. Qubit-string-based bit commitment protocols with physical security. arxiv:1011.5099v3(2010).

[43] Lu X, Ma Z, Feng D G. A Computationally Secure Quantum Oblivious Transfer Scheme[C]// Advanced Communication Technology, 2006. Icact 2006. the, International Conference. 1996:1547-1551.

[44] He G P, Wang Z D. Oblivious transfer using quantum entanglement[J]. Physical Review A, 2006, 73(1): 012331.

[45] Namiki R, Hirano T. Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection[J]. Physical Review A, 2006, 74(3): 032302.

[46] Chen I C, Hwang T, Li C M. Efficient one-out-of-two quantum oblivious transfer based on four-coherent-state postselection protocol[J]. Physica Scripta, 2008, 78(3): 035005.

[47] Rührmair U. Oblivious transfer based on physical unclonable functions[C]//International Conference on Trust and Trustworthy Computing. Springer Berlin Heidelberg, 2010: 430-440.

[48] L. Yang, Bit commitment protocol based on random oblivious transfer via quantum channel. arXiv: 1306.5863, 2013.

[49] Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. Proceedings of the thirty-third annual ACM symposium on Theory of computing. ACM(2001): 134-142.

[50] G. Molina-Terriza, et al. Experimental quantum coin tossing. Physical review letters 94.4 (2005): 040501.

[51] David Fattal, et al. Experimental realization of quantum oblivious transfer. Quantum Electronics and Laser Science Conference. Optical Society of America (2008): QFB4.

[52] Nelly Huei Ying Ng, et al. Experimental implementation of bit commitment in the noisy-storage model. Nature communications 3 (2012): 1326.

[53] Adrian Kent. Unconditionally secure bit commitment by transmitting measurement outcomes. Physical review letters 109.13 (2012): 130501.

[54] Tommaso Lunghi, et al. Experimental bit commitment based on quantum communication and special relativity. Physical review letters 111.18 (2013): 180504.

[55] Yang Liu, et al. Experimental unconditionally secure bit commitment. Physical review letters 112.1 (2014): 010504.

§2.3 选举协议

公平的选举是现代社会的基本需求之一。传统的纸质选举方式常常要求选民在指定的时间到指定的地点投票，并通过人工的方式对选票进行统计。这种方式容易受到人为环境的影响，已经逐渐满足不了人们的需求。随着信息时代的到来，越来越多的日常事务通过数字通信网络来处理，传统的选举方式逐渐被基于网络的电子选举所代替。有关电子选举的研究始于上个世纪 80 年代，当时一些日本学者先后发表了关于电子选举的应用方案。最早的使用密码学来保证选举私密性的协议是由 Chaum 在 1981 年提出的[1]，它使人们能够通过不安全的网络环境进行匿名投票，但这并不能保证选民的身份无法被追踪。但之后一直进展不大，直到密码学突破军事应用的限制，在各个领域得到广泛的应用以及密码学研究本身的飞速发展，如盲签名方案的蓬勃发展，电子选举才有了可喜的进展。

2.3.1 传统电子选举方案

1981 年，Chaum 提出的第一个密码学意义上的选举协议是基于 Mix-net，实现使用 RSA 公钥体制，加密消息的长度和用户计算量 Mix net Server 的个数成正比，其使用基于 RSA 困难问题安全假设的公钥算法来隐藏参与者身份，达到了基于 RSA 困难问题安全假设的计算安全性。1983 年，Chaum 基于 RSA 公钥密码系统，提出基于因子分解问题的盲签名方案[2]。1985 年，J.cohen 和 M.Fischer 在 IEEE 第 26 届计算机科学基础年会上提出一个集中式的电子选举方案[3]。其采用盲签名及 Mix-net 扰乱消息来实现匿名投票，但不满足投票的隐私性。1986 年，J.Benaloh 和 M.Yung 将集中权利进行分布式处理，并将分布式计算与密码技术相结合[4]，保证了对单个选民的隐私保护，但选举机构仍然掌握所有投票人的信息。1987 年，J.Benaloh 基于 Shamir 的秘密共享和高次剩余问题的同态概率公钥加密[5]，给出可验证性的秘密投票方案。1992 年，A.Fujioka、T.Okatnoto 和 K.Ohta 利用盲签名对选民身份进行匿名发送选票[6]，其选民身份的匿名安全性基于 RSA 的计算安全性。1997 年，R.Cramer、R.Gennaro 和 B.Schnoeranakers 利用门限同态加密、公告板和零知识证明等方法提出一个选

举方案[7]，其安全性是基于 ElGamal 的计算安全性。2000 年，姚亦峰等提出了利用二元仿射变换，以 Harn 和 Xu 提出的 18 种安全广义 ElGamal 型数字签名方案为基础，构造出 18 种相应的盲签名方案，基于此构造相应的电子选举协议。同时期，各种基于密码学的电子选举协议相继被提出，目前传统的选举协议主要有以下三种：

（1）基于同态的选举协议。在这些协议中，设明文空间为（运算符为o），密文空间为（运算符为o），一组同态加密方案为$\{E_i\}_{i\in N^+}$，其中$E_i: V \to C$（$v \to c = E_i(v)$）。同态性质可以如下定义：设$c_j = E_{i_j}(v_j)$，其中$j, i_j, k, i_k \in N^+$；那么，$\exists i \in N^+$，满足:$c_j o c_k = E_i(v_j o v_k)$。这一特性允许记票者在未对每个选票进行逐一解密的情况下实现选举结果的统计。由于这些选举协议的安全性是基于 RSA、ElGamal 等公钥密码体制的，因此这些选举协议不满足后量子安全性。

（2）基于 Mix-net 的选举协议。1981 年，Chaum 提出了第一个基于 Mix-net 的匿名选举协议，其使用基于 RSA 困难问题安全假设的公钥算法来隐藏参与者身份。基于 Mix-net 的选举协议的主要思想是基于所谓的“Dinning Cryptographers Problem” 问题。假设选举者两两之间共享了一个随机数$|C_{jk}|$，其中$C_{jk} = -C_{kj}$。每个选民 k 选择$v_k = 0$或者$v_k = 1$来表示选票的支持与反对，然后公布$S_k = v_k + \sum_{j\neg k} C_{jk}\ (mod 2)$。由于$C_{jk} = -C_{kj}$，因此$\sum_k S_k = \sum_k v_k$。这样每个人都可以通过计算$\sum_k S_k$来确定选票中“支持”的个数、虽然这类协议中选民的身份是匿名的，但是它不能防止恶意选民的重复投票，不能达到选举协议要求的不可重复性。也有一些被提出的基于 Mix-net 的选举协议能够防止重复投票，但它们都是基于的计算安全性的困难问题。

（3）基于盲签名的选举协议。这种协议最早也是有 Chaum 提出，被应用于匿名选举以及支付方案中。其协议基本内容为签字者对某一个盲化后的消息进行签名，接受者对签名进行处理恢复签字者对原始消息的签名，签名者不能由公布的签名对原始消息进行追踪。由于在协议中使用到的签名算法依然是依赖于难解的数学问题，如 RSA，ElGamal 等，因此它们也无法满足后量子安全性。

同时满足安全性和私密性是许多选举协议面临的最大的障碍。以上提到的选举协议中，多数是依赖于一个难解的数学难题假设，虽然能够满足选举协议要求的各种性质，但是只能满足现有计算机数学计算上的安全性和私密性（如使用基于公钥密码体制的同态加密技术、盲签名技术的选举协议，以 Fujioka 等人提出的 FOO 协议[8]为代表）；有的能够达到选民身份的无条件私密性和选举协议的无条件安全性，但是却满足不了选举协议的不可重复性[9]，如何在最大可能满足选举的各种性质的前提下，构造信息论安全的适用于大规模选举的选举协议成为一个新的问题。

2.3.2 量子选举方案

量子密码学开启了一种应用于选举系统的新方法。和经典的密码学不同，量子密码学的安全性是由量子力学的特性来保证的[10]，使用量子系统能够完成无条件安全的经典信息传输[11]。近年来，越来越多的人将目光投入到量子选举系统上。按照是否利用了纠缠特性，量子选举协议分为以下两大部分:

第一部分：使用量子纠缠的选举协议

2005 年， Vaccaro 等人提出了一种量子选举方案[12]。在他们的方案中，每个选民通过对代表选票的量子态进行不同的局域操作来表示自己的选票内容，如果选民的选则是“Yes”，那么选民对量子态进行某个事先约定的幺正操作；如果选民的选择是“No”，那么他不对量子态进行任何操作。做完这些后该选民将量子态传给下一个选民。最终所有选民的选择被编码成为同一个纠缠态的相位信息。读取选举的结果需要进行一次复杂的测量过程，统计者能够根据测量结果得出选民所选的“Yes”的个数，但是无法得知选民的身份信息，有效地保证了选举的匿名性。

另一个类似的协议是由 Hillery 等人提出的[13]，同样是使用量子态来记录选票的信息，通过量子测量来读取选举的结果。在协议中作者利用了纠缠粒子的特性，制备一对纠缠粒子，用其中的一个作为量子选票在选民之间传输，另一个保存在计数者手里。当作为量子选票的粒子传递到某个选民手中时，该选民通过是否进行某一个特定的操作来表示自己的选票内容。在选举的最后，该粒子被传递到计数者手中，通过对纠缠粒子进行测量来得到选择“Yes”的选民个数。这个协议对参与者的诚信度要求很高，要求所有的参与者均是诚实的，一旦某个选民私自对量子选票进行了测量，将破坏整个选举过程。同时，协议发现不了重复投票的行为。

上面的两种方案是量子选举的比较显著的进展，都是利用量子态的传递来完成选举，也都需要在最后进行复杂的量子测量。2006 年，Dolev 等人提出了一种不需要进行复杂的量子测量的量子选举协议[14]。在他们的方案中，选举结果可以直接由基态读取，而不需要进行复杂的测量。这个协议是基于傅里叶变换的，一旦傅里叶变换能够有效实施，这个协议就可以顺利实现；另一方面，协议同样对参与者的诚信度要求过高，发现不了选民的重复投票问题，一旦某些选民有重复投票等作弊行为，就可能破坏整个选举过程。

2009 年，易智等人提出了一种基于双模压缩态的量子投票协议[15]，该协议通过随机选择信号加载的方式，充分利用量子信号测不定性原理实现了分布式投票系统，并分析了可能遇到的攻击。双模压缩态的模间关联性保证了该方案的安全性。林崧等人也提出了一种基于单粒子的量子选举方案[16]。投票者利用局域幺正操作进行投票，计票员可根据测量的结果计算出投票的结果。通过对方案的正确性和秘密性进行分析，表明该方案是安全的。而且，与采用 N 维量子纠缠态的量子投票方案相比，该方案只涉及二维量子态，测量较为简单。需要注意的是，虽然文章的协议中只是使用了二维纠缠态，但是选举时需要选民对每个候选人分别进行投票，相当于进行了多次的二选一投票。

同样是 2009 年，Horoshko 等人提出了一种新的匿名量子选举方案[17]，与之前的方案相比，他们的方案有了新的进展。文章同时考虑到了来自计数者和选民的安全威胁，所提出的方案可以保证选民身份的无条件安全性。协议的重点是选票经过选举过程之后会重新返回到选民手中，选民可以自主决定进行投票或者检测协议的匿名性。如果选民选择投票，则他按照自己的选举意图 yes/no 制备对应的量子态$|0rangle$，$|1\rangle$；如果选民选择检测协议的匿名性，则和另一个选择检测协议匿名性的选民共同制备一个贝尔态。所有的选民都将自己的粒子连同身份标识一起发给计数者，计数者通过一个特殊的量子测量来确定所有纠缠态中$|1\rangle$的个数，然后把粒子返回给选民。如果计数者悄悄地对粒子进行单独测量，则会改变粒子的状态，从而被选民发现。由于每个选民都自主地选择进行投票或者检测匿名性，计数者即使测量了单个粒子也无法确定选民究竟做了哪种选择，从而无法确定选民的选举意图。

2011 年，Bonanome 等人在他们的文章[18]中介绍了一些使用量子力学的特性来保证私密性的量子选举方案，方案的重点在于使用纠缠量子态来保证私密性，并将之前提到的一些方法应用到了保护选举的私密性上。此外，他们还分析了对一些攻击的抵抗性，尤其是来自于不诚实的选民和非法窃听者的攻击。2011 年，温小军等人介绍了了一种使用 GHZ 态光子的纠缠特性来实现无条件安全性的量子投票模型[19]。协议中引入了“监票人”的定义，用来监督验票人（即选票统计者）的行为，改之前的事后审计为即时监督。

第二部分：不使用量子纠缠的选举协议

2008 年， Okamoto 提出了一种不使用量子纠缠的量子选举协议[20]。协议包含了多个候选人。对于每个选民，选举管理系统制备一个未知量子态作为其空白选票，由于无法对未知量子态进行复制，因此他人无法伪造合法的空白选票。选举时，选民首先对选票加一个随机因子，然后根据自己所选的候选人生成自己的选票。文章同时讨论了协议可能面对的不安全因素。这个协议需要在一个半诚实的模式下进行，且提出了一种分布式协议来防止选举管理员伪造选票，但是由于在选举最后只是公布了一个最后的选举结果，协议的可验证性无法得到满足，选民无法确定自己是否投票成功，也无法对自己的选票进行追踪。

2012 年，周瑞瑞和杨理提出了一种不使用量子纠缠的量子选举协议[21]，协议包含了多个候选人，单个管理者和单个计票员。协议基于共轭编码的原理实现了选举协议满足的 7 条性质。但其模式为半诚实模式。其中文章指出单个管理者的情况和半诚实的模式限制了实际使用的范围，同时该协议还需要指定管理者和计票员不会合谋攻击。

2013 年，周瑞瑞和杨理还提出一种基于分布式系统和共轭编码的量子选举协议[22]。协议包含了多个选举人，多个管理者，单个计票员。协议采用了分布式的思想，多个管理者分布式帮助选举人与计票员之间匿名地建立选举密钥，满足了选举协议的 7 条性质。但在其选举之前，需要无条件安全的密钥预处理过程。

2016 年，Rishi Dutt Sharma 和 Asok De 提出一种只使用单一量子位的新型量子投票方案[23]。具体来说，该协议是通过修改一个基于量子位的控制位设计了一套安全量子通信的方案。在文章中，其作者分析了在一些特定的攻击中的协议安全性。而且，单一量子位的设计影响小于多量子位的量子选举的设计方案。

言而总之，量子密码学开启应用于选举方案的新方法。可以基于相关的量子力学的特性和密码学的基本原语，构造更实用更安全的选举协议。

参考文献

[1] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2):84–90, 1981.

[2] Chaum D. Blind signature, system[J]. Crypto, 1983:153-158.

[3] J.D. Cohen and M.J. Fischer. A robust and verifiable cryptographically secure election scheme. Yale University, Department of Computer Science, 1985.

[4] Benaloh J C, Yung M. Distributing the power of a government to enhance the privacy of voters[C]// Podc86: Principles of Distributed Computing Symposium. 1986:52-62.

[5] Benaloh, Josh Daniel Cohen. Verifiable secret-ballot elections, 1987.

[6] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. In Advances in CryptologyAUSCRYPT'92, pages 244–251. Springer, 1993.

[7] Cramer R, Gennaro R, Schoenmakers B. A Secure and Optimally Efficient Multi-Authority Election Scheme[C]// International Conference on Theory and Application of Cryptographic Techniques. Springer-Verlag, 1997:103-118.

[8] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. In Advances in CryptologyAUSCRYPT'92, pages 244–251. Springer, 1993.

[9] Hong. Zhong, Liu Sheng. Huang, and Yong Long. Luo. A multi-candidate electronic voting scheme based on secure sum protocol. Journal of Computer Research and Development, 43(8):1405–1410, 2006.

[10] Nicolas. Gisin, Gr′egoire. Ribordy, Wolfgang. Tittel, and Hugo. Zbinden. Quantum cryptography. Rev. Mod. Phys., 74:145–195, Mar 2002

[11] Hitoshi Inamori, Norbert L¨utkenhaus, and Dominic Mayers. Unconditional security of practical quantum key distribution. The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics, 41(3):599–627, 2007.

[12] J. A. Vaccaro, Joseph. Spring, and Anthony. Chefles. Quantum protocols for anonymous voting and surveying. Phys. Rev. A, 75:012333, Jan 2007.

[13] M. Hillery, M. Ziman, V. Buzek, and M. Bielikov′a. Towards quantum-based privacy and voting. Physics Letters A, 349(1-4):75–81, 2006.

[14] S. Dolev, I. Pitowsky, and B. Tamir. A quantum secret ballot. Arxiv preprint quant-ph/0602087, 2006.

[15] Zhi. Yi, GuangQiang. He, and Gui Hua. Zeng. Quantum voting protocol using two-mode squeezed states. Acta PhysicaSinica, 58(5):3166–3172, 2009.

[16] Song. Lin and ZhiQiang. Yao. Quantum voting scheme based on qubits. Journal of PutianUnievrsity, 16(5):47–51, 2009.

[17] D. Horoshko and S. Kilin. Quantum anonymous voting with anonymity check. Physics Letters A, 2011.

[18] M. Bonanome, V. Bu˘zek, M. Hillery, and M. Ziman. Toward protocols for quantum-ensured privacy and secure voting. Phys. Rev. A, 84:022331, Aug2011.

[19] Xiao Jun. Wen and Xue Jun. Cai. Secure quantum voting protocol. Journal of Shandong University, 46(9), 2011.

[20] Tatsuaki. Okamoto, Koutarou. Suzuki, and Yuuki. Tokunaga. Quantum voting scheme based on conjugate coding. NTT Technical Review, 6, 2008.

[21] R.R.Zhou,L.Yang. Quantum election scheme based on anonymous quantum key distribution. Chinese Physics B, 2012, 21(8):23-30.

[22] R.R.Zhou. L.Yang, Distributed quantum election scheme. arXiv:1304.0555, 2013.[quant-ph].

[23] Sharma R D, De A. Quantum Voting using Single Qubits[J]. Indian Journal of Science & Technology, 2016, 9(42).

§2.4 网络安全协议(Internet Protocol Secturity, IPSEC)

国际标准化组织将计算机通信分为七层：应用层，表示层，会话层，传输层，网络层，数据链路层，物理层。由于网络环境的复杂性，数据在计算机通信中传输面临着安全威胁，可能会遭遇网络敌手的攻击，面临数据泄露和数据被篡改等风险。为了保证数据的安全传输，需采用安全协议对各层数据进行保护。数据在这七层的安全性是''或''的关系，即只要其中一层是安全的，则数据在计算机网络中的传输即为安全的。保护网络层即 IP 层的安全协议称为 IPSEC(IP Security)，其安全机制对其上层的应用服务提供透明安全服务，保护 TCP/IP 通信即计算机网络通信免遭窃听和篡改，保证数据的完整性和机密性，有效抵御网络攻击，同时保持易用性。目前的 IPSEC 协议标准基于公钥基础设施 PKI，利用公钥加密、签名、对称加密和哈希算法等密码学原语来保证协议的安全性。然而，多数公钥算法均依赖于大整数分解和离散对数问题的困难性。Shor 算法等一系列量子算法的提出和量子计算机的发展使得此类公钥算法的安全性面临威胁，进而 IPSEC 协议的安全性也面临着威胁。因此，研究具有量子安全性的 IPSEC 协议即量子 IPSEC 对整个计算机网络具有重要意义。

2.4.1 经典 IPSEC

IPSEC 作为网络层协议，具有以下四个作用：作为一个隧道协议实现 VPN(虚拟专用网)通信、保证数据来源可靠、保证数据完整性、保证数据机密性。IPSEC 协议是一个协议族，包括两个安全协议，即 ESP 协议和 AH 协议。AH 协议保护数据的完整性、数据来源的可靠性，但不对数据的机密性进行保护，而 ESP 协议对数据的机密性进行保护，也可以对数据进行认证。而 IPSEC 协议即 ESP 和 AH 协议的实行需要密钥交换协议即 IKE 协议的支撑。IKE 协议为 IPSEC 协议的实行协商安全联盟 SA，用户的所有安全联盟 SA 组成了安全联盟数据库 SAD。

SA 是两个 IPSEC 通信实体之间经过协商建立起来的一种协定，内容包括采用何种 IPSec 协议(AH 还是 ESP)、运行模式(传输模式还是隧道模式)、验证算法、加密算法、密钥、密钥生存期、计数器等，从而决定保护什么、如何保护以及谁来保护，SA 是构成 IPSec 的基础，SA 是单向的，进入(inbound)SA 负责处理接收到的数据包，外出(outbound)SA 负责处理要发送的数据包，每个通信方必须有一个进入 SA 和一个外出 SA。这两个 SA 构成了一个 SA 束(SA Bundle)。通信双方在 SA 协商完毕后，都在它们各自的安全关联数据库(SAD)中存储该 SA 参数，SA 由一个三元组安全参数索引 SPI、一个用于输出处理的目的 IP 地址(或用于输入处理的源 IP 地址)和协议(如 AH 或 ESP)唯一地标识，其中 SPI 是为了唯一标识 SA 而生成的一个 32 位整数。有了 SPI，相同源、目的节点的数据流可以建立多个 SA。SAD 是将所有的 SA 以某种数据结构集中存储的一个列表。对于外出的流量，如果需要 IPSEC 来处理但相应的 SA 不存在，IPSEC 将启动 IKE 来协商出一个 SA，并存到 SAD 中。对于进入的流量，如果需要 IPSEC 来处理，IPSEC 从 IP 包中得到三元组，并利用这个三元组在 SAD 中查找一个 SA。SAD 中每个 SA 除了包含上面介绍的三元组外，还包含：本方序列号计数器、对方序列号溢出、抗重放窗口、AH 的验证算法和所需密钥、ESP 的验证算法和所需密钥(可为空)、ESP 加密算法、密钥、初始向量(IV)、IPSEC 运行模式、路径最大传输单元和 TTL 变

量、SA 生存期(可以用时间，也可以用传输的字节数衡量，或同时使用，优先采用先到者，过期后建立一个新的 SA 或终止通信)。

对于 IPSEC 数据流处理而言，除了 SAD 数据库外，还有一个必要的数据库，即安全策略数据库 SPD，SPD 指定了用于到达或者源自特定主机或者网络的数据流的策略，SAD 和 SPD 之间是通过 SAID 进行关联的，通过查看 SPD 中的 SAID 值，可对 SAD 进行查找，找到该策略项所应该实施的 SA。IPSec 运行模式包括传输模式和隧道模式：传输模式(Transport Mode)保护的是 IP 包的载荷，传输模式为上层协议提供保护，通常情况下只用于两台主机之间的通信；隧道模式保护的是整个原始的 IP 包，通常情况下，只要 IPSec 双方有一方是安全网关或路由器，就必须使用隧道模式。

经典 IPSEC 中 SA 的管理包括创建和删除，可以有两种管理方式，第一种是手动管理，即通过预共享密钥(PSK)来实现认证，这种管理方式不适合比较复杂的网络环境，面临着密钥删除和更新等一系列问题；第二种管理方式是利用 IKE 协议自动管理，这种管理方式的认证是通过公钥基础设施 PKI。IKE 协议为 IPSEC 提供密钥交换与管理、通信对等体的认证、IPSec SA 的协商与管理三大服务。IKE 包括两个阶段，阶段一协商的 SA 可以称为 ISAKMP SA，该 SA 为双方第二阶段的通信提供机密性、数据完整性以及数据源认证服务。阶段二协商的 SA 是密钥交换协议最终要交换的 SA，称为 IPSec SA，保证 AH 或者 ESP 的安全通信。阶段二的安全由阶段一协商结果来保证。阶段一协商的一个 SA 可以用于协商多个阶段二的 SA。第一阶段的密钥协商成为主模式阶段，第二阶段的 IPSEC SA 的协商称为快速模式阶段。

2.4.2 量子 IPSEC

为了抵抗量子计算机给计算机通信带来的威胁，可以考虑构造具有后量子安全性的量子 IPSEC 体系，一些简单的方法如下：

IKE 协议第一阶段引入 QKD 协议：由上面的介绍可知 IPSEC 协议中，SA 的安全性是协议安全的基础。即 IKE 协议中，通信双方协商 SA 的阶段是 IPSEC 协议里非常重要的阶段，因为 SA 内容的机密性和可认证性是整个 IPSEC 协议的基础。在 SA 的两种管理方式中，手动管理方式面临密钥更新的问题，而 IKE 自动管理方式因为在主模式阶段使用 PKI 公钥基础设施来实现认证和加密，其公钥算法可能无法抵抗具有量子能力的敌手。在 IKE 协议的快速模式中，通信双方的通信是基于对称加密，认证过程是利用主模式所生成的共享密钥，已有研究认为对称算法中 AES 128 已足够抵抗量子计算机的攻击。因此，快速模式过程能够抵抗量子敌手的攻击。基于以上考虑，通过在 IKE 主模式即第一阶段中引入量子密钥分配(QKD)协议来解决上面的问题。在 IKE 第一阶段引入 QKD 具有以下优势：一、由于 QKD 具有无条件安全性，则在第一阶段通信双方协商得到的 ISAKMP SA 具有抗量子安全性，进一步保证了 IKE 第二阶段即快速模式协商 IPSEC SA 的抗量子安全性；二、利用 QKD 协商密钥使得密钥具有熵增的性质，解决了预共享密钥中密钥更新的问题；三、由于经典协商过程成本较低，仅在第一阶段引入 QKD，第二阶段仍使用经典对称加密算法、第一阶段的协商结果及散列函数完成第二阶段的协商，相比于现有方案更节约成本。

IKE 内进行算法替代：现有的 IKE 协议中的密码算法通常基于公钥基础设施 PKI，由于量子计算机和量子算法的发展，很多基于 PKI 的公钥算法不具有后量子安全性，可以将其中使用的密码算法替换为具有抗量子安全性的密码算法，以构造具有抗量子安全性的 IKE 协议。

IPSec 中除了 IKE 协议之外，还有认证头协议（AH）和安全载荷协议（ESP）用到密码算法。AH 协议保护数据的完整性、认证数据来源的可靠性，但不对数据的机密性进行保护，AH 协议需要用到认证算法。ESP 协议对数据的机密性进行保护，也可以保护数据的完整性、认证数据来源的可靠性，即 ESP 协议需要用到加密算法和认证算法，在这里加密算法使用的密钥为通信双方在 IKE 协议里协商得到的对称密钥，所以 ESP 协议里的加密算法一般为对称加密算法。这里涉及到的加密算法仍采用 AES 加密算法，认证算法可采用已被证明是信息论安全的安全的 CRC-based MAC，使协议具有抗量子安全性。

§2.5 量子计算环境下的语义安全和不可区分性

2.5.1 概述

加密体制的安全性定义是密码学的重要分支。第一个严格的安全性定义是由 Goldwasser 和 Micali[1]提出的。安全性定义通常从两方面分析，一个是希望达到的安全目标，一个是敌手可能的攻击模型。就安全目标而言，有语义安全、加密不可区分性和不可延展性等。就敌手的攻击模型而言，有被动攻击（分为密钥无记忆被动攻击和密钥相关被动攻击）、选择明文攻击（CPA）、非自适应选择密文攻击（CCA1）和自适应选择密文攻击（CCA2）等。

随着量子计算机和量子密码学理论的发展，经典密码学受到了严重的威胁。利用 Shor 提出的算法[2]，一个拥有量子计算机的敌手能够攻破任何基于因式分解和离散对数困难问题的加密算法，如 RSA，ElGamal 等。而为了保持分组密码和哈希函数的安全性，则需要更长的密钥和输出长度[3,4]。这些都导致了抗量子密码的发展。量子密码学的迅速发展，使得不得不推广加密算法的安全概念，考虑量子计算环境下的安全性定义。[5-8]等文献都对量子计算环境下的安全性定义进行探索,其中[5-7]考虑的都是经典加密体制在量子计算环境下的安全性。在经典的安全模型中，所有的参与者及相互之间的交流都是经典的，而当希望利用安全模型去证明一个经典算法是抗量子安全的，就必须考虑敌手拥有量子计算机的情况。除此之外，敌手还将被允许进行叠加态询问。例如，经典 CPA 模型下敌手的一次询问即发送一个明文 m，然后得到密文$E(m)$，而在量子的 CPA 模型下，敌手的一次询问可以发送消息的叠加态$\sum_{m,c}\alpha_{m,c}|m,c\rangle$，并得到相应的密文叠加态$\sum_{m,c}\alpha_{m,c}|m,c\oplus E(m)\rangle$。一个叠加态中消息的个数是不受限制的，甚至可以是指数多个。在许多文献中，都考虑了这种密码体制是经典的，却允许敌手进行量子叠加态询问的情况[5,6,9-11]。之所以考虑这样的情景，是因为当经典的密码设备在很强的磁场或高温环境下可能表现出量子行为，或者敌手具有量子计算机而其他参与者只有经典计算机时也可能出现叠加态询问的情况。允许对叠加态进行询问是量子安全模型十分重要的一个特点，一个加密算法的安全性证明困难之处也常常是在归约时对叠加态的处理。

除了加密体制的安全概念，签名、消息认证码和伪随机函数等的安全定义也都被推广至量子计算场景。[9]给出了量子伪随机函数的概念，并证明了若干经典的伪随机函数在量子计算环境下仍具有安全性，包括基于伪随机生成子的 GGM 构造[12]以及基于 LWE 的构造[13]。[5]中则给出签名方案的量子安全性定义，并利用 Chameleon 哈希给出一个将经典意义下安全的签名方案转化为在量子环境下安全的签名方案的一般构造。[10]给出了基于身份的加密算法（IBE）的量子安全定义，并证明了 Gentry 等提出的 IBE 体制的量子安全性（基于

相应的格困难问题假设）。该文献中还考虑了量子的随机预言模型，[5]在量子 RO 模型下构造量子安全的签名方案。

本节主要基于 13 年及 16 年美密的论文[5]、[6]，总结文献中与经典加密体制在量子计算环境下的语义安全和不可区分性概念相关的内容。

2.5.2 选择明文攻击下的不可区分性

经典的对称加密体制定义为三个概率多项式时间的算法(Gen, Enc, Dec)，其中$Gen(1^n)$输入安全参数，输出密钥k，加密算法Enc和解密算法Dec则满足对明文空间中的任意消息 x 都有$Pr[Dec(k, Enc(k,x)) = x] = 1$。关于加密体制的安全概念本文只涉及自适应选择明文攻击下的密文不可区分性（IND-CPA）及自适应选择明文攻击下的语义安全（SEM-CPA），该定义是基于“游戏”的，分为学习阶段和挑战阶段。在 CPA 学习阶段，敌手可以自适应地选择明文，并得到相应的密文。在 IND 挑战阶段，敌手选择两个等长的密文发送给挑战者，挑战者将其中一个密文加密返回，若敌手能够猜出被加密的密文是哪一个，即获胜。IND-CPA 要求任意概率多项式时间的敌手赢得该游戏的几率超过 1/2 的部分都是可忽略的。在 SEM 挑战阶段，敌手则需生成挑战模块(S_m, h_m, f_m)，S_m是某个多项式规模的线路，可以按某个明文分布输出一个明文，h_m和f_m都是明文空间的函数，h_m是建议函数，f_m是目标函数。挑战者收到挑战模块后由S_m生成明文x并返回$(Enc_k(x), h_m(x))$，敌手的任务是输出$f_m(x)$。SEM-CPA 要求对任意一个概率多项式时间的敌手 A，都存在一个概率多项式时间的算法 A’，A 经过 CPA 学习阶段和 SEM 挑战阶段，A’不经历 CPA 学习阶段，生成与 A 完全相同的挑战模块，且在 SEM 挑战阶段只收到$h_m(x)$而不收到密文。两者获胜的概率相差可忽略。IND-CPA，SEM-CPA 具体的定义可见[14]。

在经典的 CPA 学习阶段，相当于敌手拥有一个加密预言机，当询问一个明文时，得到相应的密文。在量子的计算环境中则需考虑量子的加密预言机，敌手可以对明文的叠加态进行询问，得到相应的密文叠加态。[5]给出了一种量子加密预言机的定义：

定义 2.5.1（量子加密预言机）设Enc是对称加密体制$\mathcal{E}$的加密算法，定义相对于密钥 k 的量子加密预言机为酉算子：

$$U_{Enc_k}: \sum_{x,y} \alpha_{x,y} |x\rangle|y\rangle \to \sum_{x,y} \alpha_{x,y} |x\rangle|y \oplus Enc_k(x)\rangle. \quad (2.5.1)$$

利用量子加密预言机，定义 qCPA 学习阶段为：敌手$\mathcal{A}$可以访问预言机U_{Enc_k}（安全参数的）多项式次。在量子计算环境下，CPA 学习阶段将被替换为 qCPA 学习阶段。量子环境下对 CPA 学习阶段的扩展是自然的，只是允许对叠加态的询问。但 IND 挑战阶段在量子环境的扩展则比较复杂，在一些细节上采取不同的选择都将导致不同的安全概念。[5]中定义了一种量子的 IND 挑战阶段，称为完全量子 IND 挑战阶段（fqIND）：

定义 2.5.2（fqIND）敌手$\mathcal{A}$让寄存器处于态$\sum_{x_o,x_1,y} \alpha_{x_0,x_1,y} |x_0\rangle|x_1\rangle|y\rangle$，包含两个 m 比特的态和一个用于存储密文的辅助态。挑战者$\mathcal{C}$采样$b \xleftarrow{\$} \{0,1\}$并进行变换：

$$\sum_{x_0,x_1,y} \alpha_{x_0,x_1,y} |x_0\rangle|x_1\rangle|y\rangle \to \sum_{x_0,x_1,y} \alpha_{x_0,x_1,y} \alpha_{x_0,x_1,y} |x_0\rangle|x_1\rangle|y \oplus Enc_k(x_b)\rangle. \quad (2.5.2)$$

$\mathcal{A}$的目标是输出b。

将qCPA学习阶段与fqIND挑战阶段结合起来就得到了量子选择明文攻击下的完全量子不可区分性概念（fqIND-qCPA）。

定义 2.5.3（fqIND-qCPA）一个对称加密体制称为 fqIND-qCPA 安全的，若任意量子概率多项式时间的敌手赢得由 qCPA 学习阶段和 fqIND 挑战阶段构成的游戏的几率与$1/2$相差可忽略。

这一安全性定义不仅允许敌手在学习阶段进行加密询问时采用叠加态，在挑战阶段也允许敌手的挑战询问是叠加态，即敌手与挑战者的全部交流都允许是叠加态，这是很强的安全定义。事实上，[5]中证明了不存在任何经典对称加密体制满足这种安全性定义。该安全性定义的问题在于允许敌手询问的明文态与密文态纠缠，且这种纠缠依赖于加密的是哪个寄存器中的密文，利用这种纠缠，总可以构造挑战模块，使得以接近 1 的概率猜对b。

[5]中提出的另一种量子选择明文攻击下不可区分性定义为 IND-qCPA，即学习阶段是量子选择明文攻击，可以进行叠加态询问，而挑战阶段和经典的挑战阶段完全一样。文中证明在一些基本的计算假设下（如经典安全的伪随机函数存在），IND-qCPA 严格强于 IND-CPA。

fqIND-qCPA 的概念太强以至于没有经典对称加密算法能够满足，所以[5]中考虑了IND-qCPA。那么是否有介于这两者之间的安全性定义呢？[6]对这一问题进行了深入的探讨。文中分别从四个方面考虑量子 IND 挑战阶段的不同可能，构成二叉“安全树”，从而得到$2^4 = 16$种可能的量子不可区分性的定义，并经过分析留下合理的两种。[6]中考虑的四个方面如下：

1．Game 模型：预言机模型（$\mathcal{O}$） vs. 挑战者模型（$\mathcal{C}$）。在预言机模型中，敌手$\mathcal{A}$可以访问加密和挑战预言机，即在游戏中他可以作用酉门$\mathcal{O}_1,\cdots,\mathcal{O}_q$来进行叠加态询问。在这种情况下$\mathcal{A}$被刻画为一量子线路，交替地执行一系列的酉门$U_0,\cdots,U_q$和$\mathcal{O}_i$。对于输入态$|\varphi\rangle$，敌手计算：

$$U_q\mathcal{O}_q\cdots U_1\mathcal{O}_1U_0|\varphi\rangle. \tag{2.5.3}$$

$\mathcal{A}$本身不知道预言机$\mathcal{O}_i$的线路，只是以黑箱的形式调用它，$\mathcal{O}_i$可以看做是$\mathcal{A}$的内部线路，在整个游戏过程由$\mathcal{A}$完全控制。fqIND 定义采用的就是这种模型。而挑战者模型中，敌手$\mathcal{A}$是和一个外部的挑战者$\mathcal{C}$进行游戏，对$\mathcal{C}$进行加密询问和挑战询问，$\mathcal{A}$与$\mathcal{C}$共享一个量子寄存器，但$\mathcal{C}$可能有另外不受$\mathcal{A}$控制的量子输入和输出线路。敌手在（$\mathcal{O}$）模型中有更大的权力。

2. 明文态：量子态（Q）vs. 经典描述（c）。在（Q）模型中，$\mathcal{A}$选择作为挑战模块的两个 m 量子比特明文可以是任意的量子态，且可能与别的量子态相纠缠。（c）模型中只能选择两个量子态的经典描述。一个量子态ρ的经典描述是一个经典的比特串，刻画一个输出为ρ（没有输入且由某个固定的初始态$|0\rangle$开始）的量子线路S。即$\mathcal{A}$只可发送经典信息给$\mathcal{C}$，$\mathcal{C}$将读取经典描述并根据挑战比特 b 生成其中一个量子态。这种情况下，$\mathcal{A}$无法建立明文态与其他量子态的纠缠。

3. 明文态是否归还: Yes（Y）vs. No（n）。在（n）模型中$\mathcal{A}$挑战模块中的两个明文态不归还给$\mathcal{A}$。在（Y）模型中，两个明文态将被留在原始的寄存器，即$\mathcal{A}$在任何时候都可以得到它们。

4. 酉变换的类型（1）vs.（2）。在量子计算中，对一个叠加态计算函数$f(x)$的值通常采用的方式是利用辅助寄存器：

$$\sum_{x,y}\alpha_{x,y}|x,y\rangle \to \sum_{x,y}\alpha_{x,y}|x,y\oplus f(x)\rangle. \tag{2.5.4}$$

这种方式保证了即使在 f 不可逆的情况下，算子也是可逆的，称为（1）型变换。在模型（1）中，若Enc_k将 m 比特的明文映到 l 比特的密文，则此时的加密算子作用在 m+l 量子比特上：

$$\sum_{x,y}\alpha_{x,y}|x,y\rangle \to \sum_{x,y}|x,y\oplus Enc_k(x)\rangle. \tag{2.5.5}$$

fqIND 采用的就是这种方式。（2）模型中则考虑加密算法是某比特串空间之间双射的情况（把算法的随机值也看作输入的一部分），若加密算法不改变长度，以下变换也是可逆的：

$$\sum_{x}\alpha_{x}|x\rangle \to \sum_{x}\alpha_{x}|Enc_k(x)\rangle. \tag{2.5.6}$$

若加密算法是变长的，则变换为：

$$\sum_{x,y}\alpha_{x,y}|x,y\rangle \to \alpha_{x,y}|\varphi_{x,y}\rangle. \tag{2.5.7}$$

其中辅助寄存器的长度为$|y|=|Enc_k(x)|-|x|$且$\varphi_{x,0}=Enc_k(x)$.

通过考虑这四个方面，将得到 16 种可能的不可区分性定义，但其中很多是不合理的，如（$\mathcal{O}c\cdots$）类模型，$\mathcal{O}$意味着预言机是$\mathcal{A}$的量子线路中的量子门，所以$\mathcal{A}$完全可以询问与别的态纠缠的量子态，所以与c是矛盾的。这 16 种安全性定义中还有一些太强而不存在任何经典对称加密体制可以达到，如（$\mathcal{CQ}n1$），它们与 fqIND 安全性定义的情况一样可用纠缠态进行攻击。去掉所有这些不合理或太强的安全性定义，最终剩下两个：（$\mathcal{C}cn2$）和（$\mathcal{CQ}n2$）。将它们分别定义为“密文的量子不可区分性”（qIND）和“广义的密文量子不可区分性”（gqIND）。这两种不可区分性相应的挑战阶段具体整理如下：

定义 2.5.4（qIND 挑战阶段）$\mathcal{A}$选择两个具有有效经典描述的量子态ρ_0,ρ_1，将这两个量子态的经典描述作为挑战模块发送给挑战者$\mathcal{C}$。$\mathcal{C}$均匀随机采样一个比特 b，生成相应的ρ_b，并对ρ_b作用（2）型算子$U_{Enc_k}^{(2)}$再返回给$\mathcal{A}$，$\mathcal{A}$的目标是输出 b。

定义 2.5.5（gqIND 挑战阶段）$\mathcal{A}$选择两个量子态ρ_0,ρ_1并发送给$\mathcal{C}$。$\mathcal{C}$均匀随机采样一个比特 b，去掉（取偏迹）ρ_{1-b}，对ρ_b作用（2）型算子$U_{Enc_k}^{(2)}$并返回给$\mathcal{A}$，$\mathcal{A}$的目标是输出 b。

将以上两个挑战阶段与 qCPA 学习阶段相结合就得到了两种量子密文不可区分性的定义：量子选择明文攻击下密文的量子不可区分性（qIND-qCPA）和量子选择明文攻击下广义的密文量子不可区分性（gqIND-qCPA）。已定义的四种不可区分性之间的关系是 qIND-qCPA 严格强于 IND-qCPA，gqIND-qCPA 不弱于 qIND-qCPA，fqIND-qCPA 严格强于 gqIND-qCPA。

2.5.3 选择明文攻击下的语义安全

类似 IND-qCPA，在经典的语义安全定义的基础上允许敌手进行量子的选择明文攻击（qCPA），即得到一个量子计算环境下的语义安全性定义 SEM-qCPA。[6]中证明了 IND-qCPA 与 SEM-qCPA 是等价的。

为了定义与 qIND-qCPA 等价的语义安全概念，[6]中提出了另一种量子语义安全概念，它的学习阶段仍采用 qCPA，即敌手拥有量子加密预言机，挑战阶段定义如下：

定义 2.5.6（量子 SEM（qSEM）挑战阶段）$\mathcal{A}$发送给$\mathcal{C}$挑战模块，包含如下内容的经典描述：

- 一个量子线路G_m，以$poly(n)$比特作为输入，输出是一个 m 量子比特的明文态；
- 一个量子线路h_m，以 m 量子比特的明文态作为输入，输出$poly(n)$量子比特的建议态；
- 一个量子线路f_m，以以 m 量子比特的明文态作为输入，输出$poly(n)$量子比特的目标态。

挑战者$\mathcal{C}$采样$y \xleftarrow{\$} \{0,1\}^{poly(n)}$并计算得到两个一样的量子态$\rho_y = G_m(y)$。一个用于计算辅助信息$h_m(\rho_y)$，一个用于计算密文$U_{Enc_k}\rho_y U_{Enc_k}^{\dagger}$。$\mathcal{C}$将$(U_{Enc_k}\rho_y U_{Enc_k}^{\dagger}, h_m(\rho_y))$返回给$\mathcal{A}$，$\mathcal{A}$的目标是输出$f_m(\rho_y)$。称$\mathcal{A}$赢得 qSEM-qCPA 游戏，若没有量子多项式时间的算法可以以不可忽略的概率区分$\mathcal{A}$的输出态和目标态$f_m(\rho_y)$。

在一个约减的游戏中，模拟器$\mathcal{S}$只收到建议态$h_m(\rho_y)$而不收到密文态，也不能询问量子加密预言机。量子选择明文攻击下的量子语义安全（qSEM-qCPA）定义如下：

定义 2.5.7（qSEM-qCPA）一个对称加密体制被称为 qSEM-qCPA 的，若对每个量子多项式时间的算法$\mathcal{A}$，存在一个量子多项式时间的算法$\mathcal{S}$，$\mathcal{S}$生成与$\mathcal{A}$相同的挑战模块，且$\mathcal{A}$赢得由 qCPA 学习阶段和 qSEM 挑战阶段构成的游戏的概率与$\mathcal{S}$赢得约减游戏的概率相差可忽略。

该定义中赢得游戏的条件是输出的量子态与$f_m(\rho_y)$对量子多项式时间的区分器不可区分，而不要求两个量子态完全一样。这是因为在物理上做不到准确地判断$\mathcal{A}$的输出态与$f_m(\rho_y)$是否是同样的量子态。另一种方式是采用迹距离，但由于是采用计算基态来承载密文，很有可能两个密文迹距离很大却不可区分，所以采用对量子多项式时间算法不可区分的准则更为合理。同样，[6]中证明了 qSEM-qCPA 与 qIND-qCPA 等价。

2.5.4 安全的加密方案

[6]中利用量子安全的伪随机置换总体构造了一个具有 gqIND-qCPA 安全（从而具有 qIND-qCPA 安全）的对称加密体制。一个有效的置换总体是经典置换构成的集合$\Pi_n = \{\pi_k : \{0,1\}^n \to \{0,1\}^n\} \subset S_{2^n}$，有着密钥空间$\mathcal{K}_\Pi$和定义域$\{0,1\}^n$。并存在三个概率多项式时间的算法$(\mathcal{I}, \Pi, \Pi^{-1})$满足：

1.初始化算法$\mathcal{I}$输入安全参数，输出密钥空间的一个随机密钥$k \xleftarrow{\$} \mathcal{K}_\Pi$；

2.函数Π以密钥 k 和定义域中的元素 x 作为输入，输出$\pi_k(x)$；

3.函数Π^{-1}以密钥 k 和定义域中的元素 x 作为输入，输出$\pi_k^{-1}(x)$。

一个量子安全的伪随机置换总体是一个效置换总体，满足与S_{2^n}上均匀随机分布的总体不可区分。具体定义为：

定义 2.5.8（量子 PRP）一个有效置换总体Π_n称为量子安全的伪随机置换总体，若对任意量子多项式时间的预言机$\mathcal{A}$，成立：

$$|Pr_{\pi\xleftarrow{\$}\Pi_n}[\mathcal{A}^{|\pi\rangle}(1^n)=1]-Pr_{\pi\xleftarrow{\$}S_{2^n}}[\mathcal{A}^{|\pi\rangle}(1^n)=1]|\leq negl(n), \qquad (2.5.8)$$

其中$|\cdot\rangle$表示可对叠加态进行询问。

利用量子安全的伪随机置换总体可构造具有 gqIND-qCPA 安全的对称加密体制如下：

构造 2.5.1 .对安全参数 n，设$m=poly(n)$，$\tau=poly(n)$。$\Pi_{m+\tau}=(\mathcal{I},\Pi,\Pi^{-1})$为作用在$m+\tau$长比特串上的有效置换总体，密钥空间为$\mathcal{K}_\Pi$。明文空间为$\mathcal{M}=\{0,1\}^{\mu m}$，其中$\mu\in\mathbb{N},\mu=poly(n)$。密文空间为$\mathcal{C}=\{0,1\}^{\mu(m+\tau)}$。

密钥生成算法$k\leftarrow Gen(1^n)$: 输入安全参数 n，密钥生成算法运行$k\leftarrow\mathcal{I}(1^{m+\tau})$并返回密钥 k；

加密算法$y\leftarrow Enc_k(x)$: 输入消息$x\in\mathcal{M}$和密钥$k\in\mathcal{K}$，加密算法将 x 分为μ个 m 比特的块$x_1,\cdots,x_\mu$。对每个块x_i，均匀随机地采样一个新的τ比特串$r_i\xleftarrow{\$}\{0,1\}^\tau$，计算$y_i=\pi_k(x_i\parallel r_i)$。输出密文$y=y_1\parallel\cdots\parallel y_\mu$。

解密算法$x\leftarrow Dec_k(y)$:对输入密文$y\in\mathcal{C}$和密钥$k\in\mathcal{K}$，解密算法将 y 分为μ个$m+\tau$比特的块$y_1,\cdots,y_\mu$。对每个块计算$x_i'=(\pi_k^{-1}(y_i))_m$，其中$(s)_m$表示取比特串的前 m 比特。输出明文$x'=x_1',\cdots,x'_\mu$。

[6]中证明了只要$\Pi_{m+\tau}$是量子安全的伪随机置换总体（qPRP），则构造 1 中的对称加密体制(Gen,Enc,Dec)是 gqIND-qCPA 安全的。证明思路如下：假设$\mathcal{D}$是任意一个量子多项式时间的区分器，希望证明它在 qCPA 学习阶段和 gqIND 挑战阶段构成的游戏中获胜的概率与 1/2 相差可忽略。首先利用$\Pi_{m+\tau}$的量子伪随机性将从$\Pi_{m+\tau}$选取置换π改为从$S_{2^{m+\tau}}$中均匀随机地选取置换π。$\mathcal{D}$在原游戏中和修改后的游戏中获胜的几率相差是可忽略的,否则可以利用$\mathcal{D}$区分$\Pi_{m+\tau}$总体和$S_{2^{m+\tau}}$总体，与$\Pi_{m+\tau}$的量子伪随机性矛盾。再引入量子操作$\mathcal{T}$，证明加密过程对应的量子操作作适当修改后（修改后的游戏与原游戏中$\mathcal{D}$获胜的概率相差可忽略）的操作$\mathcal{E}$与$\mathcal{T}$的距离是可忽略的。而量子操作$\mathcal{T}$是输入任意量子态都输出完全混合态的量子操作。所以可以将原游戏修改为一个新的游戏，$\mathcal{D}$在两个游戏中获胜的概率相差可忽略，而在新游戏中，$\mathcal{D}$在挑战阶段发送的任意明文态被加密后都是返回完全混合态，从而$\mathcal{D}$不能区分两个明文的密文。

在[9]中，Zhandry 证明了几种经典的伪随机函数总体的构造是量子安全的（在格困难问题或其它一些假设下）。但目前还没有文献证明某个伪随机置换总体是量子安全的。

2.5.5 总结

经典的安全概念在量子计算机实现后将不再适用，所以发展量子计算环境下的安全概念对保障密码体制的长期安全性是十分重要的。加密体制、签名算法和消息认证码等密码体制

的量子安全概念都已有了一定的研究，但距离形成完善的体系还有很长的距离，需要更深入地探索。

参考文献

[1] Goldwasser, S., Micali, S. Probabilistic encryption. J. Comput. Syst. Sci. 28(2), 270–299 (1984)

[2] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In FOCS'94, pages 124-134. IEEE Comput. Soc. Press, 1994.

[3] L. K. Grover. A fast quantum mechanical algorithm for database search. In STOC'96, pages 212-219. ACM Press, 1996.

[4] G. Brassard, P. Hoyer, and A. Tapp. Quantum Algorithm for the Collision Problem. arXiv:quant-ph/9705002, 1997.

[5] Boneh D, Zhandry M. Secure signatures and chosen ciphertext security in a quantum computing world. In: CRYPTO 2013, Part II. pp. 361-379. Springer Berlin Heidelberg, 2013.

[6] Gagliardoni, Tommaso, Andreas Hülsing, and Christian Schaffner. Semantic security and indistinguishability in the quantum world. In: CRYPTO 2016, Part III, pp. 60-89. Springer, Heidelberg,2016.

[7] Alagic G, Broadbent A, Fefferman B, et al. Computational Security of Quantum Encryption[J]. arXiv preprint arXiv:1602.01441, 2016.

[8] C. Xiang and L. Yang. Indistinguishability and semantic security for quantum encryption scheme. SPIE Photonics Asia 2012, in Proceedings of SPIE 8554, p.85540G

[9] Zhandry M. How to construct quantum random functions. Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on. IEEE, 2012: 679-687.

[10] Zhandry M. Secure identity-based encryption in the quantum random oracle model. In: CRYPTO 2012。pp. 758-775. Springer, Heidelberg,2012.

[11] J. Watrous. Quantum algorithms for solvable groups. In STOC '01, pages 60-67. ACM Press, 2001.

[12] Goldreich O, Goldwasser S, Micali S. How to Construct Random Functions. Journal of the ACM (JACM), 33(4):792–807, 1986.

[13] Banerjee A, Peikert C, Rosen A. Pseudorandom Functions and Lattices. In: EUROCRYPT 2012, pp.1–26, 2011.

[14] O. Goldreich. Foundations of Cryptography: Volume 2, Basic Applications.Cambridge University Press, Cambridge, UK, 2004.

§2.6 量子公钥加密

公钥密码系统在不预先共享密钥的前提下安全传递信息是公钥密码的优势，经典公钥密码系统已经广泛应用到生活中，比如网上支付用的 U 盾、网页安全浏览、电子护照等等。1976 年，Diffie 和 Hellman 提出公钥加密的概念[1]，随后，各种基于经典图灵机模型的公钥加密协议及证明其安全性的理论被相继提出，然而经典公钥的安全性是基于未被证明的数学困难问题，且量子计算机的发展和各种量子算法的提出使得基于大整数分解和离散对数的公钥密码方案的安全性面临巨大威胁。因此研究抵抗量子计算机攻击的公钥加密方案具有重大意义。抵抗量子计算机攻击的公钥密码体制依据计算环境可以分为两类，一类是基于经典计算环境，属于经典抗量子密码，这类公钥密码方案是基于量子计算机不擅长计算的一些数学问题而设计的，主要有：基于编码的密码体制如文献[2]、基于多年变量值的密码体制如[3]、基于格的密码体制如[4]等；一类是基于量子计算与量子通信环境，其安全性依赖于量子力学基本原理，如未知量子态不可克隆原理和非正交量子态不可区分。

量子公钥加密到目前为止已有近二十年的发展史，2000 年，Okamoto 提出一个基于背包方案的公钥加密方案[5]，在文献[5]中，量子门限单向函数起着举足轻重的作用，方案的安全性建立在求子集和问题对任何量子多项式图灵机都是棘手的计算假设上。2001 年，Gottesman 在他的量子签名文章中首先提出用量子态作公钥[6]。2003 年杨理提出经典 McEliece 公钥加密的一个推广，提出量子信息的公钥加密，该加密方案也可加密经典信息[7]。2005 年，A. Kawachi 等提出一个加密经典比特的量子公钥加密方案，利用如何区分两个随机陪集的计算困难问题提出量子加密方案，该方案第一次将量子公钥算法的安全性规约到图的自同构[8]。2008 年，M.Nikolopoulos 基于单量子比特旋转提出一个量子公钥加密方案，在该方案中，消息的接收者根据自己的私钥对量子态旋转相应的角度作为量子公钥，私钥是经典的，消息发送者根据所要发送的经典信息对公钥相应的泡利操作，解密时接受者根据私钥对密文量子态反向旋转相应的角度再对量子态作测量即可得明文信息[9]。2010 年，杨理等构造了诱导陷门单向量子变换，是陷门单项函数在量子态空间上的推广，建立了经典单向函数到量子单向变换之间的联系，用量子语言统一描述了七类经典的公钥加密算法[10]，并提出了一个公钥为量子态+经典向量的量子公钥加密方案[11]，该方案私钥是布尔函数，加密信息为经典信息。2012 年，H. Fujita 提出一个基于量子纠错码的方案[12]，针对 Fujita 的质疑，杨理等提出了二次加密的量子公钥加密协议[13]，梁敏等将私钥量子信道(PQC)和[11]中的量子公钥加密方案相结合构造了一个用量子态作为公钥加密量子信息的公钥加密方案[14]，杨理等还提出了基于共轭基编码的加密单比特经典信息的量子公钥加密方案，其中公钥是量子态，一个私钥对应多个公钥，并将其扩展为可加密多比特消息的公钥加密方案，并证明其是有界信息论安全的。由于该方案无须利用纠缠态，更易于在实验室实现[15]。文献[15]还分析了[11]所提出的协议的安全性，给出一种通过对其公钥进行攻击完全攻破其私钥的攻击方法。2015 年，吴辰苗等提出一种按比特加密的量子公钥加密方案[16]。

公钥加密算法的六要素分别为明文、密文、加密算法、解密算法、公钥、私钥，每种元素都有经典空间和量子空间两种情况，按照每种元素的性质，量子公钥加密协议共可分为 64 类，由于物理性质的限制，并不是每种协议都能实现，目前已有八种协议已被构造出来。分别是：第一类，六个元素都属于经典空间，常用的公钥加密算法如 RSA[17]，ECC[18]等即该类型，文献[5]中的协议，在密钥生成过程中用到了量子算法，该协议中加密算法的六要素均为经典的，因此，该协议也属于此类协议；第二类，明文、密文、公钥、私钥、加密算法均属于经典空间，只有解密算法属于量子空间，如使用 Shor 算法求解离散对数问题，可对基于离散对数问题的公钥加密方案进行解密，得到明文；第三类，明文、公钥、私钥属于经典空间，密文、加密算法、解密算法属于量子空间；第四类，明文和私钥属于经典空间，

密文、加密算法、解密算法、公钥属于量子空间；第五类，明文属于经典空间，密文、公钥、私钥、加密算法、解密算法属于量子空间；第六类，公钥和私钥属于经典空间，明文、密文、加密算法、解密算法属于量子空间；第七类，私钥属于经典空间，公钥、明文、密文、加密算法、解密算法属于量子空间；第八类，私钥、公钥、明文、密文、加密算法、解密算法均属于量子空间。

下面介绍一下量子公钥加密涉及到的两个安全性概念。其一是 Holeve 界，Holeve 界是可访问信息的一个上界，在量子信息理论中扮演者重要的角色，Holeve 界定义如下：设 Alice 以概率$p_0, p_1, \ldots, p_n$制备的量子态的密度算子为ρ_x，其中$x = 0,1,..,n$。Bob 进行 POVM 元$E_y = \{E_0, E_1, \ldots, E_m\}$描述的测量，测量结果为$Y$。Holeve 界断言，对 Bob 可以进行的任何测量，有$H(X{:}Y) \leq S(\rho) - \sum_x p_x S(\rho_x)$，其中$\rho = \sum_x p_x \rho_x$。Holeve 界有一个专门的名称，叫 Holeveχ，简记为χ。Holeve 界在量子公钥加密体系中有很重要的应用，它限制了跟私钥相关的量子公钥可以发布的份数，这个定理也使得第三者或窃听者无法从量子公钥获取到私钥的完整信息，保护了私钥和密文的私密性，也保障了量子公钥加密方案的安全性；在量子公钥加密系统中，为了保护合法用户之间的通信，每个量子公钥可以发布的份数受限于一个上限值，这个上限就是 Holeve 量χ，即跟解密私钥相对应的量子公钥最多可以发布χ份。其二是量子单向门限函数，一个量子单项函数是这样一个映射：$F{:}Z \to Q$，其中Z表示一个整数集合，Q表示一个物理系统的量子状态集合，通过F由Z计算Q是高效的，而它的逆过程很困难甚至不可能，单在相关门限信息的辅助下求逆过程是很容易计算的，这样的量子单项函数叫做量子门限单向函数[9]。

量子公钥加密虽然取得一些成果，但还处在发展之中，且研究点主要集中在如何构造具体的量子公钥加密方案上，成熟和完善的量子公钥加密方案不多，其中以量子门限单向函数研究的居多，在这些研究中，Holeve 界，一个可以从公开的量子公钥中获取有关私钥的最大信息量决定了每一个私钥可以发布的最大量子公钥数，这在量子公钥加密安全性的研究中起着很重要的作用。另外，由于量子公钥需要注册，用户身份需要认证，这些问题需要量子公钥基础设施来解决，量子公钥基础设施的缓慢发展限制了量子公钥加密方案的发展。因此，量子公钥加密有很大的研究空间。

参考文献

[1].Diffie W , Hellman M . New directions in cryptography[M]. IEEE Press, 1976.

[2].Berlekamp, E, McEliece, R, van Tilborg, H. On the inherent intractability of certain coding problems (Corresp.)[J]. 1978.

[3].Boyin Yang J C. Building secure tame-like multivariate public-key cryptosystems: The new TTS[C]// 2005.

[4].MiklósAjtai, Cynthia Dwork. A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence[C]// Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing, El Paso, Texas, USA, May 4-6, 1997. ACM, 1997.

[5].Okamoto T, Tanaka K, Uchiyama S. Quantum Public-Key Cryptosystems[C]// 2000.

[6].D.Gottesman and I.L.Chuang (2001),Quantum Digital Signatures, quant-ph/0105032.

[7]. Li Yang. Quantum public-key cryptosystem based on classical np-complete problem. arXiv preprint quant-ph/0310076, 2003.

[8].A.Kawachi, T.Koshiba, H.Nishimura and T.Yamakami (2005),Computational Indistinguishability Between Quantum States and Its Cryptographic Application, Eurocrypt 2005, LNCS 3494, 268-284.

[9].G.M.Nokolopoulos (2008),Applications of single-qubit rotations in quantum public-key cryptography, Phys. Rev. A, 77(3): 032348.
[10]. Li Yang, Min Liang, Bao Li, Lei Hu, and Deng-Guo Feng. Quantum public-key cryptosystems based on induced trapdoor one-way transformations. arXiv preprint arXiv:1012.5249, 2010.
[11].Pan J, Yang L. Quantum Public-Key Encryption with Information Theoretic Security[J]. 2010, 8440.
[12].Fujita H . Quantum McEliece public-key cryptosystem[J]. Quantum information & computation, 2012, 12(3-4):181-202.
[13].Li Yang and Min Liang. A note on quantum mceliece public-key cryptosystem. arXiv preprint arXiv:1212.0725, 2012.
[14].Min L , Li Y . Public-key encryption and authentication of quantum information[J]. 中国科学：物理学、力学、天文学英文版, 2012, 55(9):1618-1629.
[15].Li Yang, Biyao Yang, and Chong Xiang. Quantum public-key encryption schemes based on conjugate coding. arXiv preprint arXiv:1112.0421, 2012.
[16].Wu C, Yang L. A complete classification of quantum public-key encryption protocols[C]//Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology. International Society for Optics and Photonics, 2015, 9648: 964818.
[17].Wu W Q, Cai Q Y, Zhang H G, et al. Bit-Oriented Quantum Public-Key Cryptosystem Based on Bell States[J]. International Journal of Theoretical Physics, 2018: 1-11.
[18]. Ronald L Rivest, Adi Shamir, and Len Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2):120–126, 1978.
[19]. Neal Koblitz. Elliptic curve cryptosystems. Mathematics of computation, 48(177):203–209, 1987.

§2.7 量子零知识证明

2.7.1 背景

随着量子计算的发展，为了保障密码协议在量子计算模型下的安全性，需要研究密码协议在量子攻击模型下的安全概念。Hallgren 等人研究两方协议的量子安全概念[1]，并提出一个可以安全计算任意多项式时间函数的两方协议，该协议的安全性基于合理计算假设。Boneh and Zhandry 则研究量子安全的签名协议[2]。他们提出量子选择消息攻击模型，允许敌手对消息的叠加态进行询问，并提出两个将经典安全的签名协议转化为量子安全的签名协议的一般性构造。Song 等人则给出分析经典安全性证明在量子计算情景是否成立的一般性框架[3]。具体的，他将安全证明分为几个安全规约，并给出在什么条件下安全规约在量子计算情境下仍然成立。Unruh 定义了量子计算绑定的概念[4]，构造一个量子计算绑定的承诺协议，并基于该承诺协议构造任意 NP 语言的三轮统计零知识证明。

零知识证明系统是最基础的安全协议之一，由 Goldwasser 等人提出[5]。许多用于隐私保护或身份认证的密码协议都是基于零知识证明系统构造，一旦底层的零知识在量子计算环境下不具有安全性，则这些密码协议的安全性也将面临威胁。Watrous 首先学习量子交互证明系统[6]，他证明 PSPACE 类中的如何语言都具有三轮量子交互证明系统，这表明常数轮的情况下经典证明系统的能力严格弱于量子交互证明系统。Kitaev 和 Watrous 证明任意具有双边有界错误的多项式轮量子交互证明系统都可以转化为具有单边指数小错的三轮量子证

明系统[7]。随后，Watrous 开启量子零知识的研究，他定义了诚实验证者的量子统计零知识证明系统，并基于量子态区分问题是诚实验证者量子统计零知识证明类（QSZKHV）中的一个完全问题，证明了该类的许多性质[8]。Ben-Aroya 和 Ta-Shma 则给出了 QSZKHV 的另一个完全问题，即量子熵差异问题[9]。由于在量子计算模型中使用“重绕”技术的困难性，证明一个证明系统对非诚实验证者具有零知识性是一个难题。Damgård 等人首先尝试研究非诚实验证者的零知识性证明系统，但他们假定了公共参考串（CRS）的存在[10]。Watrous 随后在这一问题上实现了真正的跨域，他基于振幅放大算法提出了量子重绕技术，并利用该技术证明了图三着色问题的经典零知识证明系统具有量子零知识性[11]。Kobayashi 继续量子零知识证明系统的研究，证明任意量子零知识证明系统都可以转化为公开投币且具有完美完备性的三消息量子零知识证明系统[12]。

Unruh 开启研究量子计算环境下的知识的证明[13]，他提出一种新的量子重绕技术，并基于该技术构造了所有 NP 语言的量子安全的知识的证明。Watrous 和 Unruh 提出的量子重绕技术都只适用于特殊的情景，如何给出一个一般性的量子重绕技术仍是一个难题[14]。Unruh 还对非交互的量子零知识证明进行研究，提出在量子随机语言模型下将一般的量子安全的Σ协议转化为非交互量子零知识证明系统的方法[15]。Broadbent 等人则不局限于 NP 语言，他们研究计算 QMA 语言类，并证明在量子计算隐藏和统计绑定的比特承诺协议存在的假设下，QMA 中的任意语言都具有量子零知识证明协议[16]。

2.7.2 交互证明系统与量子计算不可区分

设 n 是安全参数，v(n)表示 n 的任意一个可忽略函数。对于任意 NP 语言 L，它的证据关系是一个二元关系 R_L，它通过如下关系刻画语言 L：

$$L = \{x: \exists \omega s.t. (x, \omega) \in R_L\}。 \tag{2.7.1}$$

也即$x \in L$当且仅当存在ω使得$(x, \omega) \in R_L$。任意使得$(x, \omega) \in R_L$的ω被称为是x的证据。令$R(x) = \{\omega: (x, \omega) \in R\}$。交互证明系统的定义如下：

定义 2.7.1（交互证明系统）一对交互图灵机(P, V)被称为是语言 L 的交互证明系统，如果V是多项式时间的且(P, V)满足：

1. 完备性：对任意的$x \in L$，

$$Pr[< P, V > (x) = 1] > 1 - v(|x|)。 \tag{2.7.2}$$

2. 合理性：对任意$x \notin L$和任意的交互图灵机$P*$:

$$Pr[< P*, V > (x) = 1] < v(|x|)。 \tag{2.7.3}$$

这里|x|表示 x 的长度。

量子计算不可区分的概念由 Watrous 提出[11]，包括量子态的不可区分和量子操作的不可区分，下面定义中，称一个量子操作为 p-in 和 q-out，表示其具有 p 量子比特的输入和 q 量子比特的输出。量子态的不可区分性定义如下：

[量子态的不可区分]：设$m: \{0,1\}* \to \mathbb{N}$是一个多项式有界的函数，$S \subseteq \{0,1\}*$是一个无限集。对任意的$x \in S$,$\rho_x$和$\xi_x$是$m(x)$量子比特的混合态，则系综$\{\rho_x\}_{x \in S}$和$\{\xi_x\}_{x \in S}$是量子计算不可区

分的，若对任意选择的：
1.多项式 P；

2.多项式有界的函数$k:\{0,1\}*\rightarrow \mathbb{N}$，

3. 系宗$\{\sigma_x\}_{x\in S}$，其中σ_x是$k(x)$量子比特的混合态；

4. 一个(m(x)+k(x))-in，1-out 的规模不超过 p(|x|)的量子线路 Q，都成立

$$|<1|Q(\rho_x\otimes\sigma_x)|1>-<1|Q(\xi_x\otimes\sigma_x)|1>|<v(|x|)。 \quad (2.7.4)$$

定义 2.7.2（量子操作的不可区分）设$n,m:\{0,1\}*\rightarrow \mathbb{N}$是多项式有界的函数，$S\subseteq\{0,1\}*$是一个无限集。对任意的$x\in S$,$\Phi_x$和$\Psi_x$是两个$n(x)$ -in，$m(x)$ -out 的量子操作，则系综$\{\Phi_x\}_{x\in S}$和$\{\Psi_x\}_{x\in S}$是量子计算不可区分的，若对任意选择的：
1.多项式 P；

2.多项式有界的函数$k:\{0,1\}*\rightarrow \mathbb{N}$，

5. 系宗$\{\sigma_x\}_{x\in S}$，其中σ_x是$n(x)+k(x)$量子比特的混合态；

6. 一个(m(x)+k(x))-in，1-out 的规模不超过 p(|x|)的量子线路 Q，都成立

$$|<1|Q(\Phi_x\otimes I(\sigma_x))|1>-<1|Q(\Psi_x\otimes I(\sigma_x))|1>|<v(|x|)。 \quad (2.7.5)$$

量子态的不可区分性和量子操作的不可区分性在量子安全定义中有广泛的应用，是定义量子零知识性的基础。它们通过多项式时间的量子敌手无法区分两个量子态系综或量子操作系综来刻画两个量子态或量子操作的距离。

2.7.3 量子零知识证明

简单地说，零知识性要求在交互证明的过程中，验证者 V 不能得到关于被证明的断言以外的任何知识。在经典的零知识定义中，一个异常的验证者 V*得到公共输入 x 和一个辅助输入，然后通过和证明者 P 的交互计算得到一个输出，这个输出表示某个本身被证明的断言以外的知识。零知识性要求存在一个模拟器，该模拟器在不与 P 交互的情况下能够“模拟”出 V*的输出。这意味着 V*不能从 P 得到任何额外的知识。

在量子计算场景中，V*仍然具有公共输入 x 和辅助输入，但它的辅助输入和输出都可以是量子态，V*也可以执行量子操作。设$k,l:\{0,1\}*\rightarrow \mathbb{N}$是多项式有界的函数，且分别表示 V*的辅助输入量子比特数和输出的量子比特数。V*与 P 在公共输入 x 的交互过程由一个将$k(x)$量子比特态映为$l(x)$量子比特态的量子操作$\Phi^P_{V*,\ x}$表示。类似地，模拟器 S 也具有公共输入 x，$k(x)$量子比特辅助输入和$l(x)$量子比特输出，它自身的计算可以表示为一个$k(x)$-in,$l(x)$-out 的量子操作$\Phi_{S,x}$，量子零知识证明定义如下：

定义 2.7.3（量子零知识证明）一个语言 L 的交互证明系统(P,V)是量子零知识证明，若对任意的多项式时间的量子验证真 V*，存在多项式时间的量子模拟器 S，使得系综$\{\Phi^P_{V*,\ x}\}_{x\in L}$和$\{\Phi_{S,x}\}_{x\in L}$是量子计算不可区分的。

Blum 曾构造哈密顿圈图语言的 3 轮经典零知识证明协议[17]。若 Blum 协议中使用的承诺协议是统计绑定且量子计算隐藏的，则该协议具有量子零知识性[11]。由于哈密顿圈问题是 NP 完全的，利用标准规约，可以得到任何 NP 语言的量子零知识证明。

参考文献

[1]Hallgren, S., Smith, A., Song, F.: Classical cryptographic protocols in a quantum world. CRYPTO 2011, Santa Barbara, CA, USA, 2011, pp. 411−428

[2]Boneh, D., Zhandry, M.: Secure signatures and chosen ciphertext security in a quantum computing world. Advances in Cryptology −CRYPTO'13, Santa Barbara, CA, USA, 2013, pp. 361−379

[3]Song, F.: A note on quantum security for post-quantum cryptography. Int. Workshop on Post-Quantum Cryptography, Cham, 2014, pp. 246−265

[4]Unruh, D.: Computationally binding quantum commitments. EUROCRYPT 2016, Vienna, Austria, 2016, pp. 497−527

[5]Goldwasser, S., Micali, S., Rackoff, C.W.: The knowledge complexity of interactive proof systems, *SIAM J. Comput.*, 1989, **18**, (1), pp. 186−208

[6]Watrous, J.: PSPACE has constant-round quantum interactive proof systems. Proc. of the 40th Annual Symp. on Foundations of ComputerScience, New York, USA, 1999, pp. 112−119

[7] Kitaev, A., Watrous, J.: Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. STOC 2000, Portland, OR, USA, 2000, pp. 608−617

[8] Watrous, J.: Limits on the power of quantum statistical zero-knowledge. The 43rd Annual IEEE Symp. on Foundations of Computer Science, Vancouver, Canada, 2002, pp. 459−468

[9] Ben-Aroya, A., Ta-Shma, A.: Quantum expanders and the quantum entropy difference problem. arXiv preprint quant-ph/0702129, 2007,

[10] Damgård, I., Fehr, S., Salvail, L.: Zero-knowledge proofs and string commitments withstanding quantum attacks'. Advances in Cryptology −CRYPTO 2004, Santa Barbara, CA, USA, 2004, pp. 254−272

[11]Watrous, J.: Zero-knowledge against quantum attacks. Proc. of the 38th Annual ACM Symp. on Theory of Computing (STOC'06), Seattle, WA, USA, 2006, pp. 296−305

[12] Kobayashi, H.: General properties of quantum zero-knowledge proofs. Theory of Cryptography Conf. (TCC 2008), New York, USA, 2008, pp. 107− 124

[13]Unruh, D.: Quantum proofs of knowledge. EUROCRYPT 2012, Cambridge, UK, 2012, pp. 135−152

[14]Ambainis, A., Rosmanis, A., Unruh, D.: Quantum attacks on classical proof systems: the hardness of quantum rewinding'. Foundations of Computer Science (FOCS'14), Philadelphia, PA, USA, 2014, pp. 474−483

[15]Unruh, D.: Non-interactive zero-knowledge proofs in the quantum random oracle model'. EUROCRYPT 2015, Sofia, Bulgaria, 2015, pp. 755-784

[16]Broadbent, A., Ji, Z., Song, F.*, et al.*: Zero-knowledge proof systems for QMA. Foundations of Computer Science (FOCS'16), New Brunswick, NJ, USA, 2016, pp. 31−40

[17]Blum, M., Feldman, P., Micali, S.: Non-interactive zero-knowledge and its applications (extended abstract)'. Proc. of the 20th Annual ACM Symp. on Theory of Computing (STOC'88), 1988, Chicago, IL, USA, pp. 103−112

第 3 章量子计算模型

§3.1 量子逻辑线路

3.1.1 经典逻辑门和可逆逻辑门

经典逻辑线路模型所计算的函数为逻辑函数 $f:\{0,1\}^k \to \{0,1\}$。由于回路可能会不稳定，计算模型中一般不采用回路结构。

(1)单比特上非门运算线路

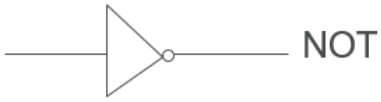


图 3.1-1 单比特非门

(2)双比特上与门运算线路

图 3.1-2 双比特与门

(3)双比特上或门运算线路

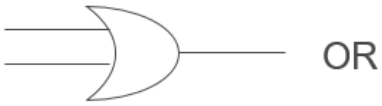


图 3.1-3 双比特或门

(4)双比特上异或运算线路

图 3.1-4 双比特异或门

下面两组等价的逻辑运算表示

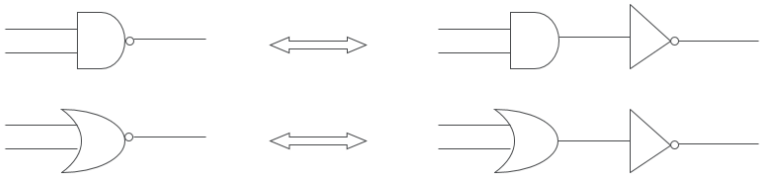


图 3.1-5 两组等价逻辑线路

(5) 半加器(HA)线路，进位比特 c 当 x 和 y 都是 1 时才置 1，否则置 0

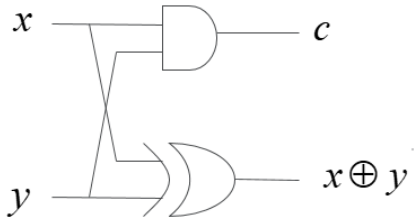


图 3.1-6 半加器（HA）线路

（6）全加器(FA)线路

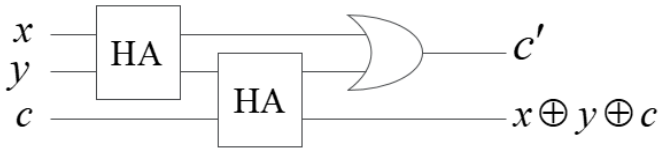


图 3.1-7 全加器（FA）线路

三比特整数的加法线路，输入$x = x_2x_1x_0$和$y = y_2y_1y_0$，输出$z = z_3z_2z_1z_0$

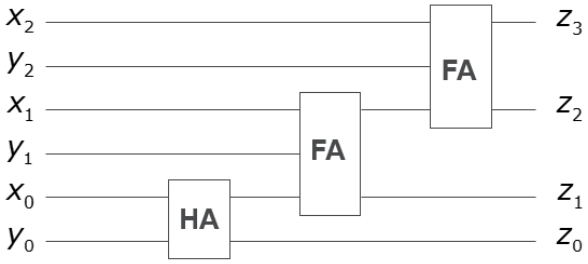


图 3.1-8 三比特整数加法线路

(7)递归构造任意布尔函数的线路

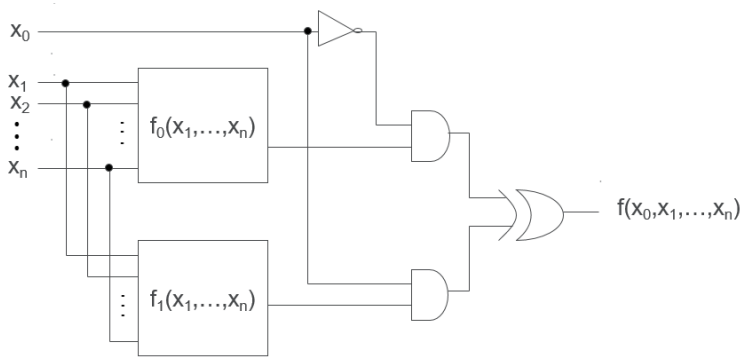
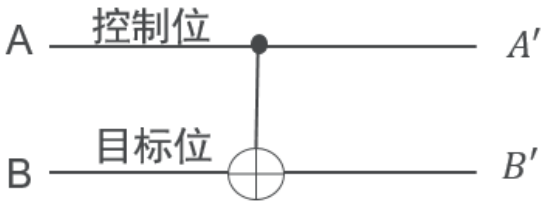


图 3.1-9 递归构造任意布尔函数线路

基本的可逆逻辑门包括非门、受控非门、双控非门（ Toffoli 门）、受控交换门（Fredkin 门）等。

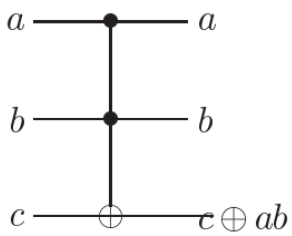
(1) 非门

(2) 受控非门(C-NOT 门)

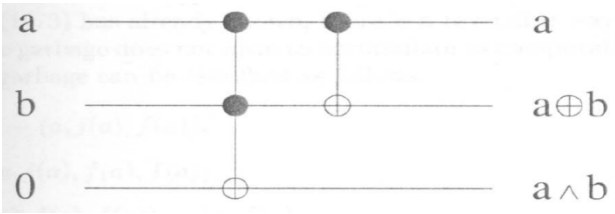


(3) 双控非门(Toffoli 门)

Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

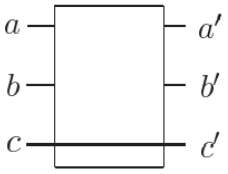


基于 Toffloi 门的可逆两比特加法器

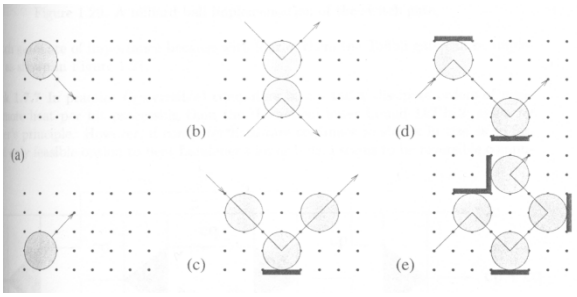


(4) 受控交换门(Fredkin 门)，若控制位 c 为 1，则交换比特 a 和比特 b

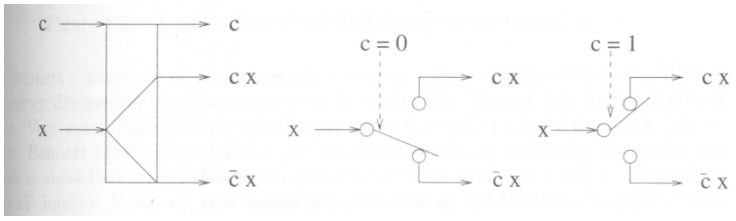
Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	0	1
1	0	0	1	0	0
1	0	1	0	1	1
1	1	0	1	1	0
1	1	1	1	1	1



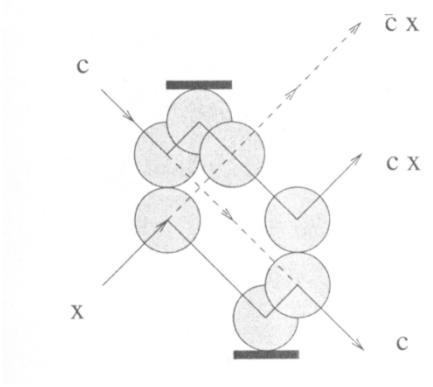
硬球模型：



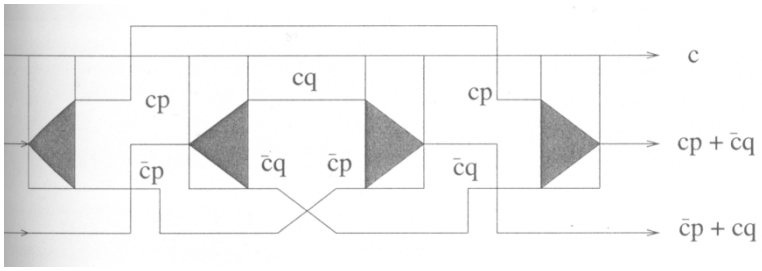
受控切换开关：



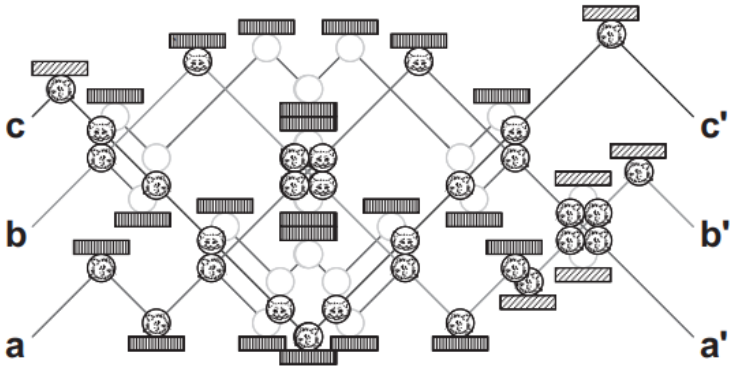
硬球受控交换：



利用 4 个受控交换开关实现（反）Fredkin 门:



Fredkin 门的硬球模型实现:



3.1.2 Deutsch 定理

任意d维幺正变换总可以被分解为$2d^2-d$个二维幺正变换的乘积，并且任何作用在一组量子位上的幺正变换均可以用一系列单量子位门（$U(\alpha,\phi)$门）和双量子位门（CNOT 门）依次作用实现。

证明：用$d-1$个幺正变换可以实现$\begin{bmatrix}a_1\\ \vdots\\ a_d\end{bmatrix}\rightarrow\begin{bmatrix}1\\0\\ \vdots\\0\end{bmatrix}$

为此，取$A_2=\frac{1}{\sqrt{|a_1|^2+|a_2|^2}}\begin{bmatrix}a_1^{*} & a_2^{*}\\ a_2 & -a_1\end{bmatrix}$，有$A_2\begin{bmatrix}a_1\\a_2\end{bmatrix}=\begin{bmatrix}\sqrt{|a_1|^2+|a_2|^2}\\0\end{bmatrix}$,

再取

$$A_3=\frac{1}{\sqrt{|a_1|^2+|a_2|^2+|a_3|^2}}\begin{bmatrix}\sqrt{|a_1|^2+|a_2|^2} & a_3^{*}\\ a_3 & -\sqrt{|a_1|^2+|a_2|^2}\end{bmatrix}, \tag{3.1.1a}$$

$$A_3\begin{bmatrix}\sqrt{|a_1|^2+|a_2|^2}\\a_3\end{bmatrix}=\begin{bmatrix}\sqrt{|a_1|^2+|a_2|^2+|a_3|^2}\\0\end{bmatrix} \tag{3.1.1b}$$

如此继续下去，可得

$$\tilde{A}_d\cdots\tilde{A}_3\tilde{A}_2\begin{bmatrix}a_1\\ \vdots\\ a_d\end{bmatrix}=\sqrt{|a_1|^2+\cdots+|a_d|^2}\begin{bmatrix}1\\0\\ \vdots\\0\end{bmatrix} \tag{3.1.2}$$

这里的$\tilde{A}_i$是2×2矩阵A_i所对应的$d\times d$矩阵。

3.1.2 单量子比特操作

单量子比特是一个向量$|\varphi\rangle=a|0\rangle+b|1\rangle$，其中，$a$和$b$是两个复数且满足$|a|^2+|b|^2=1$。对单 qubit 的操作使用$2\times2$的酉矩阵来描述，其中最重要的单 qubit 操作是 Pauli 矩阵：

$$X=\sigma_x=\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix},Y=\sigma_y=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix},Z=\sigma_z=\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}. \tag{3.1.3}$$

$\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$表示以矩阵为分量的三维向量。

除此之外还有，Hadmard 门（记为H），相位门（记为S），$\pi/8$门（记为T）

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}; S = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}; T = \begin{bmatrix}1 & 0\\ 0 & e^{\frac{i\pi}{4}}\end{bmatrix} = e^{\frac{i\pi}{8}}\begin{bmatrix}e^{-\frac{i\pi}{8}} & 0\\ 0 & e^{\frac{i\pi}{8}}\end{bmatrix}, \tag{3.1.4}$$

易得$H = (X+Z)/\sqrt{2}$,$S = T^2$，$S^2 = Z$,$Z^2 = Y^2 = X^2 = 1$.

关于$\hat{x}, \hat{y}, \hat{z}$轴旋转的旋转算子分别定义如下：

$$R_x(\theta) \equiv e^{-\frac{i\theta X}{2}} = cos\frac{\theta}{2}I - i\,sin\frac{\theta}{2}X = \begin{bmatrix} cos\frac{\theta}{2} & -i\,sin\frac{\theta}{2} \\ -i\,sin\frac{\theta}{2} & cos\frac{\theta}{2}\end{bmatrix} \tag{3.1.5a}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = cos\frac{\theta}{2}I - i\,sin\frac{\theta}{2}Y = \begin{bmatrix} cos\frac{\theta}{2} & -sin\frac{\theta}{2} \\ sin\frac{\theta}{2} & cos\frac{\theta}{2}\end{bmatrix} \tag{3.1.5b}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = cos\frac{\theta}{2}I - i\,sin\frac{\theta}{2}Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2}\end{bmatrix}, \tag{3.1.5c}$$

很容易看到，$T = R_z(\frac{\pi}{4})$

当$\vec{\lambda}$绕$\vec{n}$轴旋转θ时，$R_{\vec{n}}(\theta) \equiv e^{-\frac{i\theta\vec{n}\vec{\sigma}}{2}} = cos\frac{\theta}{2}I - i\,sin\frac{\theta}{2}(n_xX + n_yY + n_zZ)$.

任意一个在单量子比特上的酉变换都可以写成在对量子比特上的旋转和全局相位转变的组合。

定理 3.1.1（单量子比特的 Z-Y 分解）假设U是一个作用于单量子比特的酉变换，存在实数$\alpha, \beta, \gamma, \delta$使得$U = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta)$

证明可以从酉矩阵的定义出发，得到

$$U = \begin{bmatrix} e^{i(\alpha-\frac{\beta}{2}-\frac{\delta}{2})}\cos\frac{\gamma}{2} & e^{i(\alpha-\frac{\beta}{2}+\frac{\delta}{2})}\sin\frac{\gamma}{2} \\ e^{i(\alpha+\frac{\beta}{2}-\frac{\delta}{2})}\sin\frac{\gamma}{2} & e^{i(\alpha+\frac{\beta}{2}+\frac{\delta}{2})}\cos\frac{\gamma}{2}\end{bmatrix} \tag{3.1.6}$$

从而证实定理所述分解的存在。

推论 3.1.1 存在酉算子A, B, C满足$ABC = I$，使得$U = e^{i\alpha}AXBXC$

证明取$A = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)$ $B = R_y\left(-\frac{\gamma}{2}\right)R_z\left(-\frac{\delta+\beta}{2}\right)$ $C = R_z\left(\frac{\delta-\beta}{2}\right)$

则$ABC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(-\frac{\gamma}{2}\right)R_z\left(-\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) = R_z(\beta)R_z(-\beta) = I$

$$XYX = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}i & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0 & i\\ -i & 0\end{pmatrix} = -Y$$

$$XR_y(\theta)X = X\left(cos\frac{\theta}{2}I - i\,sin\frac{\theta}{2}Y\right)X = cos\frac{\theta}{2}I + i\,sin\frac{\theta}{2}Y$$

$$= cos(-\frac{\theta}{2})\,I - i\,sin(-\frac{\theta}{2})Y = R_y(-\theta)$$

$$XBX = XR_y\left(-\frac{\gamma}{2}\right)XXR_z\left(-\frac{\delta+\beta}{2}\right)X = R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right)$$

$$AXBXC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) = R_z(\beta)R_y(\gamma)R_z(\delta)$$

$$e^{i\alpha}AXBXC = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta) = U$$

3.1.4 受控运算

CNOT 门是受控运算的原型，是拥有控制量子比特和目标量子比特双量子比特门，如下图所示。受控非门的作用为$|c\rangle|t\rangle \to |c\rangle|t \oplus c\rangle$，即如果控制量子比特置为$|1\rangle$，则目标量子比特翻转，否则目标量子比特不变。矩阵表示为：$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$.

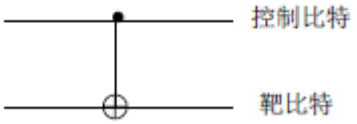


图 3.1-10 CNOT 门线路图-

受控非门的线路表示，顶上连线表示控制量子比特，底下连线表示目标量子比特。

更一般地，当U是一个单量子比特上的任意酉算子时，作用为$|c\rangle|t\rangle \to |c\rangle U^c|t\rangle$，线路如下图所示。

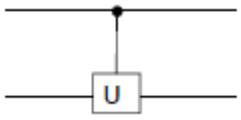
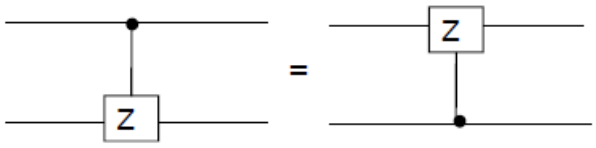


图 3.1-11 受控U运算的线路表示

很容易可以证明，如下图所示的线路等价性



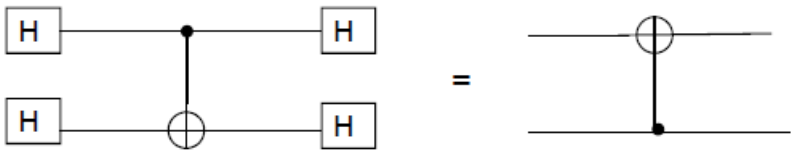


图 3.1-12 两个等价线路

下面说明如何只使用单量子比特运算和 CNOT 门实现任意单量子比特的受控-U门。

第一步是在控制量子比特控制下，在目标量子比特上相移$e^{i\alpha}$应用相位门，即作用效果为：

$$|00\rangle \to |00\rangle, |01\rangle \to |01\rangle, |10\rangle \to e^{i\alpha}|10\rangle, |11\rangle \to e^{i\alpha}|11\rangle$$

很容易可以验证

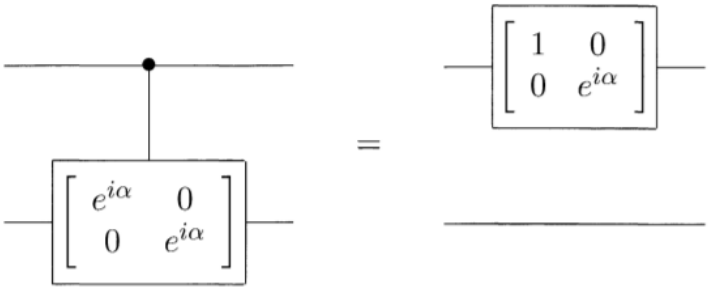


图 3.1-13 受控相移门及其双量子比特的等价线路

第二步是根据推论 3.1.1，U可以写成$U = e^{i\alpha}AXBXC$形式，其中A, B, C都是单量子比特运算，且满足$ABC = I$。设控制量子比特被置位，则$U = e^{i\alpha}AXBXC$被作用于目标量子比特；若控制量子比特没有被置位，运算$ABC = I$被作用于目标量子比特，即没有变化。因此该线路实现了受控U运算。线路如下图所示。

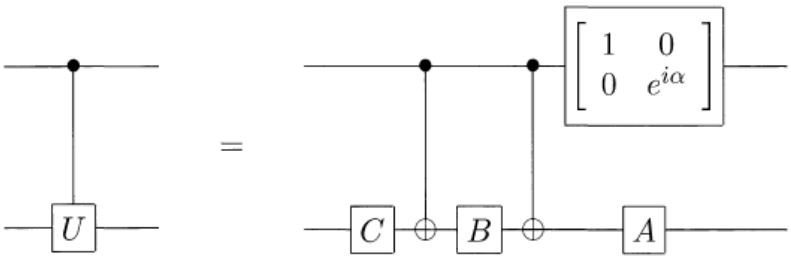


图 3.1-14 单量子比特的受控U操作的线路实现

上面都是考虑以单量子比特为控制位的情况，下面考虑用多量子比特作为控制位的情况。首先经常遇到的是可逆计算的通用门，Toffoli 门。该门使用两个控制量子比特和一个目标量子比特，只有当两个控制量子比特同时为 1，目标量子比特才翻转，否则目标量子比特不变。更一般地，设有$n + k$个量子比特，并且U是一个作用于k量子比特的酉算子，按照下式定义受控运算

$$C^n(U)|x_1x_2\cdots x_n\rangle|\phi\rangle = |x_1x_2\cdots x_n\rangle U^{x_1x_2\cdots x_n}|\phi\rangle, \tag{3.1.7}$$

其中U的指数中的$x_1x_2\cdots x_n$表示比特$x_1, x_2, \cdots, x_n$的积。只有当前n个量子比特全部为 1 时，算子U才作用于后k个量子比特；否则，不对后k个量子比特做任何操作。对该类运算，下面线路图给出给出$n = 4, k = 3$时的一个实例。

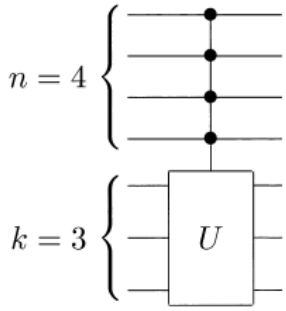


图 3.1-15 受控运算$C^4(U)$的简单线路表示

假设U是单量子比特的酉算子，且V是使得$V^2 = U$成立的酉算子，那么运算$C^2(U)$可以用下图所示线路实现。

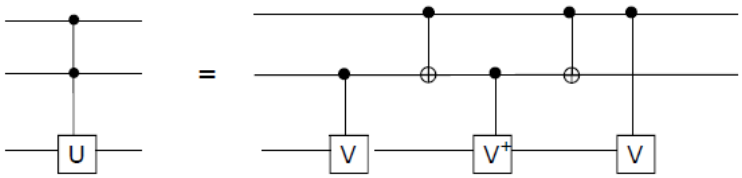


图 3.1-16 受控运算$C^2(U)$的等价线路表示

之前所知的 Toffoli 门是$C^2(U)$运算的一个特例，即$C^2(X)$。定义$V \equiv (1-i)(I+iX)/2$时，下面线路刚好对应 Toffoli 门。

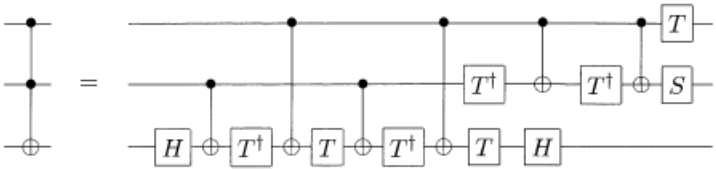


图 3.1-17 使用 Hadamard 门，相位门，CNOT 门，$\pi/8$门实现 Toffoli 门的线路图

下面考虑如何利用已有的全部门对任意的单量子比特酉算子U实现$C^n(U)$。达到该目标的一个简单线路如下图所示。下图线路使用n个控制量子比特、$n-1$个工作量子比特和 1 个目标量子比特。工作量子比特开始和结束状态均为$|0\rangle_{n-1}$，控制量子比特的初始状态为计算基中的$|c_1, c_2, \cdots, c_n\rangle$。

线路分成三段。第一段是将控制位$c_1, c_2, \cdots, c_n$以可逆的方式做“与”操作，得到乘积$c_1c_2\cdots c_n$。为此，使用第一个 Toffoli 门对c_1和c_2做“与”操作，把第一个工作量子比特变成$|c_1c_2\rangle$；使用第二个 Toffoli 门对c_1c_2和c_3做“与”操作，把第二工作量子比特变成$|c_1c_2c_3\rangle$；

如此继续使用 Toffoli 门把第n个工作量子比特变成状态$|c_1c_2\cdots c_n\rangle$。第二段线路以第n个工作量子比特置 1 为条件，执行目标量子比特上的一个U运算，即当且仅当$c_1,c_2,\cdots,c_n$全部置为 1 时，将U作用于目标量子比特上。第三段线路作用是逆转第一段的步骤，把所有的工作量子比特还原到初态$|0\rangle$，保证线路的可逆性。

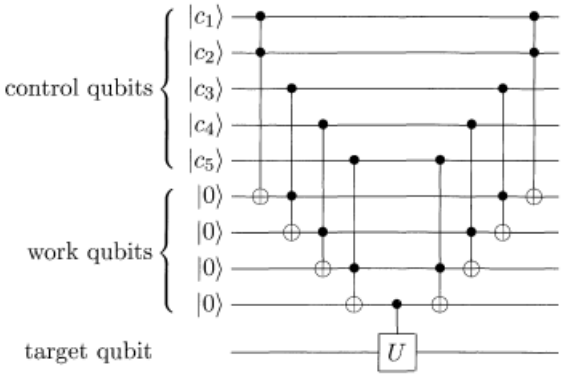


图 3.1-18 实现$C^5(U)$操作的线路图

上面所述的受控门，都是在控制位置 1 时对目标位进行作用，也可以在控制位置 0 时对目标位进行作用。例如希望实现当控制量子比特置 0 时，目标量子比特翻转的双量子比特门，线路图如下图所示。一般来讲，使用空圆圈符号表示一个量子比特置为 0，实圆圈符号表示一个量子比特置为 1.

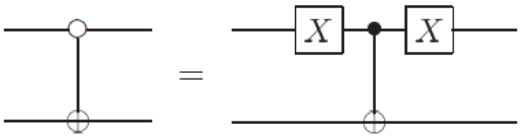


图 3.1-19 控制量子比特位 0 时，对目标量子比特作用非门的线路图

考虑更加复杂的控制条件：当第一个和第三个控制量子比特置 0，第二个量子比特置 1 时，对目标量子比特应用U门。

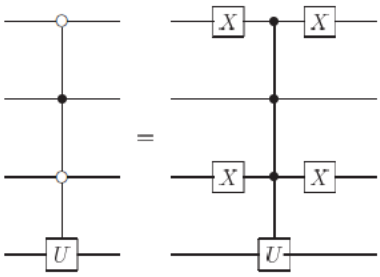


图 3.1-20 受控U操作和其等价线路

考虑允许受控非门具有多个目标量子比特的情况，如下图所示。当控制量子比特为 1 时，所有标有$\oplus$符号的量子比特都翻转，否则没有任何变化。这种线路可以应用在量子纠错线路的解码器或编码器中。

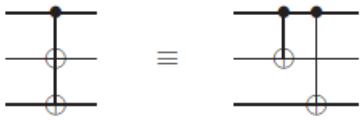


图 3.1-21 多目标量子比特的 CNOT 门

3.1.5 测量

量子线路的最后一部分就是测量，有时是隐含的。在线路中，用仪表符号表示计算基中的投影测量。在下图所示线路中没有对测量结果进一步运算，但在一般量子线路中可能会以前半部分的测量结果为条件对后半部分的线路进行改变。

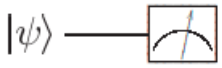


图 3.1-22 单量子比特上投影测量的符号

下面提供量子线路两个重要的原理。经典的条件运算可以用量子条件运算代替。

第一个原理是推迟测量原理（principleofdeferredmeasurement）总可以把测量步骤从量子线路的中间移到线路末端；如果测量结果被应用到线路的某部分阶段，那么经典的条件运算可以被量子条件运算代替。通常量子测量在量子线路中作为一个中间步骤，并且测量结果被用作控制后续量子门的条件。

第二个原理是隐含测量原理（principleofimplicit measurement）量子线路中任何未终结的量子连线（未被测量的量子比特）总可以假设被测量。

下面通过量子隐形传态为例来说明推迟测量原理。量子隐形传态是在发送和接收方没有量子通道连接的情况下传送量子态的一种手段。设想这样一个情形，Alice 和 Bob 很久以前相遇过并且生成了一对 EPR 对，后来每人携带 EPR 对中的一个量子比特分开并且住到距离彼此很远的地方。很多年后，Bob 躲起来。现在，要求 Alice 发送一个量子比特$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$给 Bob。Alice 不知道该量子比特的状态，即α, β的值未知，且只能给 Bob 发送经典信息。

直观上来看，Alice 不知道要发送的量子比特$|\varphi\rangle$的状态，量子力学的定律也要求他不能克隆。即便 Alice 知道状态$|\varphi\rangle$，描述这个状态也需要无穷多的经典信息。然而，量子隐形传态提供了利用 EPR 对向 Bob 发送$|\varphi\rangle$的一条途径

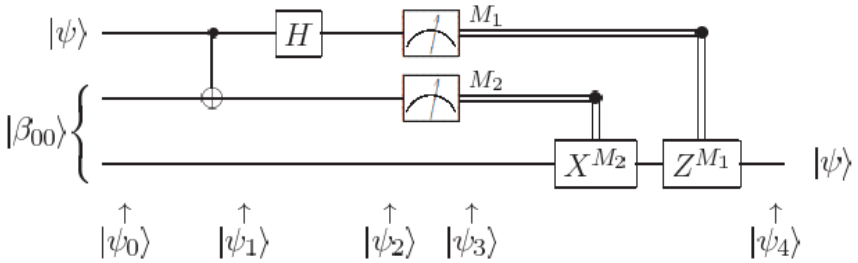


图 3.1-23 单量子比特的隐形传态线路，测量发生在线路中间

上图线路中前两个量子比特属于 Alice，第三个量子比特属于 Bob。Alice 的第二个量子比特和 Bob 的量子比特来自于同一个 EPR 对，整个过程中量子比特状态的变化情况为

$$|\Phi_0\rangle = |\Phi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)]. \quad (3.1.8a)$$

$$|\Phi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)]. \quad (3.1.8b)$$

$$|\Phi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]. \quad (3.1.8c)$$

$$= \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)$$

通过对$|\phi_2\rangle$的观察，整个表达式自然地分为四项。第一项中$|00\rangle$表示 Alice 的量子比特状态，$\alpha|0\rangle + \beta|1\rangle$表示 Bob 的量子比特状态，也就是最初的状态$|\phi\rangle$。所以可以在给定 Alice 的测量结果的情况下，读出 Bob 的测后状态：

$$00 \mapsto |\phi_3(00)\rangle \equiv [\alpha|0\rangle + \beta|1\rangle] \quad (3.1.9a)$$

$$01 \mapsto |\phi_3(01)\rangle \equiv [\alpha|1\rangle + \beta|0\rangle] \quad (3.1.9b)$$

$$10 \mapsto |\phi_3(10)\rangle \equiv [\alpha|0\rangle - \beta|1\rangle] \quad (3.1.9c)$$

$$11 \mapsto |\phi_3(11)\rangle \equiv [\alpha|1\rangle - \beta|0\rangle] \quad (3.1.9d)$$

也就是说，Bob 的量子比特所处的状态将依据于 Alice 的测量结果，这就需要 Alice 通过经典信道将测量结果M_1, M_2发送给 Bob，然后 Bob 通过对自己手中的量子比特应用量子门$Z^{M_1}X^{M_2}$从而恢复出$|\phi\rangle$。例如，Alice 测量结果为 00，则发送$M_1 = 0, M_2 = 0$这两个经典比特给 Bob，Bob 不需要做任何操作（Z^0X^0）；Alice 测量结果为 01 时，发送$M_1 = 0, M_2 = 1$给 Bob，Bob 对手中的量子比特作用X门（Z^0X^1）就可以恢复$|\phi\rangle$。

对量子隐形传态线路考虑下面问题。首先过程是否是超光速的。并没有实现超光速传输，Bob 能拿到正确的$|\phi\rangle$的前提是 Alice 需要发送经典比特M_1, M_2，然而凡是需要经典比特传输的过程一定不是超光速的。其次，考虑到 Bob 得到$|\phi\rangle$这是否违背了量子比特不可克隆定理。实际上，经过量子隐形传态线路，目标量子比特变成了$|\phi\rangle$，原始的数据量子比特变成了$|0\rangle$或者$|1\rangle$，并没有出现两个$|\phi\rangle$。最后，整个线路说明了量子力学中不同资源的可交换性。一对共享的 EPR 对和两个经典比特是至少等价于使用单个量子比特通信的资源。

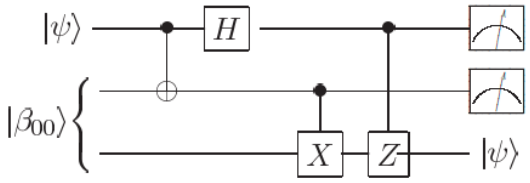


图 3.1-24 单量子比特的隐形传态线路，测量发生在线路末端

图 3.1-23 将测量结果（经典比特）作为控制条件进行经典受控条件运算，图 3.1-24 使用量子比特进行量子受控操作，测量被移到了线路末端，但是两个量子线路的整体作用相同。

假设拥有一个只含有两个量子比特的量子线路，只有第一个量子比特在线路末端被测量。那么这时测量的统计数据完全是由第一个量子比特的约化密度算子决定的。测量在量子线路中的作用是量子世界和经典世界的接口。测量一般被认为是不可逆操作，会导致破坏量子信息然后用经典信息代替。然而经过精心设计后的线路，情况并非一定如此。对于量子隐形传态和量子纠错码来说，测量结果都没有揭示任何有关要被测量的量子比特的信息。所以说为了使得一个测量变成可逆的，必须要求测量不揭示任何关于要被测量的量子比特的信息。

§3.2 量子图灵机

Church-Turing 论题断言数学概念“Turing 机可计算函数” 和直观概念 “算法可计算函数”之间的等价性，这表示 Turing 机模型为计算机科学提供了一个好的基础。量子计算机也服从 Church-Turing 论题，即量子计算机可以计算的函数类与 Turing 机可计算的函数类相同。

图灵机是计算机的一种抽象原型，计算机主要包括控制器、存储器、运算器等部分，其特征为：⑴基本信息单位是离散的；⑵有存储器，容量至多是可数无限；⑶有运控部件，执行程序指令。⑷有指令系统，完成传递信息、加工信息和决定指令执行的顺序。

3.2.1 波斯特-图灵机

波斯特-图灵机的结构如图 3.2-1 所示

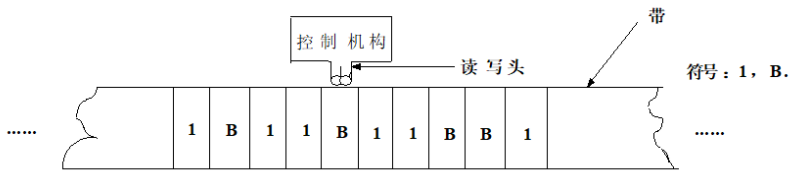


图 3.2-1 波斯特-图灵机的结构

波斯特-图灵机的基本指令包括 WRITE 1、WRITE B、RIGHT、LEFT、TO A IF READ 1 和 TO A IF READ B 六部分，其工作过程如下：

1) 带上有限符号序列：$x_1x_2\ldots x_n, x \in \{1, B\}^*$;

2) 读写头的位置：

$$x_1x_2\cdots\underset{\downarrow}{x_k}\cdots x_n$$;

3) 将执行的指令：正整数 p 表示将执行的指令编号为 p，$\omega = (p, x, k)$为图灵机某一时刻的格局，$\omega_0 = (1, x_0, 1)$表示从第一条语句开始，将读写头放于第一位且初始输入为x_0，执行基本指令后格局的改变为

$$(p, x, k) \vdash_T (p', x', k')$$

其中$p' = p + 1$（或 r，即转移到 r 行）（T 为转移），x'中某位改变（写）或向某一边扩展。

波斯特-图灵机程序举例：

初始信息：$x_0 = 111B11$

计算过程：

ω_0 : (1, 1 1 1 B 1 1, 1) RIGHT

ω_1 : (2, 1 1 1 B 1 1, 2) TO A IF READ 1

ω_2 : (1, 1 1 1 B 1 1, 2) RIGHT

ω_3 : (2, 1 1 1 B 1 1, 3) TO A IF READ 1

ω_4 : (1, 1 1 1 B 1 1, 3) RIGHT

ω_5 : (2, 1 1 1 B 1 1, 4) TO A IF READ 1

ω_6 : (3, 1 1 1 B 1 1, 4) WRITE 1

ω_7 : (4, 1 1 1 1 1 1, 4) RIGHT

ω_8 : (5, 1 1 1 1 1 1, 5) TO B IF READ 1

ω_9 : (4, 1 1 1 1 1 1, 5) RIGHT

ω_{10} : (5, 1 1 1 1 1 1, 6) TO B IF READ 1

ω_{11} : (4, 1 1 1 1 1 1, 6) RIGHT

ω_{12} : (5, 1 1 1 1 1 1 B, 7) TO B IF READ 1

ω_{13} : (6, 1 1 1 1 1 1 B, 7) LEFT

ω_{14} : (7, 1 1 1 1 1 1 B, 6) WRITE B

$$\omega_{15}:\ (8,\ 1\ 1\ 1\ 1\ 1\ \underset{\lceil}{B}\ B,\ 7) \qquad \text{LEFT}$$

$$\omega_{16}:\ (9,\ 1\ 1\ 1\ 1\ 1\ \underset{\lceil}{B}\ B,\ 5) \qquad \text{WRITE B}$$

$$\omega_{17}:\ (10,\ 1\ 1\ 1\ 1\ \underset{\lceil}{B}\ B\ B,\ 5) \qquad \text{LEFT}$$

$$\omega_{18}:\ (11,\ 1\ 1\ 1\ 1\ \underset{\lceil}{B}\ B\ B,\ 4)$$

编号 11 的指令不存在，ω_{18}为终止格局，图灵机停机，计算结果为 111BBB.

3.2.2 图灵机可计算函数

定义 3.2.1（图灵机可计算函数）称定义域内可停机的函数为部分可计算函数；称全函数且部分可计算的$y = f(x_1, \dots, x_n)$为可计算函数。

若函数$y = f(x_1, \dots, x_n)$是部分可计算的，则必存在图灵机 T 和一组输入$x = (x_1, \dots, x_n)$使$f(x)$有定义且 T 对x工作后必得一计算结果y，记为$F_T(x) = y$，即

$$\begin{cases} y = F_T(x), & \text{当 f(x)有定义；} \\ F_T(\text{x})\text{无效}(\text{对 x 永不停机}), & \text{当 f(x)无定义.} \end{cases} \tag{3.2.1}$$

引理 3.2.1 存在可计算函数$q: \sum^* \to \sum^*$,对任意串 W，$q(W)$是图灵机P_W的描述，P_W打印出 W 后停机。

定理 3.2.1（递归定理）设 T 是计算函数$t: \sum^* \to \sum^*$.的一个图灵机，则存在计算函数$r: \sum^* \to \sum^*$,的一个图灵机 R，使得对每个 W 有$r(W) = t(\langle R\rangle, W)$.

考虑下面的句子：

打印下面引号内语句的两个副本，在第二个副本上加引号：

“打印下面引号内语句的两个副本，在第二个副本上加引号：”

定义 3.2.2（A+B 复合系统）能打印自身（描述）的图灵机 SELF。

设 A 是一个能打印出$\langle B\rangle$的图灵机，则 A 的描述只能在构造出 B 之后，所以 B 不可以是一个能直接打印出$\langle A\rangle$的图灵机，而只能是根据数据带上 A 打印的数据（$\langle B\rangle$）计算出$\langle A\rangle$，再打印出来。

3.2.3 通用图灵机

定义 3.2.1（五重组图灵机）图灵机$T = (s, Q, \delta, q_0)$. 其中s表示纸带上的符号集合；Q表示机器状态集合；δ为$Q \times s \to s \times M \times Q$的映射，即刻画了控制表的转换函数，例如$q_i s_j s_k M q_l \Leftrightarrow \delta(q_i, s_j) = (s_k, M, q_l)$；$q_0 \in Q$表示开始状态

定义 3.2.3（通用图灵机）能够模拟其他任何图灵机的图灵机。

构造通用图灵机的方法如下：

1) 对所有图灵机进行编码，如$CCC1RBC11R1CC11RBC111R1CC0C0CCC$;

2) 在输入带上记录专用图灵机的转移函数，并用第二条带上的符号标识状态起点和数据起点。

3) 通用图灵机（双带）的初始输入：

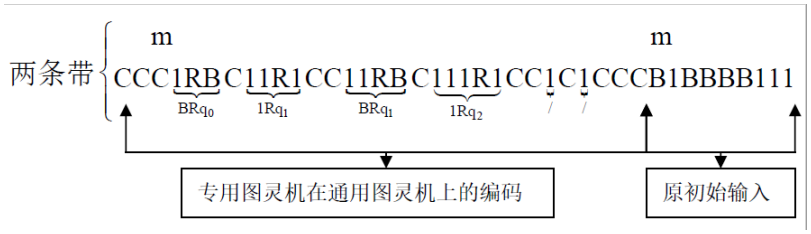


图 3.2-2 通用图灵机（双带）初始输入

4) 令 M 任一图灵机，T_M是与 M 相关联的图灵数，则在二进制表示后面接一个空白符号，再在带子的剩余部分跟上任意符号串 x，通用图灵机的输出结果即为机器 M 把 x 作为输入时的输出。

由图灵机编码方案的存在可知只能有可数无穷多不同的图灵机，只能有可数无穷多不同的递归函数，并且几乎所有数论函数都不可计算。

3.2.4 图灵停机问题

图灵机停机问题是指对于任意一个图灵机 T 和初始输入 x，是否存在一个图灵机 M，它能判定 T 对输入 x 是否停机。针对这一问题，有以下定理：

定理 3.2.2 设$L = \{x_i | F_{T_i}(x_i)$无意义$\}$，则 L 非空（因为至少与对任何输入都为死循环的图灵机编号相同的数据就是 L 的元素），且不存在有且仅对 L 中的元素停机的图灵机。

其中T_i是对图灵机的编号，x_i为初始输入编号，$F_T(x)$为 T 对 x 的工作结果。定理 3.2.2 可利用反证法证明，具体证明留给读者练习。

定理 3.2.3 图灵停机问题是不可判定的。

证明假设有T_s能判定任何 T 对任何 x 是否停机，现构造图灵机 M：

1) 由x找出i，$x_i = x$；

2) 由i找出T_i；

3) 模拟T_s判定T_i对x_i是否停机的过程；

4) 当“T_i对x_i不停机”时，令 M 停机，反之亦反。

上述构造的 M 称为有且仅对 L 中任何元素均停机的图灵机，与定理 3.2.2 矛盾，假设不成立。

3.2.5 非确定图灵机

非确定性是一个有用的概念，已经对计算理论产生了巨大的影响，五元组$\{Q,\Sigma,\delta,q_0,F\}$称为非确定型有穷自动机（NFA）,例如 NFA N_1:

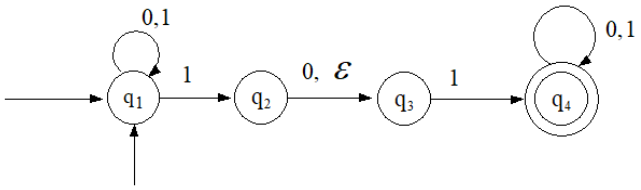


图 3.2-3 NFAN_1

NFA N_1在读入“1”后，把自己分裂成两个备份并且并行地执行所有的可能性；如果下一个输入符号不出现在它所处的状态射出的任何箭头上，则机器的这个备份和与其相关联的计算分支一块死掉；射出箭头上标有ε则不用读任何输入，机器分裂成多个备份，有一个标记ε的箭头就有一个备份跟踪，还有一个备份停留在当前的状态。

非确定型图灵机的非确定性与非确定型有穷自动机的非确定性相同，有关定理如下：

定理 3.2.4 每个非确定型图灵机都有一个与之等价的确定型图灵机。

定理 3.2.5 设$t(n)$是一个函数，有$t(n)\geq n$，则每一个$t(n)$时间的非确定型单带图灵机都与一个$2^{O(t(n))}$时间的确定型单带图灵机等价。

3.2.6 概率图灵机

概率算法中运用的也是一种“非确定型”的图灵机，即概率图灵机（PTM），它与前述“非确定型图灵机”并不相同。

计算模型中引入随机性，不能从本质上改变计算模型计算能力，可计算的函数类不因模型中引入的随机性而有所变化。

定义 3.2.4（概率图灵机）

- 每一非确定步称为掷硬币步，有且只有两个合法的下次动作；
- 每一掷硬币步，按下述方式把概率赋给 M 对输入ω的每一个计算分支 b，

  $\Pr[b]=2^{-k}$其中 k 是分支 b 中出现掷硬币的步数；
- 定义 M 接受ω的概率Pr[M 接受ω]$=\sum_b \Pr[b]$（b 是接受分支）。

当概率图灵机识别语言时，对于$0\leq\varepsilon<1/2$，如果$\omega\in A$蕴含Pr[M 接受ω]$\geq 1-\varepsilon$，或者$\omega\notin A$蕴含Pr[M 接受ω]$\geq 1-\varepsilon$（此公式错）则称 M 以错误概率ε识别语言 A.

定义 3.2.5（BPP）多项式时间概率图灵机以错误概率 1/3 识别的语言类。

定理 3.2.6 设M_1是一台错误概率为$\varepsilon<1/2$的多项式时间概率图灵机，则对于任意的多项式$poly(n)$，存在与M_1等价的错误概率为$2^{-poly(n)}$的多项式时间概率图灵机M_1.

3.2.7 可逆图灵机

对于单带确定型图灵机而言，“可逆”是指每一个格局c_i都可以由后一个格局c_{i+1}唯一确定。可以证明，如果图灵机$M=\{\Sigma, \mathrm{Q}, \mathrm{q}_0, \delta\}$是可逆的，满足$M(c)=c'$，则一定存在图灵机$M'=\{\Sigma, \mathrm{Q}, \mathrm{q'}_0, \delta'\}$满足$M(c')=c$.

思考：用转移函数所满足的关系给出图灵机可逆的充要条件。

1973 年，Bennett 证明，如果f是单带图灵机$t(n)$时间可计算函数，则存在图灵机三带可逆图灵机，额外消耗常数时间，计算出下面结果：$a \to (a, j(a), f(a))$,其中$j(a)$是”garbage”保存了计算的历史信息，以保证可逆性。Bennett 最初的方案空间代价十分巨大，但他同时给出计算垃圾可以用可逆计算的方式清除。

1989 年，Bennett 证明，任意图灵机可以被一个可逆图灵机模拟，该可逆图灵机在时间上只是增加常数的额外消耗，在空间上也只是占用平方倍的资源。

考虑 1997 年 Vazirani 的可逆图灵机模型。设 M 是单带图灵机，可计算f，M’是可逆图灵机，可计算$x \to (x, f(x))$，M’包含一条记录历史信息的附加带。可以证明，M 的每一步可以由 M’用两步来模拟：第一步是将 M 的当前状态和所读符号写入附加带；第二步同 M 的操作。这样的计算可以在$2t(n)$时间内完成，$t(n)$是 M 的计算时间,空间需求增加到$t(n)+s(n)$，其中$s(n)$是 M 的空间需求，空间资源需求可以被压缩到$O(s(n)\lg(t(n)))$，代价是计算时间增加到$t^{1+\varepsilon}(n)$，ε是任意小量。

3.2.8 量子图灵机

定理 3.2.7 存在一个 Orcale 和一个在量子计算机上通过调用该 Oracle 可以用多项式时间以有限错误概率求解的问题，在任何概率图灵机上以有限错误概率求解该问题（调用该 Oracle），都存在无限多长度为 n 的输入需要指数时间的运算（至少$2^{n/2}$步）。

这一定理表明，在某些环境下，QTM 比 PTM 更强大。这一结果涉及的问题有一定的人为性。沿着这一思路取得的重要进展是 Shor（1994）做出的大整数因子分解和计算有限域上离散对数的有效量子算法，这两个问题的难解性在公钥密码体制的算法设计中具有重要意义。

图灵机的量子形式在量子计算机理论中将扮演基础性的角色，正如经典图灵机在经典可计算性理论和复杂性理论中所起的作用一样。不过，从构造具体的量子算法或建造样机而言，量子线路模型更具有技术意义。

定义 3.2.6 一个（单带）量子图灵机$M=\{\Sigma, \mathrm{Q}, \mathrm{q}_0, q_f, \delta\}$（简写为 QTM），可以类似于 PTM 的定义方法，初态q_0，终态q_f，转移函数为：$\delta: Q \times \Sigma \times \Sigma \times Q \times \{\leftarrow \downarrow \rightarrow\} \longrightarrow C$.这里要求$\delta$能保证 M 的量子演化是酉的，不要求酉条件时的量子图灵机为准量子图灵机（quasi-QTM, qOTM）。

1997 年 Hirvensalo 证明，如果准量子图灵机满足下述强合式条件，其演化的幺正性将得到保证。

定义 3.2.7（强合式 qQTM） qQTM$M=\{\Sigma, \mathrm{Q}, \mathrm{q}_0, q_f, \delta\}$如果满足下述条件将被称为强合式的:

1) 局域概率条件，对于任意$(q_1, \sigma_1) \in Q \times \Sigma$，有

$$\sum_{(\sigma,q,d)\in\Sigma\times Q\times\{\leftarrow\downarrow\rightarrow\}}|\delta(q_1,\sigma_1,\sigma,q,d)|^2=1 \qquad (3.2.2)$$

2) 可分离条件 I，对于集合$Q\times\Sigma$中任意两个不同的对$(q_1,\sigma_1),(q_2,\sigma_2)$，有

$$\sum_{(\sigma,q,d)\in\Sigma\times Q\times\{\leftarrow\downarrow\rightarrow\}}\delta^*(q_1,\sigma_1,\sigma,q,d)\delta(q_2,\sigma_2,\sigma,q,d)=0 \qquad (3.2.3)$$

3) 可分离条件 II，集合$\Sigma\times Q\times\{\leftarrow\downarrow\rightarrow\}$中任意两元素$(q,\sigma,d)$和$(q',\sigma',d')$，如果满足$(q,\sigma,d)\neq(q',\sigma',d')$，则有

$$\sum_{(\sigma,q,d)\in\Sigma\times Q\times\{\leftarrow\downarrow\rightarrow\}}\delta^*(q_1,\sigma_1,\sigma,q,d)\delta(q_1,\sigma_1,\sigma',q',d')=0 \qquad (3.2.4)$$

4) 可分离条件 III，对于任意$(q_1,\sigma_1,\sigma_1'),(q_2,\sigma_2,\sigma_2')\in Q\times\Sigma\times\Sigma$及$d_1\neq d_2\in\{\leftarrow\downarrow\rightarrow\}$，有

$$\sum_{q\in Q}\delta^*(q_1,\sigma_1,\sigma',q,d_1)\delta(q_2,\sigma_2,\sigma_2',q',d_2)=0 \qquad (3.2.5)$$

定义 3.2.8 QTM 的一个计算是叠加态$c_0,c_1,\ldots$的一个序列，这里c_0为初始格局，对于$i\geq 1$，有$c_i=U_M(c_{i-1})$，或c_i是通过测量从c_{i-1}得到的。

定义 3.2.9（Unidirectional 量子图灵机）一个 QTM $M=\{\Sigma,\mathrm{Q},\mathrm{q}_0,q_f,\delta\}$被称为 Unidirectional（uQTM），如果每当$\delta(q_1,\sigma_1,\sigma_1',q,d_1)\neq 0\neq\delta(q_2,\sigma_2,\sigma_1',q,d_2)$，都有$d_1=d_2$，即读写头的进入方向由将进入的状态唯一确定，不受其他变量的影响，或者说，同一内部状态由同一方向的移动生成。

定理 3.2.9 任意 QTM 可以被 uQTM 模拟，并且减速因子不大于 5.

定义 3.2.10QTM M'称为以减速函数$f:N\to N$和精度ε模拟 QTM M, 如果下述关系成立: M 对输入 x 作用 t 步后，产生分布 D，M'对 x 作用$f(t)$步后产生分布D'，则$|D-D'|\leq\varepsilon$.

定理 3.2.10 任何 QTM 可以在常数减速意义下被实振幅 QTM 模拟。

定义 3.2.11（ε-接近）两个 QTM 是ε-接近的，如果它们具有相同的状态集和符号集，并且任何一对相应的振幅不超过ε.

第 4 章量子算法

可以认为量子并行计算与经典随机化方法很相近。差别在于：在经典概率计算机上，不同概率分支总是相互排斥的，而在量子计算机上，不同的叠加分量却可能通过干涉而给出函数的某种全局性质。

许多量子算法设计的本质在于：精心选择函数和最终变换，以便有效地确定有关函数的有用的全局信息。这种全局信息在经典计算机上是不能有效得到的。

§4.1 量子并行性与早期量子算法

量子并行性使得量子计算机可以一次同时对多个不同的x同时计算函数值$f(x)$。在经典中，对布尔函数$f:\{0,1\}\mapsto\{0,1\}$计算$f(0)\ f(1)$需要做两次计算。然而，由于量子并行的性质，只需要一次计算便可以同时得到$f(0)\ f(1)$。

例子：构造计算函数f的量子线路U_f，$U_f:|x,y\rangle\mapsto|x,y\oplus f(x)\rangle$

在输入为$|+\rangle|0\rangle$，线路功能为：

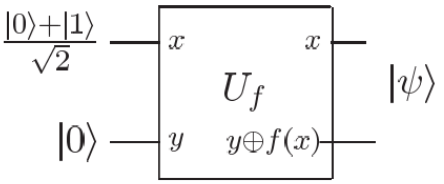


图 4.1-1 量子线路U_f在输入为$|+\rangle|0\rangle$时的线路功能

以叠加的形式输入到量子线路中，将会给出叠加的输出，这是后面 Shor 大数分解算法、Grover 搜索算法的基础。下面给出几个应用量子并行性的算法。

4.1.1 Deutsch 算法

Deutsch 问题：给定$f:\{0,1\}\mapsto\{0,1\}$，计算$f(0)\oplus f(1)$。

解决 Deutsch 问题的经典算法步骤为：①计算$f(0)$；②.计算$f(1)$；③上面两步结果相加一共需要经过 3 步计算。

解决 Deutsch 问题还可以采取如图 4.1-2 的量子算法：

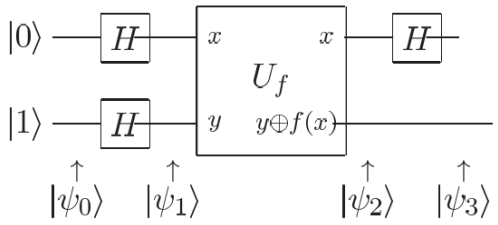


图 4.1-2 量子线路U_f

线路状态变化的详细过程如下所示

$$|\psi_0\rangle = |01\rangle,\ |\psi_1\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle-|1\rangle}{\sqrt{2}},\ |\psi_2\rangle = \begin{cases} if\ f(0) = f(1), \pm\frac{|0\rangle+|1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle-|1\rangle}{\sqrt{2}} \\ if\ f(0) \neq f(1), \pm\frac{|0\rangle-|1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{cases}$$

$$|\psi_3\rangle = \begin{cases} if\ f(0) = f(1), \pm|0\rangle \cdot \frac{|0\rangle-|1\rangle}{\sqrt{2}} \\ if\ f(0) \neq f(1), \pm|1\rangle \cdot \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{cases},$$

即，$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle \cdot \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

只需要 1 步计算就可完成算法目标。

4.1.2. Deutsch-Jozsa 算法

Deutsch-Jozsa 问题：对于给定的函数$f: x \in \{0,1\}^n \to \{0,1\}$，要么是常函数要么平衡函数。判断函数$f(x)$是常函数还是平衡函数。常函数和平衡函数定义如下：

常函数：$\forall x \in \{0,1\}^n, f(x) = b$；

平衡函数：$\forall x \in \mathcal{H}, f(x) = 0; \forall x \notin \mathcal{H}, f(x) = 1; \mathcal{H} \in \{0,1\}^n, |\mathcal{H}| = 2^{n-1}$

解决 Deutsch-Jozsa 问题经典算法在最坏情况下至少需要做$2^{n-1}+1$次访问才能判断出函数是常函数还是平衡函数。

下面考虑解决 Deutsch-Jozsa 问题的量子算法。Deutsch-Jozsa 算法是 Deutsch 算法的拓展版本。与 Deutsch 算法的不同之处只在于工作寄存器变成了n位，下图中斜杠/线表示通过此线的是一组量子比特。

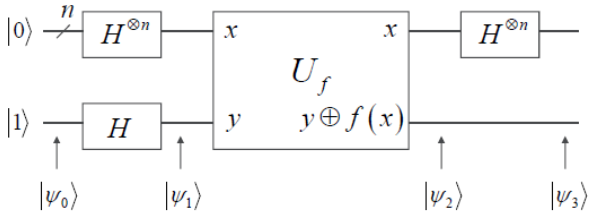


图 4.1-3 Deutsch-Jozsa 算法

算法执行过程中状态的变化情况为：

$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle.$

$\to |\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right],$

$\to |\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right],$

$$\to |\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x\cdot z+f(x)}|z\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

其中，

$$H^{\otimes n}|x_1,\dots,x_n\rangle=\frac{\sum_{z_1,\dots,z_n}(-1)^{x_1z_1+\cdots+x_nz_n}|z_1,\dots,z_n\rangle}{\sqrt{2^n}} \tag{4.1.1a}$$

$$H^{\otimes n}|x\rangle=\frac{\sum_z(-1)^{x\cdot z}|z\rangle}{\sqrt{2^n}} \tag{4.1.1b}$$

考虑对x的求和：

①如果$f(x)$是常数函数，则和为$(-1)^{f(x)}(\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{x\cdot z})=(-1)^{f(x)}\delta_{z,0}$，这是因为$z\neq 0$时，$(-1)^{x\cdot z}$有半数等于$+1$，半数等于$-1$，所以测量这个寄存器将以概率 1 得到$|z=0\rangle$。

②如果$f(x)$是平衡函数，对$z=0$的态，有$\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot z}=0$，这是因为函数$(-1)^{f(x)}$对$x=0$到$x=2^n-1$求和时有半数等于$+1$，半数等于$-1$，所以测量这个寄存器将以概率 0 得到$|z=0\rangle$。

所以可以将 Deutsch-Jozsa 算法总结如下：

输入对$x\in\{0,\dots,2^n-1\}$和$f(x)\in\{0,1\}$进行变换，已知$f(x)$对所有的x是或者是常数或者是平衡的（对所有可能的x一半取 1，另一半取 0）。

输出当且仅当f是常数，输出为 0。

运行时间计算U_f一次，总是成功的。

过程

（1）状态初始化：$|0\rangle^{\otimes n}|1\rangle$

（2）用 Hadamard 门产生叠加：

$$\rightarrow\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

（3）用U_f计算函数f：

$$\sum_x\frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \tag{4.1.2}$$

（4）进行 Hadamard 变换：

$$\sum_x\sum_x\frac{(-1)^{f(x)+x\cdot z}|z\rangle}{2^n}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \tag{4.1.3}$$

（5）测量最终输出z

但是算法也有一些局限性。首先，Deutsch 问题不是一个很重要的问题，没有什么实际的应用价值。其次，在某些方式上，经典和量子算法完全是没有任何的可比性。最后，如果 Alice 拥有概率经典计算机，那么她可以随机选择几个x，然后让 Bob 帮她计算$f(x)$，这种情况下，她将以很高的概率来判断f是一个常函数还是平衡函数。

4.1.3 Bernstein-Vazirani 算法

Bernstein-Vazirani 问题：设a是一个n位串，假设量子黑箱可以计算函数f_a: $f_a(x) = a \cdot x$，求a.

经典算法要确定a必须运行黑箱n次，通过求解n元现行方程组得到a。然而，Bernstein 和 Vazirani 设计的如下量子算法，只需要运行黑箱一次。Bernstein-Vazirani 算法的线路图与 Deutsch-Jozsa 算法线路图(图 4.1-3)相同。

$$\begin{aligned} U_{f_a}&:\left[|x\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right] \\ &=(-1)^{f_a}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \\ &=(-1)^{a\cdot x}|x\rangle\tfrac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \end{aligned} \tag{4.1.4}$$

$$U_{f_a}[H^{\otimes(n+1)}|0\rangle^n|1\rangle]=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{a\cdot x}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

$$\xrightarrow{\text{前}n\text{ 位}H^{\otimes n}}\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{a\cdot x}\sum_{y=0}^{2^n-1}(-1)^{y\cdot x}|y\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

考虑对变量的求和，由于$\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{a\cdot x}\sum_{y=0}^{2^n-1}(-1)^{y\cdot x}=\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{(a\oplus y)\cdot x}=\delta_{a,y}$

即：

$$\begin{aligned} &\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{a\cdot x}\sum_{y=0}^{2^n-1}(-1)^{y\cdot x}|y\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \\ &=\textstyle\sum_{y=0}^{2^n-1}\delta_{a,y}\,|y\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)=|a\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \end{aligned} \tag{4.1.5}$$

测量前n位寄存器将以概率 1 得到a.

4.1.4 Simon 算法

Simon 问题：对函数f: $\{0,1\}^n \to \{0,1\}^m$是$2 \to 1$的同态，且对于确定的$a \in \{0,1\}^n$，有$f(x \oplus a) = f(x)$，求a.

经典算法求解a最坏情形需要$2^{n-1}+1$次运算，然而使用量子黑箱只需要n次运算就可以求得a。Simon 算法的线路图如图 6.1-5 所示

$$U_f\left[\tfrac{1}{\sqrt{2^n}}\textstyle\sum_{x=0}^{2^n-1}|x\rangle\,|0\rangle\right]=\tfrac{1}{\sqrt{2^n}}\textstyle\sum_{x=0}^{2^n-1}|x\rangle\,|f(x)\rangle \tag{4.1.6}$$

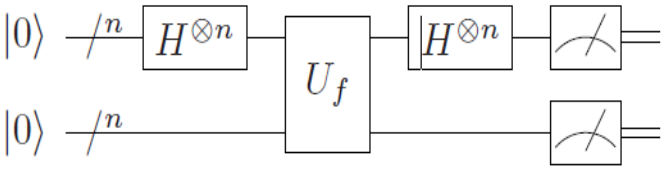


图 4.1-4Simon 算法线路图

测量第二个寄存器，设测量结果是$f(x_0)$。由于只有x_0 和x_0+a被映射为$f(x_0)$，所以第一个寄存器态为$\frac{1}{\sqrt{2}}(|x_0\rangle+|x_0\oplus a\rangle)$。

$$H^{\otimes n}\frac{1}{\sqrt{2}}(|x_0\rangle+|x_0\oplus a\rangle)$$

$$=\frac{1}{\sqrt{2^{n+1}}}\sum_{y=0}^{2^n-1}\left[(-1)^{x_0\cdot y}+(-1)^{(x_0\oplus a)\cdot y}\right]|y\rangle$$

$$=\frac{1}{\sqrt{2^{n+1}}}\sum_{y\cdot a=0}(-1)^{x_0\cdot y}|y\rangle \tag{4.1.7}$$

测量第一个寄存器，随机得到一个$|y\rangle$，满足$a\cdot y=0$。重复算法可以求得$n-1$个线性独立的y值，通过解方程组

$$\begin{cases} y_1\cdot a=0 \\ y_2\cdot a=0 \\ \quad\vdots \\ y_{n-1}\cdot a=0 \end{cases} \tag{4.1.8}$$

可以求得a，即使考虑到两次运行黑箱可能得到同一个y值，或者是与已得y值线性相关的值，重复运行黑箱的次数仍是n的多项式，可知量子算法获得了指数加速的效果。

§4.2 量子傅里叶变换

目前在量子计算中最新奇的发现就是量子计算机可以执行一些在经典计算机中不可行的任务。比如$n-bit$大整数的质因子分解问题，经典中已知的最好的算法—数域筛法，执行过程需要$e^{\Theta(n^{1/3}\,log^{2/3}\,n)}$次操作，是一个指数级别的算法。所以在经典计算机中，可以认为分解是不可行的。然而量子算法却可以只执行$O(n^2\,log\,n\,loglog\,n)$次操作就完成大整数的分解。也就是说，相比于经典中已知的最好的算法，量子计算机可以实现指数加速。实际上，量子傅里叶变换是一个执行量子力学幅度变换的高效量子算法。

解决一个问题最有用的方法就是把它变成一些其他的已知解的问题。量子计算的很大发现是这样的计算在量子计算机中可以变得更快。

（1）离散傅里叶变换（Discrete Fourier Transform）

输入：长度为N的一个复数向量$x_0,\cdots,x_{N-1}$

输出：长度为N的一个复数向量$y_0,\cdots,y_{N-1}$，$y_k \equiv \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} x_j e^{2\pi ijk/N}$

（2）量子傅里叶变换（Quantum Fourier Transform）

输入：$|j\rangle$

输出：$\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle$

对于任意态$\sum_{j=0}^{N-1} x_j|j\rangle$，有：

$$\sum_{j=0}^{N-1} x_j|j\rangle \xrightarrow{QFT(N)} \sum_{j=0}^{N-1} x_j \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle$$

$$= \sum_{j=0}^{N-1}\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} x_j e^{2\pi ijk/N}|k\rangle = \sum_{j=0}^{N-1} y_k|k\rangle \qquad (4.2.1)$$

酉性：只需要证明$|j_1'\rangle = QFT(N)|j_1\rangle$和$|j_2'\rangle = QFT(N)|j_2\rangle$满足$\langle j_1'|j_2'\rangle = \delta_{j_1',j_2'}$即可。

$N = 2^n$，$n$qubit 的量子计算机的N个基为$|0\rangle$，…，$|2^n-1\rangle$，对j使用二进制表示有$j = j_1 j_2 \cdots j_n$，有：

$$j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0,\ 0.j_l j_{l+1}\ldots j_m = \frac{j_l}{2} + \frac{j_{l+1}}{4} + \cdots + \frac{j_m}{2}^{m-l+1} \qquad (4.2.2)$$

量子傅里叶变换可以有如下的乘积表示：$|j_1,\cdots j_n\rangle \rightarrow \frac{(|0\rangle+e^{2\pi i 0.j_n}|1\rangle)(|0\rangle+e^{2\pi i 0.j_{n-1}j_n}|1\rangle)\cdots(|0\rangle+e^{2\pi i 0.j_1 j_2\cdots j_n}|1\rangle)}{2^{n/2}}$

证明如下：

$$\begin{aligned}
|j_1,\cdots j_n\rangle &\rightarrow \frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n}|k\rangle \\
&= \frac{1}{2^{n/2}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1} e^{2\pi ij\left(\sum_{l=1}^{n} k_l 2^{-l}\right)}|k_1\ldots k_n\rangle \\
&= \frac{1}{2^{n/2}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}\bigotimes_{l=1}^{n} e^{2\pi ijk_l 2^{-l}}|k_l\rangle \\
&= \frac{1}{2^{n/2}}\bigotimes_{l=1}^{n}\left[\sum_{k_l=0}^{1} e^{2\pi ijk_l 2^{-l}}|k_l\rangle\right] \\
&= \frac{1}{2^{n/2}}\bigotimes_{l=1}^{n}\left[|0\rangle + e^{2\pi ijk_l 2^{-l}}|1\rangle\right] \\
&= \frac{\left(|0\rangle+e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle+e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle+e^{2\pi i 0.j_1 j_2\cdots j_n}|1\rangle\right)}{2^{n/2}}
\end{aligned} \qquad (4.2.3)$$

具体过程如下图所示，其中$R_k \equiv \begin{bmatrix}1 & 0\\ 0 & e^{2\pi i/2^k}\end{bmatrix}$

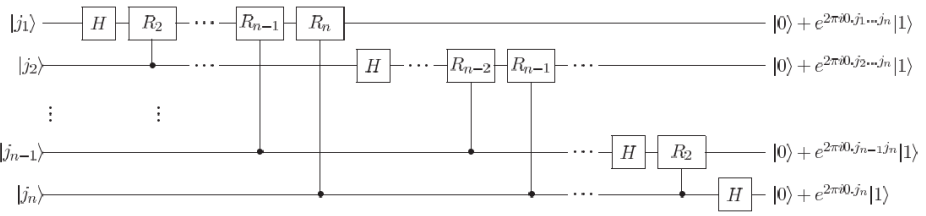


图 4.2-1 量子傅里叶变换的有效线路，这里在线路末端省略了逆转量子比特顺序的交换门和输出的$\frac{1}{\sqrt{2}}$归一化因子

图 4.2-2 所示给出 3qubit 的量子傅里叶变换。

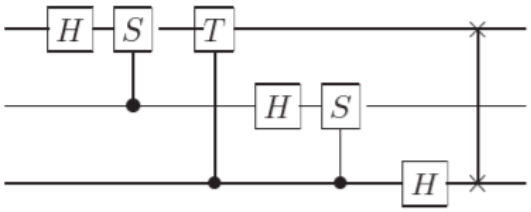


图 4.2-2 三量子比特傅里叶变换线路图

设$\omega = e^{2\pi i/8} = \sqrt{i}$，量子傅里叶变换的矩阵表示为

$$\frac{1}{\sqrt{8}}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & 1 \end{bmatrix} \tag{4.2.4}$$

分析：

根据线路的构造过程，因为每个门都是酉操作，所以量子傅里叶变换是酉变换，现在来说明线路使用的门的个数。对第一个 qubit，做 1 次 Hadamard 变换，做$n-1$次R_k操作，一共需要$(n-1+1)$个门；对第二个 qubit，做 1 次 Hadamard 变换，做$n-2$次R_k操作，一共需要$(n-2+1)$……依次类推，线路的实现一共需要$n+(n-1)+\cdots+1=n(n+1)/2$个门。

在线路末端，为了实现目标，还需要进行比特交换，最多需要$n/2$次交换，每个交换可以使用三个受控非门来实现。因此这个线路为执行量子傅里叶变换提供了一个$\Theta(n^2)$的算法。其次，经典中类似于快速傅里叶变换这种计算离散傅里叶变换的最好的算法，需要$\Theta(n2^n)$个门。也就是说，量子傅里叶变换实现了相对于经典傅里叶变换的指数加速。

然而，即便傅里叶变换在现实生活的数据处理中是一个很重要的应用，但是目前还没有量子傅里叶变换的实际应用。原因是多方面的。量子态的幅度不能通过测量得到，因此没有办法确定要进行傅里叶变换的初始状态的幅度，而且，一般上没有方法能制备要进行傅里叶变换的初始状态。

§4.3 量子傅里叶变换的应用

4.3.1 相位估计

量子傅里叶变换是相位估计的核心步骤，也就意味着是很多量子算法的核心步骤。

问题：酉算子U有一个本征值为$e^{2\pi i\varphi}$的本征向量$|u\rangle$，且φ未知

目标：估计φ

假定：拥有一个可获得的黑盒：准备状态$|u\rangle$，执行受控操作$U^{2^j}j \geq 0$

说明：使用两个寄存器。第一个寄存器存放t个初始状态处于$|0\rangle$的 qubit；第二个寄存器存放$|u\rangle$

过程：

（1）第一阶段运行下图线路

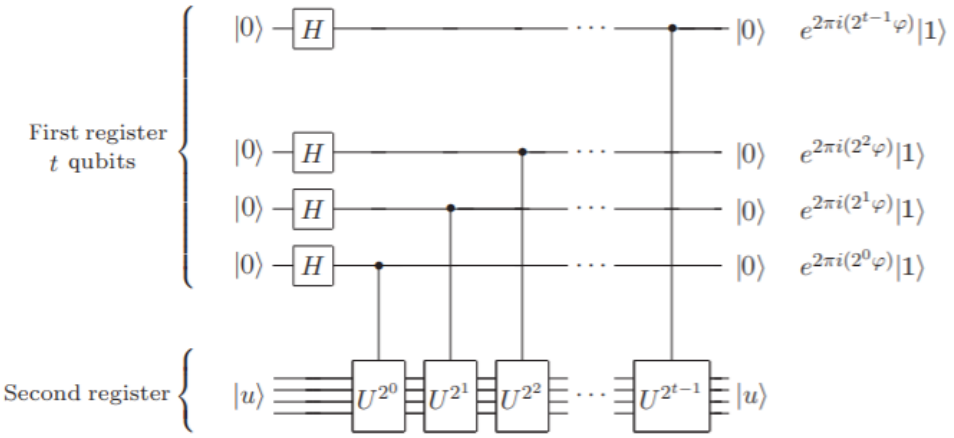


图 4.3-1 相位估计的第一阶段，右边省略了归一化因子$\frac{1}{\sqrt{2}}$

第一个寄存器的最终状态为

$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i 2^{t-1}\varphi}|1\rangle\right)\left(|0\rangle + e^{2\pi i 2^{t-2}\varphi}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 2^{0}\varphi}|1\rangle\right) = \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}|k\rangle$$

第二个寄存器的状态在线路运行过程中始终是$|u\rangle$

（2）第二个阶段应用量子傅里叶逆变换$(QFT)^{-1}$

当$\varphi = \frac{j}{N}, N = 2^t$时，易见

$$(QFT)^{-1}\left[\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi ijk/N}|k\rangle\right] = |j\rangle \overset{测量}{\Rightarrow} \varphi = \frac{j}{N} \tag{4.3.1}$$

$$\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}|k\rangle \overset{(QFT)^{-1}}{\rightarrow} \frac{1}{2^t}\sum_{k,l=0}^{2^t-1} e^{-2\pi ikl/2^t} e^{2\pi i\varphi k}|l\rangle \tag{4.3.2}$$

当$\varphi = 0.\varphi_1 \cdots \varphi_t$时，第一阶段的线路给出的结果正好是量子傅里叶变换的积表示，否则量子傅里叶逆变换后给出的是计算基态的叠加。

相位估计的总线路图为：

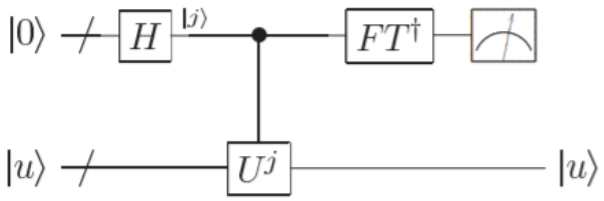


图 4.3-2 相位估计总线路图

上述线路实现的变换为$\frac{1}{2^{t/2}}\sum_{j=0}^{2^t-1} e^{2\pi i\varphi j}|j\rangle|u\rangle \to |\tilde{\varphi}\rangle|u\rangle$，最后在计算基下的测量将会给出$|\varphi\rangle$的估计值。

下面给出参数估计过程。

取$0 \le b \le 2^t - 1, b/2^t = 0.b_1 \cdots b_t$，满足$0 \le \delta \equiv \varphi - b/2^t \le 2^{-t}$。即：在小于$\varphi$的数中$b$是$\varphi$的$t$比特最佳近似（比如，取$\varphi$的前$t$比特）。

$$\frac{1}{2^t}\sum_{k,l=0}^{2^t-1} e^{-2\pi ikl/2^t} e^{2\pi i\varphi k}|l\rangle = \frac{1}{2^t}\sum_{k,l=0}^{2^t-1} e^{\frac{2\pi ik(2^t\varphi - l)}{2^t}}|l\rangle$$
$$= \frac{1}{2^t}\sum_{k=0}^{2^t-1}\frac{1-e^{2\pi i\delta}}{1-e^{\frac{2\pi i\delta}{2^t}}}|l\rangle \ (2^t\delta = 2^t\varphi - l \quad (4.3.3)$$

$$\alpha_l \equiv \frac{1}{2^t}\sum_{k=0}^{2^t-1}(e^{2\pi i(\varphi-(b+l)/2^t)})^k = \frac{1}{2^t}\frac{1-e^{2\pi i(2^t\varphi-(b+l))}}{1-e^{2\pi i(\varphi-(b+l)/2^t)}} \quad (4.3.4)$$

假设m为最后的测量结果，e是表示误差容忍度的正整数。e满足：

$$\frac{m}{2^t} - \frac{b}{2^t} < \frac{1}{2^n} \to e = 2^{t-n} - 1。 \quad (4.3.5)$$

因此为了以至少$1-\varepsilon$的概率获得n比特近似的φ，我们选择$t = n + \left\lceil log(2 + \frac{1}{2\varepsilon})\right\rceil$。

$$p(|m-b| > e) \equiv \sum_{|l-b|>e}|\alpha_l|^2 = \sum_{-2^{t-1}<l<-(e+1)}|\alpha_l|^2 + \sum_{e+1<l<2^{t-1}}|\alpha_l|^2 \quad (4.3.6)$$

当$-2^{t-1} < \alpha_l < 2^{t-1}$时，$|\alpha_l| \le \left|\frac{1}{2^{t+1}(\delta - l/2^t)}\right|$。又$0 \le 2^t\delta \le 1$，所以有：

$$p(|m-b| > e) \le \frac{1}{2(e-1)} \quad (4.3.7)$$

选择相位φ估计的精确度：精确到$2^{-n} \to e = 2^{t-n} - 1$，如果算法中使用$t = n + p$量子比特，可知获得此精度的概率为：

$$1 - p(|m-b| > e)|e = 2^{t-n} - 1 \ge 1 - \frac{1}{2(e-1)} = 1 - \frac{1}{2(2^{t-n}-2)} \equiv 1 - \varepsilon \quad (4.3.8)$$

则有$2\varepsilon = \frac{1}{2^{t-n}-2}, \frac{1}{2\varepsilon} + 2 = 2^{t-n}, t = n + \left\lceil log(2 + \frac{1}{2\varepsilon})\right\rceil$

下面给出量子相位估计算法的详细过程。

输入：

（1） 执行受控-U^j操作的黑盒

（2） 对应于U的本征值$e^{2\pi i\varphi}$的本征向量

（3） $t=n+\left\lceil log(2+\frac{1}{2\varepsilon})\right\rceil$个初始状态为$|0\rangle$的 qubit

输出：对于φ_u的n-bit 逼近结果φ_u

运行时间：$O(t^2)$个操作和一次调用受控-U^j。成功概率至少是$1-\varepsilon$

过程：

（1）$|0\rangle|u\rangle$ 初始化状态

（2）$\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle\,|u\rangle$ 创建叠加

（3）$\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle\,U^j|u\rangle$

$=\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}e^{2\pi ij\varphi_u}|j\rangle\,|u\rangle$ 应用黑盒得到结果

（4）$\rightarrow |\widetilde{\varphi_u}\rangle|u\rangle$ 应用逆傅里叶变换

（5）$\rightarrow \widetilde{\varphi_u}$ 测量第一个寄存器

注意当φ_u不能精确的表示为t比特时，$|\widetilde{\varphi_u}\rangle$应该是一个计算基底态的叠加。测量后才随机进入一个计算基底态$|m\rangle$，而且$|m/2^t-\varphi|<2^{-n}$的概率是$1-\varepsilon$。

4.3.2 求阶与分解

首先，这说明量子计算机本质上强于经典计算机，也对强邱奇-图灵理论提出了挑战。第二，任何新奇的算法，无论是经典还是量子的，都具有很大的研究价值。第三，从实用的角度来看，高效的求阶与分解算法可以被用来打破 RSA 公钥密码体制。

求阶问题：对一个正整数x和N，$x<N$，且无公因子。对使得$x^r=1(mod\ N)$的最小正整数定义为$x\ mod\ N$的阶。求阶问题就是在给定x和N的情况下，确定阶r。在经典计算机中，求阶问题被认为是困难问题，也就是说没有已知的算法能在多项式时间内解决问题。

定义酉算子：

$$U|y\rangle\equiv\begin{cases}|xy(mod\ \ N)\rangle，\ 0\le y<N\\ |y\rangle，\ N\le y\le 2^L-1\end{cases}\tag{4.3.9}$$

定义状态$|u_s\rangle\equiv\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{\frac{-2\pi isk}{r}}\left|x^k\ \ mod\ \ N\right\rangle$

容易验证，对$0\le s\le r-1$

$$
\begin{aligned}
U|u_s\rangle &= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi isk/r}\left|x^{k+1} \bmod N\right\rangle \\
&= e^{2\pi is/r}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi is(k+1)/r}\left|x^{k+1} \bmod N\right\rangle \\
&= e^{2\pi is/r}\frac{1}{\sqrt{r}}\sum_{k=1}^{r} e^{-2\pi isk/r}\left|x^{k} \bmod N\right\rangle \\
&= e^{2\pi is/r}\frac{1}{\sqrt{r}}\left[\sum_{k=1}^{r-1} e^{-2\pi isk/r}\left|x^{k} \bmod N\right\rangle + e^{-2\pi is}\left|x^{r} \bmod N\right\rangle\right] \\
&= e^{2\pi is/r}\frac{1}{\sqrt{r}}\left[\sum_{k=1}^{r-1} e^{-2\pi isk/r}\left|x^{k} \bmod N\right\rangle + e^{-2\pi i\cdot 0}\left|x^{0} \bmod N\right\rangle\right] \\
&= e^{2\pi is/r}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi isk/r}\left|x^{k} \bmod N\right\rangle = e^{2\pi is/r}\left|u_s\right\rangle
\end{aligned}
\tag{4.3.10}
$$

即，$|u_s\rangle$酉算子U的对应于本征值$e^{2\pi is/r}$的本征态。

任给正整数k，有$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1} e^{2\pi isk/r}|u_s\rangle = \left|x^k \mod N\right\rangle$

证明：记$k_0 = k(mod\ \ r)$

$$
\begin{aligned}
\text{左边} &= \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1} e^{2\pi isk/r}\frac{1}{\sqrt{r}}\sum_{k'}^{r-1} e^{2\pi isk'/r}\left|x^{k'} \bmod N\right\rangle \\
&= \frac{1}{r}\sum_{s=0}^{r-1}\sum_{k'=0}^{r-1} e^{2\pi i\frac{s}{r}(k_0-k')}\left|x^{k'} \bmod N\right\rangle \\
&= \frac{1}{r}\sum_{k'=0}^{r-1}\left(\sum_{s=0}^{r-1} e^{2\pi i\frac{s}{r}(k_0-k')}\left|x^{k'} \bmod N\right\rangle\right) \\
&= \frac{1}{r}\sum_{k'=0}^{r-1} r\cdot\delta_{k'k_0}\left|x^{k'} \bmod N\right\rangle = \left|x^{k_0} \bmod N\right\rangle \\
&= \left|x^{k} \bmod N\right\rangle
\end{aligned}
\tag{4.3.11}
$$

能够使用相位估计过程有两个重要的要求：一个要求是对所有的j必须有高效的过程来实现受控-U^{2j}操作，另一个要求是必须能够高效制备有着非平凡本征值的本征态，或者所有这样的本征态的叠加态。第一个要求可以通过模指数操作完成。通过模指数操作，就可以实现整个使用$O(L^3)$个门的相位估计程序受控-U^{2j}操作序列。第二个要求说明为了制备本征态$|u_s\rangle$，必须知道r，很明显这是不可能的。然而可以绕过这个问题。因为有：

$$
\begin{aligned}
\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle &= \frac{1}{r}\sum_{s,k=0}^{r-1} e^{\frac{-2\pi isk}{r}}\left|x^{k} \bmod N\right\rangle \\
&= \sum_{k=0}^{r-1}\left[\frac{1}{r}\sum_{s=0}^{r-1} e^{\frac{-2\pi iks}{r}}\right]\left|x^{k} \bmod N\right\rangle \\
&= \sum_{k=0}^{r-1}\delta_{0,k}\left|x^{k} \bmod N\right\rangle \\
&= |1\rangle
\end{aligned}
\tag{4.3.12}
$$

在相位估计过程中，如果在第一个寄存器准备$t = 2L + 1 + \left\lceil log(2 + \frac{1}{2\varepsilon}) \right\rceil$个 qubit，第二个寄存器准备状态$|1\rangle$。对于每个在 0 到$r - 1$的$s$，能够以至少$(1 - \varepsilon)/r$的概率，精确到$2L + 1$个比特，得到相位的估计结果$\varphi \approx s/r$。

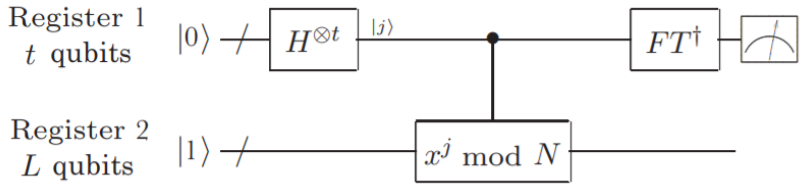


图 4.3-3 求阶算法的量子线路，同样可以用来做因子分解

故量子求阶算法可如下总结。

输入：

（1）黑盒$U_{x,N}$，执行的转换为$|j\rangle|k\rangle \to |j\rangle\left|x^j k \mod N\right\rangle$

（2）$t = 2L + 1 + \left\lceil log(2 + \frac{1}{2\varepsilon}) \right\rceil$个初始状态为$|0\rangle$qubit

（3）L个初始化为$|1\rangle$的 qubit

过程：

（1）$|0\rangle|1\rangle$ 初始化状态

（2）$\to \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|1\rangle$ 创建叠加

（3）$\to \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle\left|x^j \mod N\right\rangle$
$\approx \frac{1}{\sqrt{r2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1} e^{2\pi isj/r}|j\rangle|u_s\rangle$ 应用$U_{x,N}$

（4）$\to \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|s/r\rangle|u_s\rangle$ 对第一个寄存器应用逆傅里叶变换

（5）$\to s/r$ 测量第一个寄存器

（6）$\to r$ 应用连分数算法

分解问题：给定一个正合数N，考虑什么质数相乘可以得到它。分解问题等价于求阶问题，求阶的快速算法可以很容易地转换成分解的快速算法。下面把分解问题规约到求阶问题。

算法：分解

输入：合数N

输出：非平凡的因子N

运行时间：$O((log \ N)^3)$次操作，成功概率是$O(1)$

过程：

（1）如果N是偶数，返回因子 2；

（2）对于整数$a \geq 1$和$b \geq 2$判定$N = a^b$是否成立，如果成立返回因子a；

（3）随机选择$x \in [1, N-1]$。如果$gcd(x, N) > 1$，返回因子$gcd(x, N)$；

（4）使用求阶子程序找到$x \ \ mod \ \ N$的阶r；

（5）如果r是偶数，并且$x^{r/2} \neq -1(mod \ \ N)$，那么计算$gcd(x^{r/2} - 1, N)$和$gcd(x^{r/2} + 1, N)$。然后测试两个结果中的一个是否是非平凡的因子，如果是就返回这个因此；否则算法失败。

下面给出分解问题的一个实例：尝试分解$N = 15$。具体过程如下

（1）随机选择整数$x = 7$

（2）计算满足$x^r = 1 \ \ mod \ \ N$的r

1）初始化状态$|0_t\rangle|0_4\rangle$

2）对第一个包含 11 个 qubit 的寄存器应用 H 门，保证$\varepsilon \leq 1/4$

$$\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}|k\rangle|0_4\rangle = \frac{1}{\sqrt{2^t}}[|0\rangle + |1\rangle + |2\rangle + \cdots + |2^t - 1\rangle]|0\rangle \qquad (4.3.13)$$

3）计算$f(k) = x^k \ \ mod \ \ N$

$$\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}|k\rangle|x^k \ \ mod \ \ N\rangle = \frac{1}{\sqrt{2^t}}[|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + |6\rangle|4\rangle + \cdots] \qquad (4.3.14)$$

4）对第一个寄存器应用逆傅里叶变换，并进行测量。测量第二个寄存器，获得一个 1,7,4 或 13 的随机结果。

5）假设测量结果是 4，意味着输入到$FT^{\dagger}$的状态是$\sqrt{\frac{4}{2^t}}[|2\rangle + |6\rangle + |10\rangle + |14\rangle + \cdots]$

6）在应用了$FT^{\dagger}$后，获得一些状态$\sum_l \alpha_l|l\rangle$，概率分布如下：

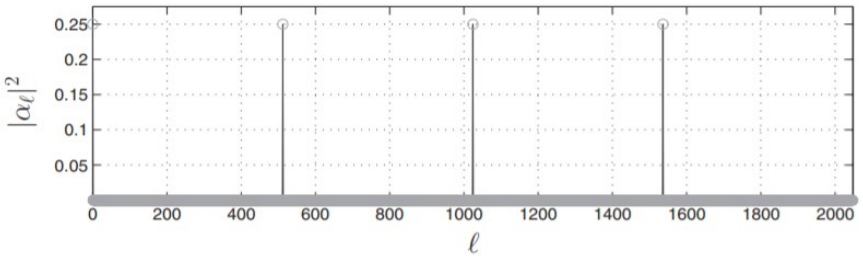


图 4.3-4 测量后的概率分布图

最后的测量给出了 0,512,1024,1536，每个概率几乎是 1/4

（3）假设得到的$l=1536$，计算连分数展开得到$\frac{1536}{2048}=1/(1+(1/3))$，因此在展开中$3/4$将会收敛。

（4）r是偶数，$x^{r/2}\ mod\ N=4\neq -1\ mod\ 15$，所以$gcd(x^2-1,15)=3$和$gcd(x^2+1,15)=5$都是非平凡的因子。

§4.4 量子傅里叶变换的一般应用

4.4.1 求周期问题

假设f是一个产生单比特输出的周期函数，并且对于未知的$0<r<2^L$，有$f(x+r)=f(x)$，其中，$x,r\in\{0,1,2,\dots\}$。定义量子黑盒：

$$U|x\rangle|y\rangle\rightarrow|x\rangle|y\oplus f(x)\rangle \tag{4.4.1}$$

考虑为确定r，需要多少次量子黑盒访问和其他操作？下面的量子算法仅使用一次量子黑盒访问和$O(L^2)$次其他操作就可以解决这个问题。

基于相位估计，与量子求阶算法中类似，引入$|f(x)\rangle$的傅里叶变换结果

$$\left|\hat{f}(l)\right\rangle\equiv\frac{1}{\sqrt{r}}\sum_{x=0}^{r-1}e^{\frac{-2\pi ilx}{r}}|f(x)\rangle \tag{4.4.2}$$

故，$|f(x)\rangle=\frac{1}{\sqrt{r}}\sum_{l=0}^{r-1}e^{\frac{2\pi ilx}{r}}\left|\hat{f}(l)\right\rangle$。很容易可以通过$\sum_{l=0}^{r-1}e^{2\pi ilx/r}=r$验证得到。

输入：

（1） 执行计算的黑盒$U|x\rangle|y\rangle\rightarrow|x\rangle|y\oplus f(x)\rangle$

（2） 存储函数计算值的状态，初始化为$|0\rangle$

（3） $t=O\left(L+log\left(\frac{1}{\varepsilon}\right)\right)$个量子比特，初始化为$|0\rangle$

输出：使得$f(x+r)=f(x)$成立的最小的整数$r>0$

运行时间：一次调用U和$O(L^2)$次操作。成功概率是$O(1)$。

过程：

（1）初始化：$|0\rangle|0\rangle$

（2）创建叠加：$\rightarrow\frac{1}{\sqrt{2^t}}|x\rangle|0\rangle$

（3）应用量子黑盒U

$$\begin{aligned}&\rightarrow\frac{1}{\sqrt{2^t}}|x\rangle|f(x)\rangle\\&\approx\frac{1}{\sqrt{r2^t}}\sum_{l=0}^{r-1}\sum_{x=0}^{2^t-1}e^{\frac{2\pi ilx}{r}}|x\rangle\left|\hat{f}(l)\right\rangle\end{aligned} \tag{4.4.3}$$

（4） 对第一个寄存器应用逆傅里叶变换

$$\rightarrow \frac{1}{\sqrt{r}}\sum_{l=0}^{r-1}\left|\frac{l}{r}\right\rangle\left|\hat{f}(l)\right\rangle \tag{4.4.4}$$

（5）测量第一个寄存器

$$\rightarrow \frac{l}{r}$$

（6）应用连分式展开算法

$$\rightarrow r$$

可以观察到，求周期算法可以看成是对量子求阶算法的推广。鉴于

$$x^r \equiv 1\, mod\, N\,, x^k\, mod\, N = x^{k+r}\, mod\, N \tag{4.4.5}$$

量子求阶算法可以看作为函数$f(k) = x^k\, mod\, N = f(k+r)$寻找周期$r$。注意到算法过程的黑盒$U$是使用本征值为$\left|\tilde{f}(l)\right\rangle$的酉算子实现的。

4.4.2 求解离散对数

离散对数问题是指在循环群上，给定$b = a^s\, mod\, N$,求出s。

给定函数$f(x_1, x_2) = a^{sx_1+x_2}\, mod\, N$，$r$表示使得$x^r\, mod\, N = 1$成立的最小

整数，$b = a^s\, mod\, N$。很容易证明这个函数是周期函数，即$f(x_1 + l, x_2 - ls) = f(x_1, x_2)$,而且周期是二元组$(l, -ls)$，其中$l$是任意整数。如果可以求出$s$，就可以解决离散对数问题，即只要求出函数$f$的周期，就可以解决离散对数问题。下面给出量子黑盒$U|x_1\rangle|x_2\rangle|y\rangle = |x_1\rangle|x_2\rangle|y \oplus f(x_1, x_2)\rangle$，量子算法可以调用一次量子黑盒$U$和进行$O(\lceil log\ \ r\rceil^2)$次其他操作求出$s$。

对$f(x_1, x_2) = a^{sx_1+x_2}\, mod\, N$定义傅里叶变换如下

$$|\hat{f}(l_1, l_2)\rangle = \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{\frac{-2\pi i l_2 j}{r}}|f(0, j)\rangle \tag{4.4.6}$$

在上述等式中，l_1和l_2的值必须满足$\sum_{k=0}^{r-1} e^{2\pi ik(l_1 s - l_2)/r} = r$。否则$\left|\hat{f}(l_1, l_2)\right\rangle$的幅度为 0.

输入：

（1） 黑盒：$U|x_1\rangle|x_2\rangle|y\rangle = |x_1\rangle|x_2\rangle|y \oplus f(x_1, x_2)\rangle$

（2） 存储函数计算值的状态，初始化为$|0\rangle$

（3） 两个$t = O(\lceil log\ \ r\rceil) + log(1/\varepsilon)$qubit 的寄存器初始化为$|0\rangle$

输出：使得$a^s = b$的最小整数s

运行时间：一次调用U，$O(\lceil log\ \ r\rceil^2)$次操作。成功概率为$O(1)$

过程：

（1）初始化状态：$|0\rangle|0\rangle|0\rangle$

（2）创建叠加→ $\frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|0\rangle$

（3）应用量子黑盒U

$$\begin{aligned}
&\to \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}\left|x_1\right\rangle\left|x_2\right\rangle\left|f\left(x_1,x_2\right)\right\rangle \\
&\approx \frac{1}{2^t\sqrt{r}}\sum_{l_2=0}^{2^t-1}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}e^{2\pi i\left(sl_2x_1+l_2x_2\right)/r}\left|x_1\right\rangle\left|x_2\right\rangle\left|\hat{f}\left(sl_2,l_2\right)\right\rangle \\
&= \frac{1}{2^t\sqrt{r}}\sum_{l_2=0}^{r-1}\left[\sum_{x_1=0}^{2^t-1}e^{2\pi i\left(sl_2x_1\right)/r}\left|x_1\right\rangle\right]\left[\sum_{x_2=0}^{2^t-1}e^{2\pi i\left(l_2x_2\right)/r}\left|x_2\right\rangle\right]\left|\hat{f}\left(sl_2,l_2\right)\right\rangle
\end{aligned} \tag{4.4.7}$$

（4）对前两个寄存器进行逆傅里叶变换

$$\to \frac{1}{\sqrt{r}}\sum_{l_2=0}^{r-1}\left|\frac{sl_2}{r}\right\rangle\left|\frac{l_2}{r}\right\rangle|\hat{f}(sl_2,l_2)\rangle \tag{4.4.8}$$

（5）测量前两个寄存器

$$\to \left(\frac{sl_2}{r},\ \frac{l_2}{r}\right) \tag{4.4.9}$$

（6）应用广义的连分式展开算法

$$\to s$$

§4.5 量子搜索算法

4.5.1 Oracle

假设希望能够在有$N=2^n$个元素的搜索空间中搜索M个元素，其中，$1\le M\le N$。关注搜索元素的下标（在0到$N-1$之间），而不是直接搜索元素。一个特定的搜索问题的实例可以通过下面函数f来表示

$$\begin{cases} f(x)=0, x\ is\ solution \\ f(x)=1, x\ is\ not\ solution \end{cases} \tag{4.5.1}$$

假设有量子 oracle O，拥有识别搜索问题的解的能力：

$$O：|x\rangle|q\rangle\to|x\rangle|q\oplus f(x)\rangle \tag{4.5.2}$$

其中，$|x\rangle$是下标寄存器，$|q\rangle$是辅助量子比特。

于是，初始化状态$|x\rangle|0\rangle$，然后应用量子 oracle，通过检查 oracle 量子比特是否翻转为$|1\rangle$来判断x是否是搜索问题的解。

如果将$|q\rangle$初始化为$\frac{|0\rangle-|1\rangle}{\sqrt{2}}$，即

$$O:\ |x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\rightarrow(-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \tag{4.5.3}$$

发现辅助量子比特的状态在量子 oracle O作用后没有发生改变，因此 oracle$O$可以简化为：

$$O:\ |x\rangle\rightarrow(-1)^{f(x)}|x\rangle \tag{4.5.4}$$

称 oracle 通过改变解的相位来实现标记解。

下面以分解问题为例来说明。假设知道一个大整数m是两个素数$p\ q$的乘积。为了确定$p\ \ q$，经典计算机的一般做法是搜索所有从 2 到$\sqrt{m}$的数，寻找两个素数中较小的那一个，然后做一个平凡的除法求出另一个素数。很显然，在经典中，这个基于搜索的算法需大概$O\left(\sqrt{m}\right)$次除法才能得到一个素因子。

然而量子算法可以加速这个过程。根据定义，对输入$|x\rangle$量子 oracle$O$的行为是用x除m，可以除尽时翻转辅助量子比特。作用这个量子 oracle$O$将会以很高的概率产生两个素因子中的一个。但是需要构建实现量子 oracle$O$的高效线路。定义函数

$$\begin{cases} f(x)=0, x|m \\ f(x)=1, otherwise \end{cases} \tag{4.5.5}$$

使用可逆计算的方法，构造一个以(x,q)为输入，以$\left(x,q\oplus f(x)\right)$为输出的经典可逆线路。这个可逆线路的资源花费一般是用来做除法的可逆的经典计算线路的 2 倍。经典的可逆线路可以直接被转化成以$|x,q\rangle$为输入，以$|x,q\oplus f(x)\rangle$为输出的量子线路。因此，即便在不知道m的素因子的情况下，依然能够构造一个量子 oracle 来识别搜索问题的解。使用这个量子 oracle，实现搜索所有从 2 到$\sqrt{m}$的数，只需要询问 oracle$O\left(m^{\frac{1}{4}}\right)$次，相比于经典中的$O\left(m^{\frac{1}{2}}\right)$实现了平方的加速效果。

当然，上面给的搜索问题的例子并不实际，在经典中存在着比搜索所有的可能的因子更快的分解方法。但是通过这个例子，发现基于搜索的经典算法都可能通过使用量子搜索算法来实现加速。其实，量子搜索算法对加速 NPC 问题的解搜索过程可以提供重要帮助。

4.5.2 过程

算法开始时，计算机初始状态$|0\rangle^{\otimes n}$，Hadamard 变换使得计算机变成均匀叠加态

$$|\psi\rangle=\frac{1}{N^{1/2}}\sum_{x=0}^{N-1}|x\rangle \tag{4.5.6}$$

量子搜索算法是一个重复使用 Grover 迭代的过程，用 G 表示。Grover 迭代有如下几个过程

（1） 应用 oracle$O$

（2） 应用 Hadamard 变换$H^{\otimes n}$

（3） 对除了$|0\rangle$之外的每个计算基态执行条件相移

$$|x\rangle \to -(-1)^{\delta_{x0}}|x\rangle \tag{4.5.7}$$

（4） 应用 Hadamard 变换$H^{\otimes n}$

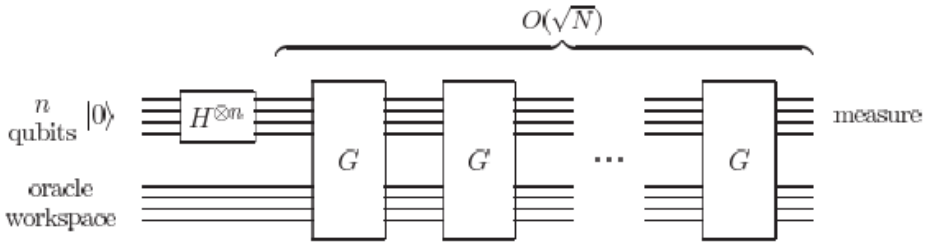


图 4.5-1 量子搜索算法的线路原理

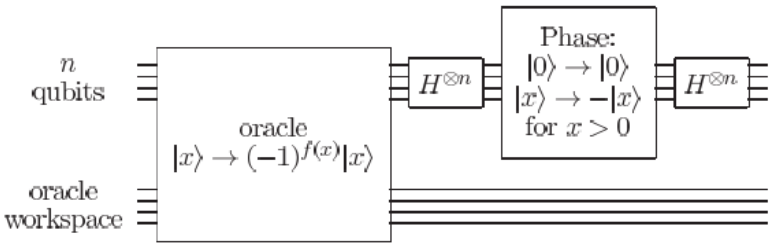


图 4.5-2 Grover 迭代 G 的线路图

在 Grover 迭代中的每个操作都可以在量子计算机上高效实现。第（2）和第（4）步中的 Hadamard 变换需要$n = log(N)$次操作。第（3）步条件相移可以使用$O(n)$个门实现。Oracle 调用的花费依赖于具体的应用场景，Grover 迭代只需要一次 oracle 调用。第（2）（3）（4）步组合结果为

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I \tag{4.5.8}$$

因此，Grover 迭代可以写成$G = (2|\psi\rangle\langle\psi| - I)O$

4.5.3 几何可视化

Grover 迭代可以看成是由初始向量$|\psi\rangle$张成的二维空间。这个状态包含搜索问题的解的均匀叠加。下面用$\sum_x{}'$表示搜索问题的所有解x的和，$\sum_x{}''$表示所有非搜索问题的解x的和。

定义如下归一化态

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}}\sum_x{}''|x\rangle，\ |\beta\rangle = \frac{1}{\sqrt{M}}\sum_x{}'|x\rangle \tag{4.5.9}$$

故，$|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$。

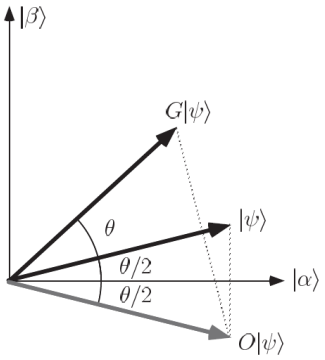


图 4.5-3 单次 Grover 迭代的作用

可以将O的作用看作是在由$|\alpha\rangle$和$|\beta\rangle$定义的平面内将状态$|\psi\rangle$关于状态$|\alpha\rangle$做反射。也就是说，$O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle$。同样的，$2|\psi\rangle\langle\psi| - I$的作用看作是在由$|\alpha\rangle$和$|\beta\rangle$定义的平面内将状态$O|\psi\rangle$关于状态$|\psi\rangle$做反射。两次反射的乘积是一个旋转，这也就说明了对于所有的k，状态$G^k|\psi\rangle$仍在由$|\alpha\rangle$和$|\beta\rangle$张成的平面内。设$cos\frac{\theta}{2} = \sqrt{\frac{(N-M)}{N}}$，所以$|\psi\rangle = cos\frac{\theta}{2}|\alpha\rangle + sin\frac{\theta}{2}|\beta\rangle$。如图所示，两次反射有

$$G|\psi\rangle = cos\frac{3\theta}{2}|\alpha\rangle + sin\frac{3\theta}{2}|\beta\rangle \tag{4.5.10}$$

且旋转角度为θ。关于θ，很容易可以得到$sin\,\theta = \frac{2\sqrt{M(N-M)}}{N}$

迭代地应用 G 会使初始状态$|\psi\rangle$变为

$$G^k|\psi\rangle = cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle \tag{4.5.11}$$

总的来讲，G 就是在由$|\alpha\rangle$和$|\beta\rangle$张成的平面内的旋转，且每次调用之后旋转角度为θ。重复地应用 Grover 迭代将会使得状态向量足够接近$|\beta\rangle$。也就是说，此时在计算基下的观测将会以很高的概率给出叠加在$|\beta\rangle$中的一个结果，即搜索问题的一个解。

下面给出$N = 4$时使用 Grover 搜索特定解的例子。

在搜索$\{0,1,2,3\}$中搜索x_0，定义函数$\begin{cases} f(x) = 0, x = x_0 \\ f(x) = 1, otherwise \end{cases}$。根据$x_0$的取值不同，对 oracle$O$设计有如下四种可能。

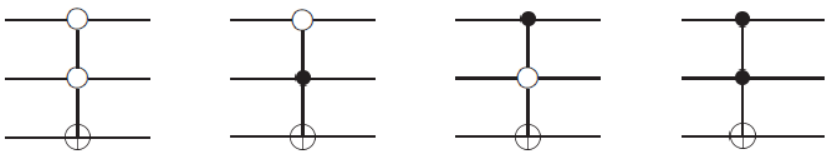


图 4.5-4 oracle$O$设计线路图，从左到右分别表示$x_0 = 0,1,2,3$

刚开始，上面两个量子比特初始化为$|0\rangle$，虚线框中表示条件相移$2|00\rangle\langle 00| - I$

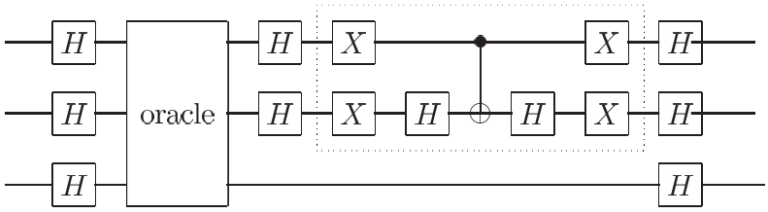


图 4.5-5 总体量子线路图

很明显，$M=1\ sin\theta=\frac{2\sqrt{M(N-M)}}{N}=\frac{\sqrt{3}}{2}$,故$\theta=\frac{\pi}{3}$。只需要一次迭代就可以得到x_0。初始状态$|\psi\rangle=\frac{(|00\rangle+|01\rangle+|10\rangle+|11\rangle)}{2}$，与$|\alpha\rangle$夹角是$\frac{\pi}{6}$，旋转一次$\theta=\frac{\pi}{3}$，就可以将状态$|\psi\rangle$旋转到$|\beta\rangle$。

4.5.4 算法性能

下面考虑需要重复多少次 Grover 迭代才能将$|\psi\rangle$旋转到状态向量$|\beta\rangle$。系统的初始状态是$|\psi\rangle=\sqrt{\frac{N-M}{N}}|\alpha\rangle+\sqrt{\frac{M}{N}}|\beta\rangle$。故旋转$arccos\sqrt{\frac{M}{N}}$度，将会把系统旋转到状态向量$|\beta\rangle$。用$CI(x)$表示最接近实数$x$的整数，这里使用向下取整，比如$CI(3.5)=3$。那么重复 Grover 迭代

$$R=CI\left(\frac{arccos\sqrt{\frac{M}{N}}}{\theta}\right) \tag{4.5.12}$$

次，将状态$|\psi\rangle$旋转到$|\beta\rangle$的一个角度$\frac{\theta}{2}\leq\frac{\pi}{4}$内。在计算基下测量这个状态将会以至少一半的概率产生搜索问题的一个解。对于特定的M,N，有可能实现更高的成功概率，比如，当$M\ll N$，有$\theta\approx sin\,\theta\approx 2\sqrt{\frac{M}{N}}$，最后状态的角度误差最多是$\frac{\theta}{2}\approx\sqrt{\frac{M}{N}}$，概率误差最多是$\frac{M}{N}$。$R$依赖于解空间$M$的个数。故如果知道了$M$，就可以应用量子搜索算法。

因为，有

$$R=CI\left(\frac{arccos\sqrt{\frac{M}{N}}}{\theta}\right) \tag{4.5.13}$$

简化表示为$R\leq\left\lceil\frac{\pi}{2\theta}\right\rceil$，故取$\theta$的下界将会产生$R$的上界。假定$M\leq\frac{N}{2}$，有

$$\frac{\theta}{2}\geq sin\frac{\theta}{2}=\sqrt{\frac{M}{N}}, \tag{4.5.14}$$

迭代次数的上界为

$$R\leq\left\lceil\frac{\pi}{4}\sqrt{\frac{N}{M}}\right\rceil \tag{4.5.15}$$

故为了以高概率获得搜索问题的一个解必须要执行$R=O\left(\sqrt{\frac{N}{M}}\right)$次 Grover 迭代。下面给出当$M=1$时的量子搜索算法过程。

输入：

（1）黑盒 oracle$O$,执行变换：$O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$。当$x = x_0$，$f(x_0) = 1$；除了$x_0$的所有$0 \le x < 2^n$，$f(x) = 0$。

（2）$n+1$个初始状态为$|0\rangle$的量子态

输出：x_0

运行时间：$O(\sqrt{2^n})$，成功概率为$O(1)$

过程：

（1）初始化状态：$|0\rangle^{\otimes n}|0\rangle$

（2）对前$n$qubit 执行 Hadamard 变换，对最后一个 qubit 执行HX操作

$$\to \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \tag{4.5.16}$$

（3）执行 Grover 迭代次数为$\pi\sqrt{2^n}/4$

$$\to [(2|\psi\rangle\langle\psi| - I)]^R \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \approx |x_0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \tag{4.5.17}$$

（4）测量前n个 qubit$\to x_0$.

4.5.5 关于“量子摇晃”

直接看 Grover 迭代是怎样放大$|a\rangle$的几率幅的。仍取$|s\rangle = \frac{1}{N}\sum_{x=0}^{N-1}|x\rangle$，设系统状态为任意态$|\varphi\rangle = \sum_{x=0}^{N-1} C_x|x\rangle$，记$\langle C_x\rangle \equiv \frac{1}{N}\sum C_x$则

$$\langle s|\varphi\rangle = \frac{1}{\sqrt{N}}\sum_x C_x = \sqrt{N}\cdot\frac{1}{N}\sum C_x = \sqrt{N}\,\langle C_x\rangle, \tag{4.5.18}$$

而

$$\begin{aligned} U_s|\varphi\rangle &= (2|s\rangle\langle s| - 1)|\varphi\rangle = 2|s\rangle\langle s|\varphi\rangle - |\varphi\rangle \\ &= 2|s\rangle\sqrt{N}\,\langle C_x\rangle - \sum_{x=0}^{N-1} C_x|x\rangle \\ &= \sum_{x=0}^{N-1}(2\langle C_x\rangle - C_x)|x\rangle \overset{\text{记}}{=\!=} \sum_{x=0}^{N-1} C_x'|x\rangle \end{aligned}$$

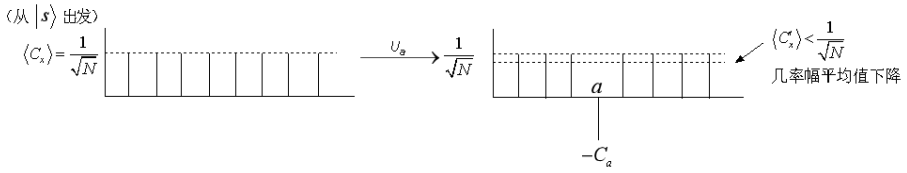
考虑$|x\rangle$的几率幅与平均几率幅之差（U_s作用后不改变$\langle C_x\rangle$）：

$$C_x-\langle C_x\rangle \xrightarrow{U_s} \underbrace{2\langle C_x\rangle-C_x}_{C_x'}-\langle C_x\rangle=\langle C_x\rangle-C_x=-\left(C_x-\langle C_x\rangle\right),$$

未作U_s之前的值

即：U_s使此量反号。由此可推知U的作用如下：

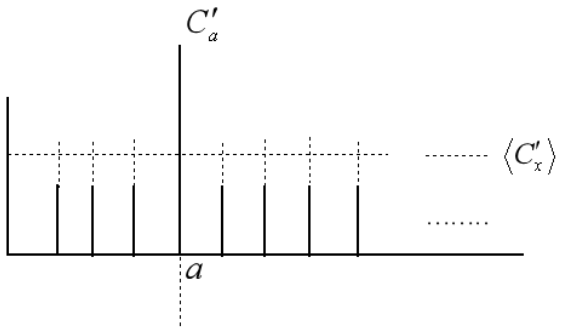
1、U_a使的$|a\rangle$几率幅反号：



2、U_s使系统在$|x\rangle$上的几率幅与平均几率幅之差$C_x-\langle C_x\rangle$反号：

1）$C_a-\langle C_x\rangle<0\xrightarrow{U_s}C_a'-\langle C_x'\rangle=-\left(C_a-\langle C_x\rangle\right)>0$

2）$x\neq a$时，$C_x-\langle C_x\rangle>0\xrightarrow{U_s}-\left(C_x-\langle C_x\rangle\right)<0$



即：U_s使各几率幅相对于$\langle C_x'\rangle$线反转。每次反转后C_a的增量与$\langle C_x'\rangle$有关，故作用逐次递减。易知

$C_a'=2\langle C_x\rangle+C_a\approx 3C_a$

$$C_a''=2\langle C_x'\rangle+C_a'\approx 5C_a$$

$$\vdots$$

$$C_a^{(l)}=2\langle C_x^{(l-1)}\rangle+C_a^{(l-1)}$$

$$\Longrightarrow C_a^{(l)}\sim lC_a=\frac{1}{\sqrt{N}}$$

故需进行$l\sim\sqrt{N}$次迭代。

第 5 章量子计算环境下密码体制安全性分析

§5.1 攻击模型

在经典密码分析中，敌手、用户都只拥有经典计算机，执行的都是经典计算。而量子计算机的呼之欲出需要考虑新的攻击模型。可以将攻击看作敌手和服务器之间的多次交互过程。敌手通过在线的远程访问服务器得到某些密文，然后在本地进行离线计算来达到破解密码系统的目的。Kaplan 等人[1]在依据 Zhandry[2]给出的 PRF 安全性概念给出了量子密码分析的两个模型 Q1 模型（也叫标准安全性）和 Q2 模型（也叫量子安全性）。在 Q1 模型和 Q2 模型下，敌手都拥有量子计算机，且能在本地进行离线的量子计算。但是在 Q1 模型下，敌手向服务器询问经典信息，得到经典信息的返回结果；而在 Q2 模型下，敌手却可以向服务器询问量子叠加态，并且得到量子叠加态返回结果。由此可见 Q2 模型是更强的攻击模型，在该攻击模型下密码体制安全性极高，然而这是非常难实现的。基于 Q1 和 Q2 模型，目前已经存在很多量子密码攻击方法。主要的研究方向是基于 Q2 模型给出的。在 Q2 模型下，经常考虑的是量子选择明文攻击（qCPA），如果将一个经典的加密函数描述为$E_k:\{0,1\}^n \to \{0,1\}^n$，那么敌手可以进行量子访问$\sum_{x,y}|x\rangle|y\rangle \to \sum_{x,y}|x\rangle|y \oplus E_k(x)\rangle$。

§5.2 量子计算环境下的对称密码安全性分析

目前应用于分组密码的量子分析的算法主要有：Grover 算法、Simon 算法、Grover 结合 Simon 算法、Bernstein-Vazirani 算法。

5.2.1 基于 Grover 算法的量子攻击

经典中穷举攻击在量子世界中的等价物是考虑使用 Grover 算法对密钥空间进行穷搜。在量子计算环境中，利用 Grover 算法，可以为任意密钥穷搜攻击提供平方阶的加速。比如对于密钥长度为k的密码算法，经典中时间复杂度为$O(2^k)$的攻击，使用 Grover 算法后，时间复杂度将降为$O\left(2^{k/2}\right)$。

Grover 算法是一个迭代过程，迭代次数依据解空间个数而选取，算法实现在无结构的搜索空间上搜索满足特定要求的元素的目标。每次迭代包括创建解空间的叠加态和标记目标解两个步骤。比如对一个密钥长度为k的密码算法$E(\quad)$，已知存在一个唯一的$k^* \in \{0,1\}^k$，使得$E_{k^*}(m) = c$，要使用 Grover 算法找到k^*。这个穷搜攻击对应的问题即为在$\{0,1\}^k$上找一个特定元素k^*，搜索空间大小为2^k，解空间个数为 1。那么，使用 Grover 算法进行$\frac{\pi}{4}\sqrt{2^k}$次迭代就可以找到唯一解k^*，也就达到了攻击密码算法的目的。这表明在后量子世界中，对称密码体制的密钥长度需要加倍才能保持与在经典世界中等价的理想安全性。

然而，密钥穷搜攻击只是定义了密码体制的理想安全性，为了理解对称密码算法在量子计算环境下的实际安全性，还需要研究量子敌手在真实世界中可能执行的其他攻击。也就是说，抵抗量子敌手的安全性不能基于量子穷举攻击是唯一可行攻击的假设，需要考虑更多的攻击手段。这一方向在近年来受到越来越多的关注。2011 年，Wang 基于 Grover 算法提出了固定重量目标解的量子算法[3]，并用于寻找 NTRU 的私钥。基于此，Wang 给出了针对

NTRU 公钥密码体制的量子中间相遇攻击算法[4]。Pang 利用 Grover 算法研究了集合运算问题，实现了对经典算法的加速[5]。除此之外，Grover 算法也常与经典的分析方法相结合应用于密码分析。Qing Zhou 等人首先将 Grover 算法应用于差分分析的密钥恢复阶段，并得到平方阶的加速[6]。2016 年，Kaplan 等人进一步将 Grover 算法应用于各类差分分析和线性分析的密钥恢复阶段，对 Q1 和 Q2 模型下的攻击复杂度给出了具体刻画，并给出了对 LAC 和 KLEIN 算法的应用示例[1]。他们的工作发现在 Q2 模型下的攻击并不总是最优的。除此之外，在 Q1 模型下，当密钥长度与分组长度相等时，相比于经典模型，量子攻击带来的复杂度降低优势很小。只有当密钥长度大于分组长度时，才能说量子攻击优势显著。除了密钥恢复阶段，Grover 算法还可以被应用于差分分析的第一阶段，即寻找高概率差分阶段。

Grover 算法还可以用来对哈希函数进行碰撞查找。对 Grover 算法不做任何修改的情况下，使用 Grover 算法对哈希函数进行碰撞查找的复杂度为$O(\sqrt{n})$。然而，当我们将生日悖论与 Grover 算法结合起来时[7]，复杂度将会降低到$O(\sqrt[3]{n})$。具体做法是创建一个大小为$\sqrt[3]{n}$的表格，利用 Grover 算法找到一个与该表格的碰撞。如果没有碰撞发生，表格中的每个值都和不在表格中的值有碰撞。在$1-\sqrt[3]{n}$个元素中搜索$\sqrt[3]{n}$个元素，这个问题是可以使用 Grover 算法在$O(\sqrt[3]{n})$时间内解决。

王婕等[8]在分析基于 Grover 搜索算法的杂凑函数通用攻击模型的基础上，重点研究了 MD5 算法的一个破译模型和两个碰撞模型，并设计了为实现这三个模型所依赖的具体的量子线路（量子线路主要有量子比特和量子逻辑门组成），如杂凑模块、基本逻辑函数模块、比较模块等。最后，通过图形仿真和程序模拟两种方式，展示了 Grover 量子搜索算法（其实质是量子并行性）在计算效率，搜索成功概率方面的优势。

欧密 20 上，Hosoyamada 等人开启了对 AES 类的哈希函数的量子碰撞攻击的研究。2020 年，Hosoyamada 等人在[9]中关注对具体哈希函数的专门碰撞攻击，这一没有受到很多关注的领域。在经典设定下，寻找一个哈希函数碰撞的复杂度是$O(2^{n/2})$，因此比如基于差分分析的碰撞攻击，比如 reboundattack 需要建立一条差分概率超过$O(2^{-n/2})$的差分路径。作者给出了在量子计算设定下使用小于生日界的差分概率寻找哈希函数 AES-MNO 碰撞的攻击，然而在经典中，当差分概率小于生日界时，认为使用该攻击是没有意义的。亚密 20 上，董晓阳等人对欧密 20 的结果做了进一步发展[10]。在欧密 20 上，使用的攻击使用了大量的量子随机访问内存(qRAM)，然而即便在量子计算机时代到来后这个资源是否能获得也是存疑的。如果没有 qRAM，这类的攻击的时间复杂度将会显著增加。董晓阳等人基于欧密 20 的结果进一步向前发展。董晓阳等人通过执行基于非全部活跃的超 S 盒的量子 reboundattack 来减少甚至避免使用 qRAM。

另外应用 Grover 算法到具体分组密码的线路设计也是近几年的研究热点。早在 2016 年，Grassl 等人给出了对 AES 实现穷搜攻击的量子线路，并且给出了 Clifford+T 门资源的详细估计[11]。在 2020 年，在轻量级分组密码的 Grover 穷搜的量子线路设计上，又有了新的进展。Ravi Anand 等人在[12]中，给出了对 SIMON 算法的所有变种的 Grover 搜索算法，并且列举了实现这样的攻击的 NOT CNOT 和 Toffoli 门的资源估计。也提供了线路的 T 深度估计和实现攻击需要的量子比特数。Ravi Anand 的结果说明了对 r 轮 SIMON2n/mn 实现 Grover 的量子比特数至少达到$O(2nr+mn)$。此外，作者还给出了在 IBMQ 的量子模拟器和 14-qubit 的量子处理上运行约减版本的 SIMON 的实现。

5.2.2.基于 Simon 算法的量子攻击

Simon 算法可用于求解布尔函数的周期，是另一个在对称密码分析中有重要应用的量子算法。给定一个二到一的周期布尔函数，Simon 算法可以通过对该布尔函数的$O(n)$次量子询问求出其周期（n为定义域的比特串长度），而经典算法求解最坏的情况需要$2^{n-1}+1$次询问。使用 Simon 算法核心是构造满足 Simonpromise 布尔函数f，即$\forall x, f(x)=f(x\oplus s)$。目前已有的使用 Simon 算法进行密码分析都是在 Q2 模型中进行，即敌手有权对服务器进行量子叠加访问。Luby 和 Rackoff 已经证明三轮 Feistel 方案是一个安全的伪随机置换。经典区分器通过$O\left(2^{n/2}\right)$此经典访问将三轮 Feistel 方案和随机置换区分开。然而，2010 年，Kuwakado 和 Morri 基于 Simon 算法构造了一个量子区分器[13]，可以在通过$O(n)$次量子访问将三轮 Feistel 方案和随机置换区分开，实现指数加速。具体方法是基于三轮 Feistel 方案的加密输出的左半部分构造出存在周期的布尔函数，对布尔函数作用 Simon 算法$O(n)$次，最后通过解线性方程组求出周期，即实现了区分。这是 Simon 算法用于构造量子区分器的第一次尝试。随后，他们又基于 Simon 算法，提出了一个可用于攻击 Even-Mansour 结构的量子算法，该算法可以有效恢复部分密钥[14]。2013 年，杨理等人基于 Simon 量子算法提出了首个求解布尔函数线性结构的量子算法[15]。这一算法的主要特点是可以用于对所处理的布尔函数不做任何假设的一般情形，从而为量子算法在分组密码差分攻击上的应用奠定了基础。2015 年，Rotteler 等人将 Simon 算法应用于相关密钥攻击[16]，该攻击针对的是分组密码的电子密码本（ECB）工作模式。在敌手拥有叠加相关密钥 oracle 访问权限时，可以使用 Simon 算法对基于密码系统$E_s(m)$构造的函数在多项式时间内求出函数的周期，即密钥s。但是必须满足要求：分组密码必须可以被作为量子线路高效实现；密钥可由少数可获得的明密文对唯一决定。2016 年，Santoli 等人发展了 Kuwakado 和 Morri 的结果[17]，将[13]中的假设放宽，证明当三轮 Feistel 结构的中间函数为一般随机函数（而未必是随机置换）时仍具有有效的量子区分器。在该文中，他们基于相同的思想，还给出了对 CBC-MAC 的一个量子伪造攻击算法。同一时期，Kaplan 等人用不同的方法扩展了[13]中的结果，并将 Simon 算法攻击 PMAC、GMAC 等消息认证码，以及 OCB、CLOC、AEZ 等认证加密方案[18]，还给出了针对于自相似结构，即轮函数相同的多轮加密算法的量子滑动攻击。但是，由于密码方案的复杂性，Simon promise 并不总是满足的，即构造依据加密算法构造的布尔函数可能是多碰撞的，对某些x有$f(x)=f(x\oplus s)=f(x\oplus t), t\neq 0, t\neq s$。针对这种情况，Kaplan 等人说明了即便布尔函数f有一个部分周期t，应用 Simon 算法依旧可以求出周期s。在欧密 2017 上，Alagic 等人研究了基于 hiddenshift 的量子安全的对称密码学。[19]在加密方案中，用$\mathbb{Z}/2^n$上的加法运算来代替$(\mathbb{Z}/2^n)$上的加法运算，并且说明了这样的修改是抵抗量子敌手安全的，而且这样的修改保留了原有经典的方案安全性质和基本的结构性质。Alagic 等人把 HSP 问题直接规约到了对称密码系统的安全性。因此，任何对这些系统的高效的量子选择明文攻击将会解决在量子复杂性理论长期存在的问题。其次对 EM 分组密码构造，将模 2 加运算改为模2^n加运算，证明了 hiddenshift 版本的 EM 分组密码能产生量子安全的伪随机函数；同样说明了 hiddenshift 版本的加密的 CBC-MAC 能产生一个抗碰撞的哈希函数。这样的改变使得以 Simon 算法为基础的攻击在更一般的情况下失效。Bonnetain[20]给出了有关 Simon 量子算法的复杂度界的新结果。Bonnetain 的结果旨在给出使用 Simon 算法的一些精准的复杂度衡量。提出了 Simon 量子算法的拓展分析，说明了在大多数情况下要成功需要的访问次数超过 n 次。并且首次对 Simon 算法的变种及离线 Simon 算法的精确复杂度衡量，展示了分别需要至多 3n 次访问和 n+k 次访问。作者还发现，对于密码相关性，有可能将周期函数的输出阶段成为某些比特，然而这对访问次数没有任何影响，这在 Simon 算法的可逆实现上将会节省量子比特。

Simon 算法在分组密码中应用举例

下面介绍拓展 Simon 算法用于分组密码的不可能差分分析上的研究成果[35]。

谢惠琴扩展 Simon 算法，使其可以应用于具有多周期和非周期碰撞的布尔函数，在此基础上基于 Simon 算法构造求解布尔函数线性结构的量子算的。基于分组密码的线性结构同时也是其概率 1 差分的事实，谢惠琴将该量子算法应用于中间相错攻击，提出寻找分组密码不可能差分的量子算法。传统的中间相错攻击技术中，无论攻击者通过寻找概率 1 的差分路径来求解概率 1 差分，还是通过直接分析整体加密函数的代数性质来寻找概率 1 差分，随着轮数的增加，整体加密函数更加复杂，求高概率差分的难度都将急剧增大。与此相比，谢惠琴提出的量子中间相错攻击技术将约减的分组密码看作一个整体黑盒地执行量子算法，一定程度上避免了轮数增加带来的复杂性。

（1）基于 Simon 算法求解线性结构

扩展 Simon 算法使其可以求解布尔函数的线性结构。首先定义一些基本概念。向量$a \in \{0,1\}^n$为多输出布尔函数$F:\{0,1\}^n \to \{0,1\}^m$（$m = poly(n)$）的线性结构当且仅当存在向量$b \in \{0,1\}^m$使得

$$F(x \oplus a) \oplus F(x) = b,\ \forall x \in \{0,1\}^n。 \tag{5.2.1}$$

若b为m维零向量，即$b = 0^m$，则向量a为函数F的周期。F的所有周期构成了一个$\mathbb{F}_2$上的n维线性空间，称为F的周期空间，记为S_F。F的一般的线性结构在向量加法下不封闭，所以不构成线性空间。

若向量$a \in \{0,1\}^n$、$b \in \{0,1\}^m$满足(5.2.1)式，称(a,b)为F的一个线性结构对，若(a_1,b_1)、(a_2,b_2)为F的两个线性结构对，则

$$F(x \oplus a_1 \oplus a_2) \oplus F(x) = F(x \oplus a_1) \oplus b_2 \oplus F(x) = b_1 \oplus b_2 \tag{5.2.2}$$

即$(a_1,b_1) \oplus (a_2,b_2)$也是$F$的线性结构对。因此，$F$的全体线性结构对构成了$\mathbb{F}_2$上$n+m$维线性空间的一个子空间。称该子空间为$F$的线性结构空间，记为$L_F$。

给定一个布尔函数F，称一个量子线路实现F，若该线路执行以下酉算子：

$$U_F:|x\rangle|y\rangle \to |x\rangle|y \oplus F(x)\rangle \tag{5.2.3}$$

由于任意量子线路都可以用通用量子门集中的量子门表示，可以假设实现F的量子线路由通用门集中的量子门组成。用符号$|F|_Q$表示执行F的量子线路中通用门的个数，该参数表示实现F的量子线路的复杂性。不失一般性，假设 Hadamard 门H和受控非门$CNOT$属于通用门集。

Simon 算法可以用于求解布尔函数的周期，但要求布尔函数满足 Simon 条件。设布尔函数为$F:\{0,1\}^n \to \{0,1\}^m$，Simon 条件要求存在向量$s \in \{0,1\}^n$使得

$$[F(x) = F(y)] \Leftrightarrow [x \oplus y \in \{0^n, s\}],\ \forall x,y \in \{0,1\}^n \tag{5.2.4}$$

应用Simon算法即可在多项式时间内求出周期s。Simon算法重复$O(n)$次Simon子程序，得到$O(n)$个向量，再以这些向量为系数求解线性方程组。运行一次 Simon 子程序需要执行$2n$

个 Hadamard 门和$|F|_Q$个额外的通用量子门，因此运行 Simon 算法总共需要$O(2n^2+n|F|_Q)$通用量子门和$n+m$量子比特。

多周期情况的 Simon 算法

为了应用 Simon 算法于中间相错攻击，需要处理布尔函数存在多个周期的情况。设$F:\{0,1\}^n\to\{0,1\}^m$为多周期的布尔函数，且F具有周期空间S_F，设$s_1,s_2\cdots,s_t$为S_F的一个基，即$S_F=\text{span}\{s_1,\cdots,s_t\}$。称$F$满足广义的 Simon 条件，若对任意的$x,y\in\{0,1\}^n$，都成立

$$[\,F(x)=F(y)\,]\Leftrightarrow[\,x\oplus y\in S_F\,] \tag{5.2.5}$$

证明了只要多周期布尔函数满足广义的 Simon 条件，Simon 算法仍可以求出布尔函数的周期。具体定理如下：

引理 5.2.1. F满足广义 Simon 条件，则运行 Simon 子程序于F输出的随机向量y满足$y\in S_F^{\perp}$，即对任意的$s\in S_F$有$y\cdot s=0$。

重复 Simon 子程序$O(n)$次可以得到$n-t$个与S_F正交的独立向量。将这些向量作为线性方程组的系数进行求解，得到的解空间即为F的周期空间S_F。以上是F存在多个中周期的情况，考虑更一般的情形，即F除了拥有非平凡的周期空间S_F外，还存在非周期的碰撞。这意味着存在点x、y使得$F(x)=F(y)$，但$x\oplus y\notin S_F$。若存在向量a不是F的周期，但却造成过多的非周期碰撞，即$f(x)=f(x\oplus a)$对过多的x成立，则 Simon 有可能无法有效求出F的周期空间。反之，若F的非周期碰撞数可以被限制，则 Simon 算法可能仍可以求出F的周期空间。为了说明这一点，定义如下参数：

$$\varepsilon(F)=\max_{a\in\{0,1\}^n\setminus S_F}\Pr_x[F(x)=F(x\oplus a)] \tag{5.2.6}$$

$\varepsilon(F)$刻画了F多接近满足广义 Simon 条件。特别地，若$\varepsilon(F)=0$，则F即满足广义 Simon 条件。

证明了只要$\varepsilon(F)$随n的增大不无限趋于 1，则 Simon 仍以接近 1 的概率能够求出F的周期空间。具体定理如下：

定理 5.2.1. 设$F:\{0,1\}^n\to\{0,1\}^m$为多输出布尔函数，周期空间为S_F，若对F运行 Simon 子程序cn次得到cn个输出$u_1,u_2,\cdots,u_{cn}$，且S为以下线性方程组的解空间：

$$\begin{cases}x\cdot u_1=0\\ x\cdot u_2=0\\ \vdots\\ x\cdot u_{cn}=0,\end{cases} \tag{5.2.7}$$

则$S_F\subseteq S$。进一步，若存在常数p_0使得$\varepsilon(F)\le p_0<1$，则$S_F\neq S$的概率不超过$(2(\frac{1+p_0}{2})^c)^n$。

由此定理可以看出，只要参数c的值大于等于$\lceil\ln 2/\ln\frac{2}{1+p_0}\rceil$，则除去一个可忽略的几率，解空间$S$将等于周期空间$S_F$。

求解线性结构的量子算法

量子中间相错攻击需要求解布尔函数的线性结构，而不只是周期。因此需要扩展 Simon 算法以求解布尔函数的线性结构。设$F:\{0,1\}^n \to \{0,1\}^m$为一个多输出布尔函数，为了求解$F$的线性结构，定义如下函数

$$W:\{0,1\}^n \times \{0,1\}^m \to \{0,1\}^m$$
$$(x,y) \quad \to F(x) \oplus y$$

若(a,b)为F的一个线性结构对，则

$$W(x,y) \oplus W(x \oplus a, y \oplus b) = F(x) \oplus F(x \oplus a) \oplus b = 0,$$

即(a,b)为W的周期。反之，若(a,b)为W的周期，容易验证(a,b)也是F的一个线性结构对。因此，F的线性结构空间L_F实际上是W的周期空间S_W，可以通过应用 Simon 算法于W来求解F的线性结构空间。

基于此，提出求给定布尔函数线性结构的量子算法 FindStru 总结如下：

算法 FindStru

输入：攻击者选择的常数c，布尔函数$F:\{0,1\}^n \to \{0,1\}^m$的量子预言机。

输出：F的线性结构空间L_F的一组基。

1.定义函数$W(x,y) = F(x) \oplus y$。由于可以访问F的量子预言机，W的量子预言机也可获得。

2.对W执行 Simon 子程序$c(n+m)$次得到$c(n+m)$个测量输出$u_1, \cdots, u_{c(n+m)} \in \{0,1\}^{n+m}$。解线性方程组

$$\begin{cases} (x,y) \cdot u_1 = 0 \\ (x,y) \cdot u_2 = 0 \\ \vdots \\ (x,y) \cdot u_{c(n+m)} = 0, \end{cases} \tag{5.2.8}$$

设$\{(a_1,b_1),(a_2,b_2),\cdots,(a_t,b_t)\}$为线性方程组的基础解系，输出该集合。

根据定理 5.2.1，算法 FindStru 的输出$\{(a_1,b_1),(a_2,b_2),\cdots,(a_t,b_t)\}$是周期空间$S_W$的一组基。由于$S_W = L_F$，它也是$F$的线性结构空间的一组基。为了分析算法 FindStru 的成功概率，考虑参数$\varepsilon(W)$。由W的定义，有

$$\begin{aligned} \varepsilon(W) &= \max_{(a,b) \in \{0,1\}^{n+m} \setminus S_W} \Pr_{x,y}[W(x,y) = W(x \oplus a, y \oplus b)] \\ &= \max_{(a,b) \in \{0,1\}^{n+m} \setminus L_W} \frac{1}{2^n} |\{x \in \{0,1\}^n \mid F(x) \oplus F(x \oplus a) = b\}| \\ &= \max_{(a,b) \in \{0,1\}^{n+m} \setminus L_W} \Pr_x[F(x) \oplus F(x \oplus a) = b]。 \end{aligned} \tag{5.2.9}$$

对任意布尔函数$F:\{0,1\}^n \to \{0,1\}^m$，定义新参数

$$\delta(F) = \max_{(a,b) \in \{0,1\}^{n+m} \setminus L_F} Pr_x[F(x) \oplus F(x \oplus a) = b] \tag{5.2.10}$$

则该参数刻画了$\{0,1\}^{n+m}$中属于L_F的线性结构空间的向量与其他向量可以被区分开的程度。由于$\varepsilon(W) = \delta(F)$，$\delta(F)$越小，算法 FindStru 找到$F$的线性结构的概率越大。以下定理可以直接由定理 1 得到：

设$F:\{0,1\}^n \to \{0,1\}^m$为多输出的布尔函数，$F$的线性结构空间为$L_F$。设对$F$以参数$c$运行算法 FindStru 输出$\{(a_1,b_1),(a_2,b_2),\cdots,(a_t,b_t)\}$。令

$$L = span\{(a_1,b_1),(a_2,b_2),...,(a_t,b_t)\}, \tag{5.2.11}$$

则$L_F \subseteq L$。进一步，若存在常数p_0使得$\delta(F) \leq p_0 < 1$，则$L_F \neq L$成立的概率至多$(2(\frac{1+p_0}{2})^c)^{n+m}$。

（2）量子中间相错攻击

中间相错技术是求分组密码不可能差分的重要方法。它的基本思想是找到两个分别从密码底端和顶端以概率 1 传播至中部并在中部不匹配的差分，将两个差分拼接即为整个分组密码的不可能差分。

设E是任意r轮分组密码，分组长度为n。记F为E的前$r-1$轮构成的映射，$\mathcal{K}$为F对应的密钥空间，即E的前$r-1$轮的子密钥空间。F的输入包括一个$\mathcal{K}$中的密钥和一个明文$x \in \{0,1\}^n$。固定一个密钥$k \in \mathcal{K}$，F对x的作用即为$F_k(x)$。设$F_k(x) = y,$，$F_k(x') = y'$，则$\Delta x = x \oplus x'$为输入差，$\Delta y = y \oplus y'$为输出差。$(\Delta x, \Delta y)$被称为F_k的一个差分。若

$$F_k(x \oplus \Delta x) \oplus F_k(x) \neq \Delta y, \ \forall x \in \{0,1\}^n, \tag{5.2.12}$$

则$(\Delta x, \Delta y)$为F_k的一个不可能差分。在不可能差分分析中，攻击者需要先找到F_k的某个不可能差分$(\Delta x, \Delta y)$，再利用它筛选最后一轮的子密钥。然而，由于密钥k是保密的，攻击者实际上无法对函数$F_k: \{0,1\}^n \to \{0,1\}^n$进行量子询问。对攻击者而言只有不指定密钥的加密函数$F: \mathcal{K} \otimes \{0,1\}^n \to \{0,1\}^n$是已知的。对此，可以求密钥独立的不可能差分。密钥独立的不可能差分定义如下：

设分组密码为$F: \mathcal{K} \otimes \{0,1\}^n \to \{0,1\}^n$，密钥空间为$\mathcal{K}$。$(\Delta x, \Delta y)$被称为$F$的密钥独立的不可能差分，若对任意$k \in \mathcal{K}$和$x \in \{0,1\}^n$，成立

$$F(k, x \oplus \Delta x) \oplus F(k, x) \neq \Delta y \tag{5.2.13}$$

密钥独立的概率 1 差分定义类似：

设分组密码为$F: \mathcal{K} \otimes \{0,1\}^n \to \{0,1\}^n$，密钥空间为$\mathcal{K}$。$(\Delta x, \Delta y)$被称为$F$的密钥独立的概率 1 差分，若对任意$k \in \mathcal{K}$和$x \in \{0,1\}^n$，成立

$$F(k, x \oplus \Delta x) \oplus F(k, x) = \Delta y \tag{5.2.14}$$

显然$(\Delta x, \Delta y)$为F的密钥独立的概率 1 差分当且仅当$((0, \Delta x), \Delta y)$为$F$的线性结构对，这里 0 表示$\mathcal{K}$中的零向量。

中间相错攻击技术通过连接两端不匹配的概率 1 差分来寻找不可能差分。具体地，对任意$v \in \{1, \cdots, r-2\}$，将F分解为两部分：$F = \check{F}_v \cdot \hat{F}_v$，其中$\hat{F}_v$对应$F$的前$v$轮，$\check{F}_v$对应$F$的后$r-1-v$。密钥空间$\mathcal{K}$也被相应地分为两部分$\mathcal{K} = \mathcal{K}_v^1 \otimes \mathcal{K}_v^2$。$\hat{F}_v$将$\mathcal{K}_v^1 \otimes \{0,1\}^n$映射到$\{0,1\}^n$，而$\check{F}_v$将$\mathcal{K}_v^2 \otimes \{0,1\}^n$映射到$\{0,1\}^n$。固定一个密钥$k \in \mathcal{K}_v^2$，$\check{F}_v$对$x$的作用表示为$\check{F}_{v,k}(x)$。定义函数

$$\begin{aligned} \check{F}_v^{(-1)}: \mathcal{K}_v^2 \times \{0,1\}^n &\to \{0,1\}^n \\ (k \ , \ y) &\to (\check{F}_{v,k})^{-1}(y), \end{aligned} \tag{5.2.15}$$

其中$(\check{F}_{v,k})^{-1}$为函数$\check{F}_{v,k}$的逆，即为F后$r-1-v$轮在子密钥k下的解密函数。若$(\Delta x_1, \Delta y_1)$和$(\Delta x_2, \Delta y_2)$分别为$\hat{F}_v$和$\check{F}_v^{(-1)}$的密钥独立的概率 1 差分，且$\Delta y_1 \neq \Delta y_2$，则$(\Delta x_1, \Delta x_2)$为$F$密钥独立的不可能差分。因此中间相错攻击技术将寻找密钥独立的不可能差分的任务转化为寻找

密钥独立的概率 1 差分。

求解概率 1 差分的量子算法

为了构造量子中间相错攻击算法，需要先构造求分组密码密钥独立的概率 1 差分的量子算法。设F和$\mathcal{K}$给定，由于向量$((0,\Delta x),\Delta y)$为F的线性结构对当且仅当$(\Delta x,\Delta y)$为F的密钥独立的概率 1 差分，可以应用算法 FindStru 于F求它的密钥独立概率 1 差分。唯一的问题是，希望算法找到的线性结构对$((\Delta k,\Delta x),\Delta y)$满足$\Delta k=0$，这里分段$\Delta k$为密钥比特对应的差。为此，算法 FindStru 需要稍作修改。设$\mathcal{K}=\{0,1\}^m$，求分组密码密钥独立概率 1 差分的量子算法步骤如下：

算法 FindPr1Diff

输入：攻击者选择的常数c，分组密码$F:\{0,1\}^m\otimes\{0,1\}^n\to\{0,1\}^n$及密钥空间$\mathcal{K}=\{0,1\}^m$，函数$F$的量子线路。

输出：F的密钥独立的概率 1 差分。

1. 定义函数如下

$$\begin{aligned} W&:\{0,1\}^n\times\{0,1\}^m\to\{0,1\}^m\\ &(x,y)\quad\to F(x)\oplus y \end{aligned}\tag{5.2.16}$$

2.对W运行 Simon 子程序$c(2n+m)$次得到$c(2n+m)$个测量输出$u_1,\cdots,u_{c(2n+m)}\in\{0,1\}^{2n+m}$。解线性方程组

$$\begin{cases}(x,y)\cdot(u_{1,m+1},u_{1,m+2}\cdots,u_{1,2n+m})=0\\(x,y)\cdot(u_{2,m+1},u_{2,m+2}\cdots,u_{2,2n+m})=0\\\vdots\\(x,y)\cdot(u_{c(2n+m),m+1},u_{c(2n+m),m+2}\cdots,u_{c(2n+m),2n+m})=0,\end{cases}\tag{5.2.17}$$

其中对$j=1,2,\cdots,c(2n+m)$，$(u_{j,m+1},u_{j,m+2}\cdots,u_{j,2n+m})$为向量$u_j$的后$2n$比特。设$\{(a_1,b_1),(a_2,b_2),\cdots,(a_t,b_t)\}$为线性方程组的一个基础解系，输出该集合。

令$L=\text{span}\{(a_1,b_1),(a_2,b_2),\cdots,(a_t,b_t)\}$。下面定理说明，除去可忽略的概率，$L$为$F$所有密钥独立的概率 1 差分构成的集合。

定理 5.2.2.设分组密码$F:\{0,1\}^m\otimes\{0,1\}^n\to\{0,1\}^n$的密钥空间为$\mathcal{K}=\{0,1\}^m$。对$F$以参数$c$运行算法 FindPr1Diff 输出集合$\{(a_1,b_1),(a_2,b_2),\cdots,(a_t,b_t)\}$。令

$$L=span\{(\mathrm{a}_1,\mathrm{b}_1),(\mathrm{a}_2,\mathrm{b}_2),...,(\mathrm{a}_t,\mathrm{b}_t)\},$$

则L包含F的所有密钥独立的概率 1 差分。进一步，若存在常数p_0使得$\delta(F)\le p_0<1$，则L中包含非F密钥独立概率 1 差分的向量的概率至多$(2(\frac{1+p_0}{2})^c)^{2n+m}$。

证明注意到(a,b)是

$$\begin{cases}(x,y)\cdot(u_{1,m+1},u_{1,m+2}\cdots,u_{1,2n+m})=0\\(x,y)\cdot(u_{2,m+1},u_{2,m+2}\cdots,u_{2,2n+m})=0\\\vdots\\(x,y)\cdot(u_{c(2n+m),m+1},u_{c(2n+m),m+2}\cdots,u_{c(2n+m),2n+m})=0,\end{cases}\tag{5.2.18}$$

的解等价于$(0,a,b)$为

$$\begin{cases}(k,x,y)\cdot u_1=0\\(k,x,y)\cdot u_2=0\\\vdots\\(k,x,y)\cdot u_{c(2n+m)}=0\\k=0^m.\end{cases}\tag{5.2.19}$$

的解，$\{(0^m,a_1,b_1),(0^m,a_2,b_2),\cdots,(0^m,a_t,b_t)\}$可以被看作前$m$比特为 0 的附加条件下，运行算法 FindStru 于F的输出。令

$$L_F^0=\{(\Delta k,\Delta x,\Delta y)|(\Delta k,\Delta x,\Delta y)\text{是}F\text{的线性结构对}\wedge\Delta k=0^m\}$$

因此L_F^0为线性结构空间L_F的子空间。

令$L'=\text{span}\{(0^m,a_1,b_1),(0^m,a_2,b_2),\cdots,(0^m,a_t,b_t)\}$由定理 5.2.2，$L'\subseteq L_F^0$，且$L'\neq L_F^0$的概率至多$(2(\frac{1+p_0}{2})^c)^{2n+m}$，由于$(\Delta x,\Delta y)$为$F$密钥独立的概率 1 差分当且仅当$((0^m,\Delta x),\Delta y)$为$F$的线性结构对，$L$包含$F$的所有密钥独立的概率 1 差分，且$L$包含其他向量的概率至多$(2(\frac{1+p_0}{2})^c)^{2n+m}$.

求解不可能差分的量子算法

为了求解分组密码F的密钥独立的不可能差分，对每个$v\in\{1,\cdots,r-2\}$，将F分为两部分$F=\check{F}_v\cdot\hat{F}_v$，分别具有密钥空间$\mathcal{K}_v^1$和$\mathcal{K}_v^2$。如前所述，若$(\Delta x_1,\Delta y_1)$和$(\Delta x_2,\Delta y_2)$分别为$\hat{F}_v$和$\check{F}_v^{(-1)}$密钥独立的概率差分，且$\Delta y_1\neq\Delta y_2$，则$(\Delta x_1,\Delta x_2)$为$F$的密钥独立的不可能差分。因此，通过将算法 FindPr1Diff 应用于$\hat{F}_v$和$\check{F}_v^{(-1)}$分别得到它们的概率 1 差分，即可求得F的密钥独立不可能差分。

给定分组密码F和密钥空间$\mathcal{K}=\{0,1\}^m$，求F的密钥独立不可能差分的量子算法如下：

算法 **FindImDiff**

输入：攻击者选择的常数c，分组密码$F:\{0,1\}^m\otimes\{0,1\}^n\to\{0,1\}^n$及密钥空间$\mathcal{K}=\{0,1\}^m$。

输出：F的密钥独立不可能差分。

1.对$v=1,2,\cdots,r-2$，将F按前述方法分解为两部分：$F=\check{F}_v\cdot\hat{F}_v$。由于$F$是公开的，每个$\check{F}_v$和$\hat{F}_v$的量子线路是可获得的。对每个$v=1,2,\cdots,r-2$，执行如下步骤：

1-1.选取常数c，运行算法 FindPr1Diff 于$\hat{F}_v$及密钥空间$\mathcal{K}_v^1$，得到集合A_v。

1-2.选取常数c，运行算法 FindPr1Diff 于$\check{F}_v^{(-1)}$及密钥空间$\mathcal{K}_v^2$，得到集合B_v。

2.初始化集合 H 为空集。对$v=1,2,\cdots,r-2$执行如下步骤：

对任意$(\Delta x_1,\Delta y_1)\in spanA_v$，任意$(\Delta x_2,\Delta y_2)\in spanB_v$，若$\Delta x_1\neq 0$，$\Delta x_2\neq 0$和$\Delta y_1\neq\Delta y_2$，令$H=H\cup\{(\Delta x_1,\Delta x_2)\}$。

3.输出集合H。

由于函数F是公开的，攻击者可以构造执行$\check{F}_v$和$\hat{F}_v$的量子线路。因此，算法 FindImDiff 不需要对分组密码进行任何量子或经典的加密询问（尽管攻击者确实需要在随后不可能差分攻击的密钥恢复阶段进行经典的加密询问）。与许多已提出的量子攻击相比，本攻击不需要敌手具有对量子叠加态进行询问的能力，更符合敌手的实际攻击能力。

（3）算法性能分析

为了分析算法 FindImDiff 的成功概率及复杂度，首先定义参数

$$\hat{\delta}(F)=\max\{\delta(\hat{F}_v),\delta(\check{F}_v^{(-1)}):1\le v\le r-2\},\tag{5.2.20}$$

其中$\delta(\hat{F}_v),\delta(\check{F}_v^{(-1)})$如式(2)定义。对任意$v\in\{1,2,\cdots,r-2\}$，$\hat{F}_v$和$\check{F}_v^{(-1)}$都是分组密码$E$的约减版本，分别具有$v$轮和$r-1-v$轮。参数$\delta(\hat{F}_v)$刻画了$\hat{F}_v$的线性结构对与其他向量的距离。因此，$\hat{\delta}(F)$刻画了$E$的约减版本的线性结构对可以与其他向量区分开的程度。下面定理可以直接由定理 2 得到。

定理 5.2.3.设$F:\{0,1\}^m\otimes\{0,1\}^n\to\{0,1\}^n$为分组密码，密钥空间为$\mathcal{K}=\{0,1\}^m$，且存在常数$p_0$使得$\hat{\delta}(F)\le p_0<1$。若以参数$c$运行算法 FindImDiff 于$F$输出集合$H$，则$H$包含非$F$的密钥独立不可能差分的向量的概率至多$2(2(\frac{1+p_0}{2})^c)^{2n}$。

条件$\hat{\delta}(F)\le p_0<1$可以理解为要求所有非E的约减版本的线性结构对的向量远离成为其线性结构对。定理 3 表明，在该条件下H中的向量以接近 1 的概率为F的密钥独立的不可能差分。事实上，由定理 5.2.3 可以得到更进一步的结论：只要F具有由两个不匹配概率 1 差分构成的密钥独立不可能差分，算法 FindImDiff 就一定能输出该差分，无论$\hat{\delta}(F)$是否小于一个小于 1 的常数。

为解释这一点，设F有一个密钥独立的不可能差分$(\Delta x_1,\Delta x_2)$，且$(\Delta x_1,\Delta x_2)$由两个不匹配的概率 1 差分构成。则存在$v\in\{1,2,\cdots,r-2\}$、Δy_1和Δy_2使得$\Delta y_1\neq\Delta y_1$，且$(\Delta x_1,\Delta y_1)$和$(\Delta x_2,\Delta y_2)$分别为$\hat{F}_v$和$\check{F}_v^{(-1)}$的密钥独立的概率 1 差分。由定理 2，$(\Delta x_1,\Delta y_1)$必须属于集合 spanAv，$(\Delta x_2,\Delta y_2)$必须属于集合 spanBv。因此，$(\Delta x_1,\Delta x_2)$属于算法 FindImDiff 输出的集合H。这意味着F的所有由两个不匹配概率 1 差分构成的密钥独立的不可能差分都可由算法 FindImDiff 求出。因此，在某种程度上，可以说若经典的中间相错攻击算法对某个分组密码有效，则提出的量子中间相错攻击算法也将有效。

考虑算法 FindImDiff 的复杂度。FindImDiff 不需要对分组密码进行加密询问，无论是量子的还是经典的。分三个部分计算算法 FindImDiff 的复杂度：通用门的个数、需要的量子比特数和经典计算部分的复杂度。

为了计算量子通用门的个数，设$\mathcal{K}_1^v=\{0,1\}^{l_v}$，$\mathcal{K}_2^v=\{0,1\}^{h_v}$，其中$l_v+h_v=m$。运行算法 FindPr1Diff 于$\hat{F}_v$需要调用 Simon 子程序$c(2n+l_v)$次，每次执行需要$2(2n+l_v)$个 Hadamard 门、$n$个单量子 CNOT 门和$|\hat{F}_v|_Q$个通用量子门。同理运行算法 FindPr1Diff 于$\check{F}_v^{(-1)}$需要调用 Simon 子程序$c(2n+h_v)$次，每次总共执行$2(2n+h_v)+n+|\check{F}_v^{(-1)}|_Q$个通用量子门。由于$l_v+h_v=m$，以及$|\hat{F}_v|_Q+|\check{F}_v^{(-1)}|_Q=|\hat{F}_v|_Q+|\check{F}_v|_Q=|F|_Q$。简单计算可知，算法 FindImDiff 需要执行的通用量子门总数为

$$c(r-2)(2n+m)(10n+2m+|F|_Q),\tag{5.2.21}$$

由于F为对应分组密码E前$r-1$轮的加密函数，它可以由量子线路有效执行，$|F|_Q$为n的多项式。因此，算法 FindImDiff 需要的通用量子门的总数是安全参数n的多项式。

运行算法 FindPr1Diff 于$\hat{F}^{(v)}$需要$2n+l_v+n=3n+l_v$量子比特，运行算法 FindPr1Diff 于$(\check{F}^{(v)})^{-1}$需要$2n+h_v+n=3n+h_v$量子比特。由于$l_v,h_v\le m$且量子比特可以重复使用。执行算法 FindImDiff 至多需要$3n+m$量子比特。

算法 FindImDiff 的经典计算部分包含两部分：解线性方程组；计算集合H。对于第二个部分，由于$\hat{F}_v$、$\check{F}_v$都为E的约减版本，它们具有的概率 1 差分通常很少。令$\alpha=$

$max_v\{|spanA_v|,|spanB_v|\}$。$\alpha$可以被看做是一个较小的数。计算集合$H$需要的计算量为$O((r-2)\alpha^2 n)$。至于求线性方程组的部分，运行算法 FindPr1Diff 于$\hat{F}_v$需要解一个有$c(2n+l_v)$个方程和$2n+l_v$个变量的线性方程组。这需要$O(c(2n+l_v)^3)$的计算量。同理，运行算法 FindPr1Diff 于$\check{F}_v^{(-1)}$时解线性方程组需要$O(c(2n+h_v)^3)$的计算量。因此，解线性方程组需要的计算量总共为

$$\begin{aligned} & \sum_{v=1}^{r-2}[\,c(2n+l_v)^3+c(2n+h_v)^3] \\ \leq\ & c\sum_{v=1}^{r-2}(4n+l_v+h_v)^3 \\ =\ & c(r-2)(4n+m)^3。 \end{aligned} \tag{5.2.22}$$

经典计算部分需要的计算量为$O((r-2)[c(4n+m)^3+\alpha^2 n])$，其中$\alpha$为一个较小的数。

（4）小结

研究量子算法与经典分析工具的结合，将 Simon 算法应用于中间相错攻击技术，提出一个用于寻找分组密码不可能差分的量子算法。提出的量子中间相错攻击算法的复杂度为多项式规模，且不需要对分组密码进行加密询问，无论是经典的询问还是量子询问。

为了论证算法的可行性，证明只要分组密码满足一定的代数性质，算法输出的差分将以趋于 1 的概率为分组密码的不可能差分。同时，论证了只要分组密码具有由两个不匹配的概率 1 差分构成的密钥独立的不可能差分，算法一定输出该差分。因此，一定程度上可以说传统的中间相错攻击能够求出的不可能差分，量子中间相错攻击算法也一定能够输出。传统的中间相错攻击技术中，无论攻击者通过寻找概率 1 的差分路径来求解概率 1 差分，还是通过直接分析整体加密函数的代数性质来寻找概率 1 差分，随着轮数的增加，整体加密函数更加复杂，求高概率差分的难度都将急剧增大。与此相比，量子中间相错攻击技术将约减的分组密码看作一个整体黑盒地执行量子算法，一定程度上避免了轮数增加带来的复杂性。

5.2.3Grover 算法与 Simon 算法结合

2017 年，亚密 17 上，Leander Gregor 和 AlexanderMay 第一次给出了使用 Grover 算法结合 Simon 算法恢复 FX 结构（$E(x)=E_{k_0}(x\oplus k_1)\oplus k_2$）的密钥三元组$(k_0,k_1,k_2)$的攻击方法[21]。攻击算法的核心是使用 Grover 算法搜索k_0，即首先通过并行版本的 Simon 算法的后处理过程（判断向量组构成的空间维数）作为识别 oracle 实现对k_0的标记，然后通过迭代对k_0进行幅度增强。之后测量得到k_0后使用 Simon 算法的方程组计算容易得到k_1，经过 check 步骤验证成立后，很容易就可以得到k_2。2018 年，受到 Leander 两人的启发，王小云等人将 Kuwakado 和 Morri 构造的三轮 Feistel 结构的量子区分器与 Grover 算法结合，第一次考虑了对 Feistel 结构进行密钥恢复攻击，攻击r轮密码需要$2^{(0.25nr-0.75n)}$次量子询问[22]。随后，王小云等人研究广义 Feistel 结构的量子区分器，对 d-branch Type-1 的 GFS 结构构造$2d-1$轮的多项式时间量子区分器，对 2d-branch Type-2 GFS 结构构造$(2d+1)$轮量子区分器[23]。2019 年，基于 Simon 算法，GembuIto[24]等人给出了对r轮 Feistel 密码的选择密文攻击。首先，对 Kuwakado 和 Morri 在量子选择明文攻击下使用 Simon 算法构造的三轮区分器拓展一轮，给出了在量子选择密文攻击下对 4 轮 Feistel 结构和随机置换的量子区分器，在多项式次询问后达到区分目的。然后使用 Grover 算法猜测剩下的$r-4$轮的密钥。相比于之前使用 Simon 算法进行攻击的方法，这里使用的 Simon 算法是不用恢复周期的，也就避免了 Kaplan 等人在[18]中提出的对多余碰撞概率的计算。2020 年，董晓阳等人

[26]结合 Simon 算法和 Grover 算法对 GOST 密码方案实现了全轮密钥恢复，相比于直接使用 Grover 穷搜降低了$2^{13.2}$的复杂度。董晓阳只考虑在 Q2 模型下量子敌手对 GOST 算法的后 30 轮（第 3-32 轮）的攻击。

上面给出的攻击基本都是在 Q2 模型下进行的，并没有考虑敌手只有经典 oracle 访问权限的 Q1 模型下的攻击，然而 Q2 模型的实际性不大。加之，目前小内存的量子计算机才具有可能性。所以，考虑到攻击的实际性，应当考虑使用多项式量子比特的在 Q1 模型下的攻击。最近，Xavier 等人[25]给出了基于 Grover 结合 Simon 算法的思想，通过将在线访问和离线计算阶段分离给出了离线 Simon 算法用于密码分析的概念。第一次给出了在 Q1 模型下的攻击，并且优化了 Q2 模型下的原有的攻击。在 Q1 模型下，敌手将在线访问阶段得到的经典数据制备成量子叠加态。离线计算阶段，Q1 和 Q2 模型都是通过重用叠加态来降低量子访问次数。

5.2.4 基于 Bernstein-Vazirani 算法的量子攻击

Bernstein-Vazirani 算法（下面简称为 BV 算法）一次运行就可以求出一个形式为$f(x) = a \cdot x$的布尔函数的a。又因为对对称密码来说，研究布尔函数的意义巨大。理解布尔函数的线性结构对设计密码算法和进行密码分析有很重要的意义。故将 BV 算法应用于密码分析成为很自然的方向，在量子差分分析方面已有一些研究成果，这些成果一定程度上反应了量子算法与经典密码分析工具相结合的优势。

Floess 等人在[27]中证明了：如果一个布尔函数$f(x_1, x_2, \dots, x_n)$并不依赖于输入变量x_i，那么对函数f应用 BV 算法得到的第i位一定为 0。[28]拓展了 Floess 等人的结果，并且证明了 BV 算法输出结果在每个位置i上为 1 的概率等于x_i对布尔函数f的影响因子。以此为基础，给出了计算布尔函数的任意变量的影响因子的逼近算法，并将此逼近算法应用到某些带有 junta 的布尔函数。相比于[27]的确定性算法，[28]给出的概率算法速度更快。

布尔函数的线性结构对应于分组密码的高概率差分。[29]提出了两种将 BV 算法应用到差分分析的方法并且给出了对算法的分析。第一种是使用量子算法对每个 S 盒寻找到高概率的差分。另一种方法是将加密看做一个整体。这一算法的主要特点是可以用于对所处理的布尔函数不做任何限定假设的一般情形，从而为量子算法在分组码差分攻击上的应用奠定了基础。

根据[29]和[30]，对一个布尔函数运行不带测量的 BV 算法，将会产生所有状态$|\omega\rangle$ $(\omega \in \{0,1\}^n)$的叠加，每个$|\omega\rangle$的幅度将对应于谱变换值$S_f(\omega)$。另外布尔函数的线性结构和它的谱变换值之间还存在着关系。基于这样的观察，可以证明布尔函数线性结构组成的集合由所有 Walsh 谱不为零的向量表示的关系式，基于 BV 算法得到了一个用于逼近布尔函数线性结构的量子算法[31]。核心思想是基于使用 BV 算法识别线性结构[29]和使用 Simon 算法进行周期查找。这两个方法的结合给出了求解布尔函数线性结构集合的多项式时间的逼近。文中还说明了逼近的高概率如何随着运行次数的改变而变化。高概率求解布尔函数f的线性结构的时间与布尔函数f的相对差分均匀度δ_f有关。当δ_f越小，需要的时间越短。成果的最大优势是对布尔函数不做任何限定。

2019 年，文献[32]对[28]中的算法进行修改，给出了使用 BV 算法攻击分组密码的系统性的描述。文中，基于寻找布尔函数线性结构的算法给出了 3 轮 Feistel 结构的区分器并且

提出了恢复 EM 构造的部分密钥的新的量子算法。通过观察到布尔函数的线性结构是加密函数的高概率差分，将提出的量子算法应用到差分分析和不可能差分分析。另外，由于算法找到的线性结构是每个成员函数的线性结构，基于这个观察，谢惠琴提出了一个新的差分类型，叫做量子低概率差分。最后，算法高效性和成功概率的分析也分别被给出。因为文中提出的算法将加密函数当做一个整体，因此这避免了一般传统差分分析很难拓展路径的困难性。

下面简述[32]中的结果。假设分组密码有 r 轮，算法将前 r-1 轮对应的函数作为整体作用 Bernstein-Vazirani 算法，只关注分组密码的输入差分和倒数第二轮的输出差分。传统差分分析从寻找高概率差分路径出发，随着轮数的增加，寻找高概率差分路径的难度加大。算法只关注首尾的输入差和输出差，而不是找一条具体的高概率差分特征，一定程度上避免了因活跃盒个数增加而导致差分特征概率降低的问题。分组密码设计常采用的宽轨迹策略是通过增加活跃 S 盒的个数来降低差分特征或线性特征的概率，从而抵抗差分或线性分析。然而，不存在高概率差分特征不代表不存在高概率差分，[32]中提出的量子算法寻找的高概率不必要依赖于一条具体的高概率差分特征。因此，量子差分分析有可能抵抗宽轨迹策略。这为探索量子计算环境下的分组密码设计准则提供了一个思路。这一结果可推广至截断差分分析和不可能差分分析[33]。

由于布尔函数的周期是它的特殊的线性结构，许多基于 Simon 算法的分析算法可以类似地通过 BV 算法来完成，例如谢惠琴和杨理基于 BV 算法构造三轮 Feistel 体制的量子区分器。BV 算法更重要的应用在于差分分析。由于布尔函数的近似线性结构可以诱导出它的一个高概率差分，BV 算法可用于寻找高概率差分。传统差分分析从寻找高概率差分路径出发，随着轮数的增加，寻找高概率差分路径的难度加大，而应用 BV 算法时是将多轮的分组密码作为一个黑盒，只关心整体函数的首位差分，这在一定程度上可以减小轮数增长的影响。

Bernstein-Vazirani 算法对分组密码相关密钥攻击应用举例

基于 BV 算法研究量子计算环境下的相关密钥攻击，可给出一般分组密码的一个量子相关密钥攻击算法，并证明只要分组密码满足一定的代数性质，该攻击算法即可在多项式时间内恢复它的密钥[34]。为了论证算法成功的条件具有合理性，进一步证明若分组密码不满足该条件，则其存在一个量子区分攻击。最后，将量子相关密钥攻击算法应用于 Even–Mansour 密码。

相关密钥攻击模型赋予敌手要强于选择明文攻击的能力。在经典的相关密钥攻击模型中，敌手可以进行在不同密钥下的加密和解密询问，被询问的密钥与靶密钥具有一定的数学关系，这种关系称为密钥关系。最早，Winternitz 和 Hellman 研究的是在比特翻转密钥关系下的相关密钥攻击模型[36]。该攻击模型被用于 9 轮 Rijndael 密码[37]。随后，基于更一般的密钥关系的相关密钥攻击模型在中被研究。不少重要的密码算法在相关密钥攻击模型下可以被攻击，如用于 3G 保密和认证的 KASUMI[38-39]和用于 WIFI 无线网络的 Wired Equivalent Privacy（WEP）[40-41]。

量子相关密钥模型最早由 Roetteler 和 Steinwandt 提出。Hosoyamada 和 Aoki 随后进一步研究量子相关密钥攻击模型，并提出攻击 2 轮迭代的 Even–Mansour 体制的量子算法，该算法需要对相关密钥预言机进行两次询问[42]。

在这一章，进一步深入研究量子相关密钥攻击模型。基于 BV 算法，给出一般分组密码的一个量子相关密钥攻击算法，并证明只要分组密码满足一定的代数性质，该攻击算法即可

在多项式时间内恢复它的密钥[34]。为了论证算法成功的条件具有合理性，进一步证明若分组密码不满足该条件，则其存在一个量子区分攻击。最后，将量子相关密钥攻击算法应用于Even–Mansour 密码。

（1）基本概念

量子相关密钥攻击

设E为任意分组密码，分组长度为n，密钥长度为k。当指定密钥为$s \in \mathbb{F}_2^k$，E_s为从$\mathbb{F}_2^n$到$\mathbb{F}_2^n$的置换。假设E可由量子算法有效执行，即存在多项式时间的量子线路，以密钥和明文为输入，并输出相应的密文态。该线路实际实现以下酉算子：

$$U_E: \sum_{m,x,y} |x\rangle|m\rangle|y\rangle \to \sum_{m,x,y} |x\rangle|m\rangle|y \oplus E_x(m)\rangle \tag{5.2.23}$$

该假设对实际应用的分组密码都成立。由于U_E的执行不涉及密钥s，任何人都可以执行U_E的量子线路，包括敌手。

由于酉量子门$\{H, CNOT, Phase, \frac{\pi}{8}\}$为量子通用门集，可以假设$U_E$的量子线路由该集合中的量子门构成。这里，$H$为 Hadamard 门，$CNOT$为受控非门，$Phase$为相位门，$\frac{\pi}{8}$为$\frac{\pi}{8}$门。令$|E|_Q$表示$E$的量子线路中通用门的个数，则$|E|_Q$为安全参数$n$的一个多项式。攻击者可以将$U_E$集成到他的量子线路中，如图 5.2-1。

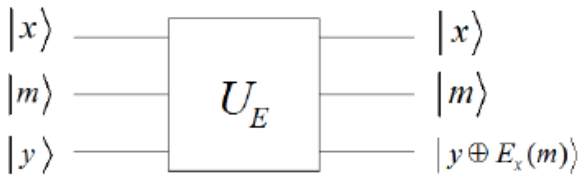


图 5.2-1 量子门U_E

首先回顾中提出的经典相关密钥攻击模型，密钥关系为比特翻转。在该模型中，给定密钥$s \in \mathbb{F}_2^k$后，敌手可以询问以下两个预言机：

$\mathcal{E}$: 输入明文$m \in \mathbb{F}_2^n$和掩码$x \in \mathbb{F}_2^k$，$\mathcal{E}$返回密文$E_{s\oplus x}(m)$。

$\mathcal{D}$: 输入密文$c \in \mathbb{F}_2^n$和掩码$x \in \mathbb{F}_2^k$，$\mathcal{D}$返回解密$E_{s\oplus x}^{-1}(c)$。

通过询问这些预言机，敌手最后输出一个向量$s' \in \mathbb{F}_2^k$作为对靶密钥s的猜测。攻击者成功当且仅当$s' = s$。

提出的相关密钥攻击算法不需要敌手询问解密预言机$\mathcal{D}$，但敌手可以用密钥的叠加态询问$\mathcal{E}$，即敌手可以询问如下作用的量子预言机$\mathcal{O}_\mathcal{E}$：

$$\mathcal{O}_\mathcal{E}: \sum_{x,m,y} |x\rangle|m\rangle|y\rangle \to \sum_{x,m,y} |x\rangle|m\rangle|y \oplus E_{s\oplus x}(m)\rangle. \tag{5.2.24}$$

该攻击模型被称为量子相关密钥攻击模型。攻击者可以将$\mathcal{O}_\mathcal{E}$集成到他的线路。我们还允许敌手询问只返回密文的单个比特的预言机。具体地，假设$E_{s\oplus x} = (E_{s\oplus x,1}, E_{s\oplus x,2}, \cdots, E_{s\oplus x,n})$，其中$E_{s\oplus x,1}, \cdots, E_{s\oplus x,n}$都是单比特输出的布尔函数。则对任意的$j = 1,2,\cdots,n$，攻击者可以询问以下量子预言机：

$$\mathcal{O}_{\varepsilon_j}:\sum_{x,m,y}|x\rangle|m\rangle|y\rangle \to \sum_{x,m,y}|x\rangle|m\rangle|y\oplus E_{s\oplus x,j}(m)\rangle。 \quad (5.2.25)$$

敌手可以用量子叠加态询问密码原语的情况在许多文献中被考虑。对量子预言机$\mathcal{O}_{\mathcal{E}}$的权限意味着敌手可以询问带密钥$s$的加密预言机。即敌手可以询问预言机

$$\mathcal{O}_{E_s}:\sum_{m,y}|m\rangle|y\rangle \to \sum_{m,y}|m\rangle|y\oplus E_s(m)\rangle. \quad (5.2.26)$$

为此，他只需要用量子态$\sum_{m,y}|\mathbf{0}\rangle|m\rangle|y\rangle$询问预言机$\mathcal{O}_{\mathcal{E}}$，然后丢弃第一个寄存器。因此，量子相关密钥攻击模型可以看作是量子选择明文攻击的扩展。

求线性结构的量子算法

2013 年文献[15]提出首个求布尔函数线性结构的量子算法。设$F=(F_1,F_2,\cdots,F_n)\in\mathcal{C}_{k,n}$。对每个$j=1,2,\cdots,n$，该算法首先调用 BV 算法于$F_j$得到$N_{F_j}$的一个子集，再利用这个子集解线性方程组求得$F_j$的线性结构，最后算法随机选择$F_1,F_2,\cdots,F_n$中的一个公共非零向量并输出。为了能够应用于量子相关密钥攻击，对该量子算法进行小的修改，使其输出包含F的所有线性结构的集合，而非一个随机的线性结构。改进的算法如下：

算法 FindStruct

初始化：$p(n)$为敌手选择的多项式。$F=(F_1,F_2,\cdots,F_n)\in C_{k,n}$，敌手可以访问每个$F_j(1\le j\le n)$的量子预言机。

1.对每个$j=1,2,\cdots,n$，对每个F_j应用 BV 算法$p(n)$次得到N_{F_j}的子集W_j，集合W_j的大小是$p(n)$。

2.对每个$j=1,2,\cdots,n$，对$i_j=0,1$，解线性方程组$\{x\cdot\omega=i|\omega\in W_j\}$得到解集$A_j^{i_j}$，令$A_j^{i_j}=A_j^0\cup A_j^1$。

3.求交集$\bar{A}=A_1\cap A_2\cap\cdots\cap A_n$。对每个$a\in\bar{A}$，令$\tilde{a}=(i_1,i_2,\cdots,i_n)$，其中$i_1,i_2,\cdots,i_n$为使得$a\in A_1^{i_1}\cap A_2^{i_2}\cap\cdots\cap A_n^{i_n}$成立的指标。令$A=\{(a,\tilde{a})|a\in\bar{A}\}$，输出集合$A$。

在上面算法中，敌手在第 2 步计算集合$A_j=A_j^0\cup A_j^1$时实际需要对A_j中的每个向量附加上一个标签。具体地，若$a\in A_j^0$，则当a被放入集合A_j时加上了标签$i_j=0$；若$a\in A_j^1$，则当a被放入集合A_j时加上了标签$i_j=1$。随后，在敌手计算集合$\bar{A}$时，对每个$a\in A_1\cap A_2\cap\cdots\cap A_n$，将相应的$n$个标签$i_1,i_2,\cdots,i_n$附于$a$放入$\bar{A}$。因此，在计算集合$A$时，敌手可以通过查看这些标签很容易地得到每个$a\in\bar{A}$相应的指标$\tilde{a}$。这些标签是用于避免要指数多次计算$n$个集合的交集。借用这些标签，敌手只需计算交集$\bar{A}=A_1\cap A_2\cap\cdots\cap A_n$一次即可得到$A$。而若没有这些标签，敌手需要对每个$i_1,i_2,\cdots,i_n\in\{0,1\}$都计算一次交集$A_1^{i_1}\cap A_2^{i_2}\cap\cdots\cap A_n^{i_n}$以获得属于$U_F^{(i_1,\cdots,i_n)}$的线性结构。

以下定理说明了算法 FindStruct 的可行性.

定理 5.2.4 设$F=(F_1,F_2,\cdots,F_n)\in C_{k,n}$，$a$为$F$的任一线性结构。令$\alpha$为满足$a\in U_F^{\alpha}$的向量。若运行算法 FindStruct 于$F$得到集合$A$，则$(a,\alpha)$一定属于集合$A$。

定理 5.2.5 设$F=(F_1,F_2,\cdots,F_n)\in C_{k,n}$，$a$为$F$的任一线性结构。令$\alpha$为满足$a\in U_F^{\alpha}$的向量。

若运行算法 FindStruct 于F得到集合A，则(a,α)一定属于集合A。

定理 5.2.5 表明F的所有线性结构都属于输出集合A。注意到向量$\mathbf{0}$为F的平凡的线性结构，集合A总是分空。定理 3.2 说明，在条件$\delta_F \le p_0 < 1$下，算法 FindStruct 输出的集合A中的向量，除去一个可忽略的概率，为F的线性结构。

（2）量子相关密钥攻击算法

在这一节，在量子相关密钥模型下给出分组密码的一个量子攻击算法。在此之前，先说明基于 BV 算法攻击分组密码的一个一般性攻击策略。设分组密码为E，攻击策略分为两步

1. 基于分组密码E构造一个新的函数F，使得满足两个条件：(I)攻击者能够对F进行量子询问；(II)F具有包含密钥信息的非平凡线性结构。

2. 运行算法 FindStruct 求解F的线性结构，以此恢复密钥。

针对分组密码的电子密码本（ECB）模式给出具体的攻击算法。对任意向量$x \in \mathbb{F}_2^k$，符号$\lceil x \rceil^n$表示x的前n比特构成的向量。若$k < n$，则$\lceil x \rceil^n$为在x末端增加$n-k$个零的向量，即

$$\lceil x \rceil^n = \begin{cases} (x_1, x_2, \cdots, x_n), k \ge n \\ \left(x_1, x_2, \cdots, x_n, \underbrace{0, \ldots 0}_{k-n}\right), k \ge n \end{cases} \tag{5.2.27}$$

设$E_s: \mathbb{F}_2^n \to \mathbb{F}_2^n$为给定密钥$s \in \mathbb{F}_2^k$的分组密码。令$m$为任意明文，定义函数

$$\begin{aligned} F_s^m: F_2^k &\to F_2^n \\ x &\to E_x(m) \oplus E_{s\oplus x}(m) \oplus \lceil x \rceil^n \end{aligned}$$

则对任意的$x \in \mathbb{F}_2^k$，有$F_s^m(x \oplus s) \oplus F_s^m(x) = \lceil s \rceil^n$。因此密钥$s$为$F_s^m$的一个非零线性结构。更具体地，$(s, \lceil s \rceil^n)$为$F_s^m$的线性结构对。因此，可以通过对$F_s^m$运行算法 FindStruct 求解$s$。注意到希望求解的线性结构对满足第一部分和第二部分具有相同的前n比特，可以修改算法 FindStruct 使得其专门求解具有形式$(a, \lceil a \rceil^n)$的线性结构，而非一般形式的线性结构(a,b)。这将大大降低攻击的复杂性。

为了符号简便，接下来假设密钥长度k不小于分组长度n。这一假设不失一般性，当$k < n$时的攻击算法可以类似构造。由 FindStruct 改进的量子相关密钥攻击算法具体如下：

算法 RecoverKey

1. 选择多项式$p(n)$，随机选取明文空间中的明文m。按式(5.4)定义函数F_s^m。设$F_s^m = (F_{s,1}^m, F_{s,2}^m, \cdots, F_{s,n}^m)$。

2. 对$j = 1,2,\cdots,n$，对$F_{s,j}^m$执行 BV 算法$p(n)$次得到$N_{F_{s,j}^m}$的一个子集W_j。集合W_j的大小为$p(n)$。

3. 对$j = 1,2,\cdots,n$，$i_j = 0,1$，解线性方程组$\{x \cdot \omega = i_j | \omega \in W_j\}$得到解集$A_j^{i_j}$。令$\bar{A_j^0} = \{a \in A_j^0 | a_j = 0\}$，$\bar{A_j^1} = \{a \in A_j^1 | a_j = 1\}$，其中$a_j$为$a$的第$j$个比特。则对任意的$a \in \bar{A_j^{i_j}}$，成立$a_j = i_j$。令$A_j = \bar{A_j^0} \cup \bar{A_j^1}$。

4. 计算交集$\bar{A}=A_1\cap A_2\cap\cdots\cap A_n$。令$A=\{(a,\lceil a\rceil^n)|a\in\bar{A}\}$。验证集合$A$中的向量以确定正确的密钥$s$。

算法 RecoverKey 要求敌手能够对F_s^m的量子预言机进行访问，敌手可以通过询问预言机$\mathcal{O}_\mathcal{E}$计算$|x,m,y\rangle\to|x,m,y\oplus E_{s\oplus x}(m)\rangle$，再执行酉算子$U_E$:$|x,m,y\rangle\to|x,m,y\oplus E_x(m)\rangle$和$n$个受控非门$CNOT^{(n)}$:$|x,m,y\rangle\to|x,m,y_1\oplus x_1,\cdots,y_n\oplus x_n\rangle$得到该预言机。实现$F_s^m$的量子线路如图 2

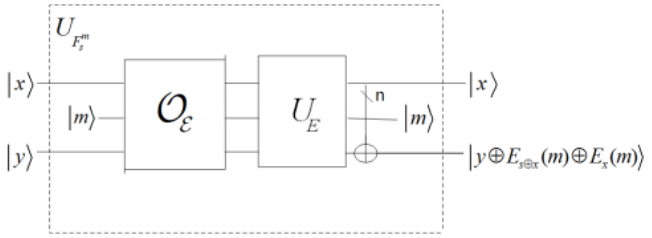


图 5.2-2 F_s^m的量子线路

（3）算法性能分析

最后，给出算法可行性和复杂度的分析。为了论证算法的可行性，首先强调以下两个事实：

• F_s^m的任意具有形式$(a,\lceil a\rceil^n)$的线性结构对都属于算法 **RecoverKey** 第四步计算的集合A。因此，$(s,\lceil s\rceil^n)$也一定属于集合A。

•若存在常数p_0使得$\delta_{F_s^m}(s)\le p_0<1$，则对集合$A$中的任意向量$(a,b)$，$(a,b)\neq(s,\lceil s\rceil^n)$成立的概率小于$p_0^{p(n)}$。

以上两个事实可以由定理 3.1 和 3.2 简单推出。结合这两个事实可知，在$\delta_{F_s^m}(s)\le p_0<1$时，以$p(n)=O(n)$运行算法 **RecoverKey** 得到$s$的概率与1只相差一可忽略的量。

现在分析算法 **RecoverKey** 的复杂性。为此，将算法分为三个部分：

(1)运行 BV 算法$np(n)$次，

(2)求解$2n$个线性方程组，

(3)求集合A_1，$A_2\cdots$，A_n的交集。

对于第一部分，BV 算法运行一次需要执行$2k+1$个 Hadamard 门，一个酉算子U_E和一次对$\mathcal{O}_\mathcal{E}$的量子询问。因此，总共需要$(2k+1+|E|_Q)np(n)$个通用量子门和$np(n)$次量子询问，这部分的计算复杂性为n的多项式。对于第二部分，攻击者需要求解$2n$个线性方程组，每个方程组有k个变量和$p(n)$个方程。由高斯消去法解具有k个变量和$p(n)$个方程的线性方程组需要的计算量为$O(p(n)k^2)$，因此这部分需要$O(2p(n)nk^2)$的经典计算量。对于第三部分，攻击者需要计算交集$A_1\cap A_2\cap\cdots\cap A_n$。令$t=\max_j|A_j|$。由分类法求这$n$个集合的交集需要$O(nt\log t)$的计算量。$t$的值依赖于$F_s^m$和$p(n)$。集合$\bar{A_j^0}$、$\bar{A_j^1}$极大地降低了集合$A_j^0$和$A_j^1$的大小，因此减小了集合$A_j$的大小。由于$A_j$是通过解具有$p(n)$个方程的线性方程组得到的，集合$A_j$的

大小将随$p(n)$的增大而迅速减小。敌手选取的$p(n)$越大，t的值就越小。因此攻击者可以通过选择较大的$p(n)$来减小t的值。对于最一般的情况，t无法保证是多项式的。但在条件$\delta_{F_s^m}(s) \le p_0 < 1$下，$t$是一个较小的数。

综上，算法 RecoverKey 需要$O((2k+1+|E|_Q)np(n))$个量子通用门，$O(2p(n)nk^2 + nt\log t)$的经典计算量和$O(np(n))$次量子询问。若存在常数p_0使得$\delta_{F_s^m}(s) \le p_0 < 1$，则$t$为一个较小的数，此时多项式$p(n)$取$O(n)$即可。

（4）对 Even–Mansour 密码的应用

作为量子相关密钥攻击的具体应用，证明了算法 **RecoverKey** 在量子相关密钥攻击模型下可以有效提取 Even–Mansour 密码的密钥。

Even–Mansour 构造基于公开的随机置换。设$P: \mathbb{F}_2^n \to \mathbb{F}_2^n$为一个公开的随机置换，明文$m$在密钥$s = (s_1, s_2) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$下的密文为

$$E_s(m) = P(m \oplus s_1) \oplus s_2 \tag{5.2.28}$$

令$k = 2n$。则E的密钥空间为$\mathbb{F}_2^k$。对任意明文$m \in \mathbb{F}_2^n$，按(1)式定义函数F_s^m

对任意的$x = (x_1, x_2) \in \mathbb{F}_2^k$，有

$$F_s^m(x) = P(m \oplus x_1) \oplus P(m \oplus x_1 \oplus s_1) \oplus s_2 \oplus x_1 \tag{5.2.29}$$

由于对任意的$x \in \mathbb{F}_2^k$，$F_s^m(x \oplus s) \oplus F_s^m(x) = \lceil s \rceil^n$，$(s, \lceil s \rceil^n)$为$F_s^m$的线性结构对。

在证明算法 **RecoverKey** 可以有效提取 Even–Mansour 密码的密钥前，先分析F_s^m的线性结构集合。设公开置换$P = (P_1, P_2, \cdots, P_n)$，$s = (s_1, s_2)$且$x = (x_1, x_2)$，则对任意的$a = (a_1, a_2) \in \mathbb{F}_2^k$，成立

$$\begin{aligned} & F_s^m(x) \oplus F_s^m(x \oplus a) \\ =& P(m \oplus x_1) \oplus P(m \oplus x_1 \oplus s_1) \oplus P(m \oplus x_1 \oplus a_1) \oplus P(m \oplus x_1 \oplus a_1 \oplus s_1) \oplus a_1 \end{aligned}$$

因此，对任意满足$\lceil a \rceil^n \in \{0, s_1\}$的向量$a$，都成立$F_s^m(x \oplus a) \oplus F_s^m(x) \equiv \lceil a \rceil^n$，即$a$为$F_s^m$的线性结构。事实上，根据(5.8)式，一个向量$a \in \mathbb{F}_2^k$是否是$F_s^m$的线性结构只取决于它的前$n$比特。并且，若求得$s_1$，则可以通过$s_2 = P(m \oplus s_1) \oplus E_s(m)$计算出$s_2$，从而恢复密钥$s = (s_1, s_2)$。因此，当运行算法 **RecoverKey** 求解F_s^m的线性结构时，只需考虑向量的前n比特。定义如下参数：

$$\begin{aligned} \delta_{F_s^m}(s_1) &\triangleq \delta_{F_s^m}(\{b \in \mathbb{F}_2^k | \lceil b \rceil^n = \mathbf{0} \text{ or } \mathbf{s_1}\}) \\ &= \max_j \max_{\substack{a \in \mathbb{F}_2^k \\ \lceil a \rceil^n \notin \{\mathbf{0}, \mathbf{s_1}\}}} \max_{i \in \mathbb{F}_2} \frac{|\{x \in \mathbb{F}_2^k | F_{s,j}^m(x \oplus a) + F_{s,j}^m(x) = i\}|}{2^k} \end{aligned}$$

参数$\delta_{F_s^m}(s_1)$与$\delta_{F_s^m}(s)$相似，只是对a取极大时是在集合$\{b \in \mathbb{F}_2^k | \lceil b \rceil^n = \mathbf{0}, \mathbf{s_1}\}$的补集内，而非在集合$\{\mathbf{0}, \mathbf{s}\}$的补集内。现在考虑存在常数$p_0$使得$\delta_{F_s^m}(s_1) \le p_0 < 1$的情况。假设运行算

法 RecoverKey 于E_s，则由定理 5.2，对任意的$a \in A_j^{i_j}, [a]^n \neq \{\mathbf{0}, \boldsymbol{s_1}\}$的概率是可忽略的。因此，仍旧可以用算法 RecoverKey 求s_1。为此，敌手只需要在求解线性方程组$\{x \cdot \omega = i_j | \omega \in W_j\}$时忽略解向量的后$n$比特，即在算法 RecoverKey 的第三步中，敌手定义集合

$$\begin{aligned} \hat{A}_j^{i_j} &= \{[a]^n | a \in A_j^{i_j}\} \\ \bar{A_j^{i_j}} &= \{a_1 = (a_1^1, a_1^2, \cdots, a_1^n) \in \hat{A}_j^{i_j} | a_1^j = i_j\} \\ A_j &= \bar{A_j^0} \cup \bar{A_j^1}。 \end{aligned} \tag{5.2.30}$$

在第四步，敌手将计算交集$\bar{A} = A_1 \cap A_2 \cap \cdots \cap A_n$，则去掉一个可忽略的概率，集合$\bar{A}$中的非零向量为$s_1$。

基于上述分析，只要存在常数$p_0 < 1$使得$\delta_{F_s^m}(s_1) \leq p_0$，则可以应用算法 **RecoverKey** 于 Even–Mansour 密码E_s以恢复密钥s。因此，只需要证明存在常数p_0使得$\delta_{F_s^m}(s_1) \leq p_0 < 1$。证明了如下定理

定理 5.2.6 当P为均匀随机选取的置换，则除去一个可忽略的几率，有$\delta_{F_s^m}(s_1) \leq \frac{11}{12}$

参考文献

[1]Kaplan, M., Leurent, G., Leverrier, A., & Naya-Plasencia, M. (2016). Quantum Differential and Linear Cryptanalysis. IACR Transactions on Symmetric Cryptology, 2016(1), 71-94

[2]Zhandry M. How to construct quantum random functions[C]//2012 IEEE 53rd Annual Symposium on Foundations of Computer Science. IEEE, 2012: 679-688.

[3] Wang X, Bao W S, Fu X Q. A quantum algorithm for searching a target solution of fixed weight[J]. Chinese Science Bulletin, 2011, 56(6): 484-489.

[4] Wang H, Ma Z, Ma C G. An efficient quantum meet-in-the-middle attack against NTRU-2005[J]. Chinese Science Bulletin, 2013, 58(28-29): 3514-3518.

[5] Pang C Y, Zhou R G, Ding C B, et al. Quantum search algorithm for set operation[J]. Quantum information processing, 2012: 1-12.

[6] Zhou, Q., Lu, S. F., Zhang, Z., et al.: Quantum differential cryptanalysis. Quantum Inf Process. 14(6), 2101-2109 (2015)

[7]Brassard G, Høyer P, Tapp A. Quantum cryptanalysis of hash and claw-free functions[C]//Latin American Symposium on Theoretical Informatics. Springer, Berlin, Heidelberg, 1998: 163-169.

[8] 王婕. 基于 Grover 搜索算法的杂凑函数攻击模型[D]. 西安电子科技大学, 2012.

[9] Hosoyamada A , Sasaki Y . Finding Hash Collisions with Quantum Computers by Using Differential Trails with Smaller Probability than Birthday Bound[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, 2020.

[10]Dong X, Sun S, Shi D, et al. Quantum Collision Attacks on AES-like Hashing with Low Quantum Random Access Memories[J].

[11]Grassl M, Langenberg B, Roetteler M, et al. Applying Grover's algorithm to AES: quantum resource estimates[J]. arXiv preprint arXiv:1512.04965, 2015.

[12]Anand, R., Maitra, A. & Mukhopadhyay, S. Grover on \(\,SIMON\,\). *Quantum Inf Process* **19,** 340 (2020).

[13] Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In: ISIT 2010, pp. 2682-2685 (2010)

[14]Kuwakado, H., Morii, M.: Security on the quantum-type Even-Mansour cipher. In: ISITA 2012, pp. 312–316 (2012)

[15] Li Yang（杨理）, Hong-Wei Li, Investigating the linear structure of Boolean functions based on Simon's period-finding quantum algorithm, arXiv:1306.2008, 2013

[16]Roetteler, Martin, and Rainer Steinwandt. "A note on quantum related-key attacks." Information Processing Letters 115.1 (2015): 40-44.

[17]Santoli, T., Schaffner, C.: Using simon's algorithm to attack symmetric-key cryptographic primitives. In: Quantum Information & Computation. 17, 65-78 (2017)

[18] Kaplan, M., Leurent, G., Leverrier, A., et al.: Breaking symmetric cryptosystems using quantum period finding. In: CRYPTO 2016, Part II, PP. 207-237 (2016)

[19]Alagic G, Russell A. Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts[J]. 2016.

[20]Bonnetain X. Tight Bounds for Simon's Algorithm[J].

[21]Leander G, May A. Grover meets Simon–quantumly attacking the FX-construction[C]//International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2017: 161-178.

[22]Dong, Xiaoyang, Li Zheng, and Wang XiaoYun. "Quantum cryptanalysis on some Generalized Feistel Schemes." SCIENCE CHINA Information Sciences.

[23]Dong, Xiaoyang, Li Zheng, and Wang XiaoYun. "Quantum cryptanalysis on some Generalized Feistel Schemes." SCIENCE CHINA Information Sciences.

[24]Ito G, Hosoyamada A, Matsumoto R, et al. Quantum chosen-ciphertext attacks against Feistel ciphers[C]//Cryptographers' Track at the RSA Conference. Springer, Cham, 2019: 391-411.

[25] Bonnetain X, Hosoyamada A, Naya-Plasencia M, et al. Quantum Attacks without Superposition Queries: the Offline Simon Algorithm[J].

[26]Dong X, Dong B, Wang X. Quantum attacks on some Feistel block ciphers[J]. Designs, Codes and Cryptography, 2020: 1-25.

[27]Floess D, Andersson E, Hillery M. Quantum algorithms for testing and learning Boolean functions[J]. Mathematical Structures in Computer Science, 2013, 23(2): 386-398.

[28]Hong-Wei Li and Li Yang (通讯作者), A quantum algorithm for approximating the influences of Boolean functions and its applications, Quantum Information Processing, 14(6),

1787-1797, 2015

[29]Li H, Yang L. Quantum differential cryptanalysis to the block ciphers[C]//International Conference on Applications and Techniques in Information Security. Springer, Berlin, Heidelberg, 2015: 44-51.

[30]Hillery M, Andersson E. Quantum tests for the linearity and permutation invariance of Boolean functions[J]. Physical Review A, 2011, 84(6):14717-14719.

[31]Hongwei Li and Li Yang (通讯作者). A quantum algorithm to approximate the linear structures of Boolean functions. Math. Struct. in Comp. Science (2018), vol. 28(1), pp. 1–13

[32] HuiqinXie and Li Yang (通讯作者). Using Bernstein-Vazirani Algorithm to Attack Block Ciphers. Designs, Codes and Cryptography

doi:10.1007/s10623-018-0510-5.

[33]HuiqinXieand Li Yang.Quantum impossible differential and truncated differential cryptanalysis. arXiv:1712.06997

[34]Xie H, Yang L. A quantum related-key attack based on the Bernstein–Vazirani algorithm[J]. Quantum Information Processing, 2020, 19(8): 1-20.

[35]HuiqinXie, Li Yang. Quantum Miss-in-the-Middle Attack. arXiv:1812.08499

[36] WINTERNITZ R, HELLMAN M. Chosen-key attacks on a block cipher[J]. Cryptologia, 1987, 11(1):16-20.

[37] FERGUSON N, KELSEY J, LUCKS S. Improved cryptanalysis of rijndael[C]//FSE'00. 2001: 213-230.

[38] BIHAM E, DUNKELMAN O, KELLER N. A related-key rectangle attack on the full kasumi [C]//ASIACRYPT'05. 2005: 443-461.

[39] DUNKELMAN O, KELLER N, SHAMIR A. A practical-time related-key attack on the kasumi cryptosystem used in gsm and 3g telephony[C]//CRYPTO'10. 2010: 393-410.

[40] FLUHRER S, MANTIN I, SHAMIR A. Weaknesses in the key scheduling algorithm of rc4 [C]//SAC'01. 2001: 1-24.

[41] MANTIN I. A practical attack on the fixed rc4 in the wep mode[C]//ASIACRYPT'05. 2005: 395-411.

[42] HOSOYAMADA A, AOKI K. On quantum related-key attacks on iterated even-mansour ciphers[C]//International Workshop on Security. 2017: 3-18.

§5. 3 量子计算环境下的公钥密码安全性分析

5.3.1 量子计算环境下基于整数分解问题的公钥密码体制分析

1978 年，Rivest、Shamir 和 Adleman[1]引入了与分解大整数分解困难问题相关的 RSA 问题，并且依据 RSA 问题的难解性提出了 RSA 密码。

所谓大整数分解问题，就是指给定一个大整数N,找到 2 个不同的质因子 p 和 q 满足$N = pq$.

RSA 密码算法过程如下：

1).选取 2 个不同的大素数：p和q，计算模数$N = pq$及欧拉函数$\phi(N) = (p-1)(q-1)$

2).选取$e \in Z$作为公钥，满足：$1 < e < \phi(N)$且$gcd(e, \phi(N)) = 1$，计算d作为私钥，满足$1 < d < \phi(N)$且$ed = 1 \, mod \, \phi(N)$;

3).RSA 对明文m加密：$c = m^e \, mod \, N$

4).RSA 对密文c解密：$m = c^d \, mod \, N$

RSA 问题是指对于一个未知分解的大整数N，计算$x = y^{1/e}(mod \, N)$。很明显，如果能求出N的分解$N = pq$，自然可以利用$\phi(N) = (p-1)(q-1)$以及$ed = 1 \, mod \, \phi(N)$计算得到私钥d。因此，有效的大整数分解算法能够破解 RSA 问题的困难性，进而也就破解 RSA 密码体制。

在经典计算中，目前不存在多项式时间内能有效求解大整数分解问题的算法。大整数分解问题既未被证明是多项式时间可解的 P 问题，也未被证明是 NP 完备问题。对于该问题当前已知的效率最高的经典算法是数域筛选法[2]，但复杂度也达到了亚指数级别$O\left(exp((\frac{64}{9} + O(1))^{1/3}(log \, N)^{1/3}(loglog \, N)^{2/3})\right)$。

1994 年,美国数学家 Peter Shor 提出的 Shor 算法[2]基于傅里叶变换原理和模幂运算的量子求阶算法，可以在多项式时间内求解大整数分解问题和离散对数问题。1997 年 Shor 又对该量子算法做了进一步详细的解释和阐述。Shor 算法对于依赖于大整数分解和离散对数问题困难问题的公钥密码体制是根本性和直接性的破解。

Shor 算法利用了大整数分解问题与求阶问题的等价性，将大整数分解问题规约为求阶问题。所谓求阶问题，即给定a和N满足：$a < N$且$gcd(a, N) = 1$，求使得$a^r = 1 \, mod \, N$成立的最小正整数r。当然求阶问题也是数学上的计算困难问题，并不存在多项式时间的有效经典算法。Shor 算法中给出了求阶的量子多项式时间算法，并利用多项式时间的量子求阶算法进一步构造大整数分解算法。Shor 算法求解大整数分解问题的复杂度为$O((log \, N)^2(loglog \, N)(logloglog \, N))$，达到多项式级别。

针对理论上的分析结果，科学家们在实际实现上进行孜孜不倦的探索：

1996 年,[3]通过有干扰和损耗的量子电路上用了 27 量子比特成功分解了 15。同时他指出对于分解大数N，需要的量子比特数应是$5L + 7$(其中L取大于等于$log_2 N$的最小正整数)。这项工作的开展给实际操作中实现 Shor 量子算法提供了很好的借鉴。

2001 年[4]，美国 IBM 公司和斯坦福大学合作，利用核磁共振技术演示了 Shor 算法对 15 进行分解的实验，但该实验不能显示其量子属性，也无法扩展到更多的比特，限制了进一步的研究。

2003 年，加拿大蒙特利尔大学使用 2n+3 量子比特的 Shor 分解的电路，还用量子电路的 11 个量子比特分解了 15。该电路的部分灵感来自于 1996 年的英国牛津大学克拉伦登

实验室。

2004 年[5]，美国赫尔辛基理工大学材料物理实验室的 JulaJ.Vartiainen 利用约瑟夫森电荷量子比特实现了 Shor 算法。他把 Shor 算法的量子电路分成了一系列两量子比特和三量子比特的量子门不仅加速了 Shor 算法的实现，而且在此基础上通过数值优化的方法成功完成了对 N=21 分解的物理实现。

2007 年，法国理论物理研究实验室在研究 Shor 算法的缺陷[6](量子比特间残余耦合造成)所产生的影响时，通过编写 Quantware 库并调用该库，用 30 个量子比特实现了 N=943 的分解。

2007 年,中国科学院公布,中国科技大学教授潘建伟和他的同事杨涛等[7]与英国牛津大学的研究人员合作,在国际上首次利用光量子计算机实现了 Shor 量子分解算法,研究发表在当年 1 月的物理评论快报上。并在该量子计算上成功操控了 4 个光子量子比特构造一个简单的线性光网络实现 N=15 的分解。

2013 年[8]，美国卫斯理大学，在一个 128 核的传统计算机集群上构建了一个虚拟的运行 Shor 算法的量子计算机，该虚拟量子计算机被分为在两种模式下实现 Shor 算法。Shor 算法的核心部分包括模幂运算和求周期运算。这两种模式也就是基于 Shor 算法划分的：第一种模式称之为 PF（周期查找）模式即只有周期查找部分没有 Shor 算法的模幂运算部分（这部分用传统模幂运算结果来代替），第二种模式称之为满 Shor 算法模式包括模幂运算和周期查找两部分。在第一种模式下运行的虚拟量子计算机可以最多控制 39 量子比特来实现 N=55793 的分解，在第二种模式下，可以最多实现 N=57 的分解。

2016 年，Thomas 等人提出基于 Kitaev 的 shor 算法的实现，通过有效使用和控制 7 格量子位和四个高速缓存量子位分解整数 15，相比较传统算法，减少了近四分之三的量子比特数。

2019 年，Craig Gidney[9]等人给出了使用量子算法分解 2048 比特 RSA 的时间和空间复杂度分析，他们的工作大大降低了分解整数和计算离散对数的成本。然而，这仍然是很不实际的，因为量子硬件的噪音预计比传统硬件高几个数量级，需要更多的量子比特，这很难实现。

2020 年，Akinori[10]等人指出对于任意整数常量l，最少进行$O(N^{1/2})$次量子询问能产生$l-$碰撞，并提出了用来寻找随机函数多碰撞（即l-碰撞）的量子算法,对于任意$1 \le c_N \le o(N^{1/(2^l-1)})$算法找到随机函数的平均量子询问复杂度为$O(c_N N^{(2^{l-1}-1)/(2^l-1)})$，对于$\tilde{O}(c_N N^{(2^{l-1}-1)/(2^l-1)})$量子位运行的时间为$\tilde{O}(c_N N^{(2^{l-1}-1)/(2^l-1)})$。

5.3.2 量子计算环境下基于离散对数问题的公钥密码体制分析

所谓离散对数问题，即是给定一个很大的素数 P 及有限乘法群Z_P^*上的一个生成元g和任意元素b，求x满足：$g^x = b \bmod P$或$x = log_g b \bmod P$。该问题在经典计算环境下是计算困难的，还未找到有效求解离散对数的多项式时间算法。目前已知的最好的经典算法复杂度为$e^{O\left(log\, p^{\frac{1}{3}}\right)(log log\, p)^{\frac{2}{3}}}$，达到亚指数级别。

基于离散对数问题的公钥密码方案最简单的当属 Diffie-Hellman 密钥交换协议[11]，针

对的是以下困难的局面：Alice 和 Bob 想共有一个密钥，用于对称加密。但是他们之间的通信渠道是不安全的。所有经过此渠道的信息均会被敌对方：Eve 看到。那他们要如何交换信息，才能不让 Eve 知道这个密钥呢？

Diffie-Hellman 密钥交换协议过程如下：

Alice 选取a，发送$g^a(mod\,p)$给 Bob;

Bob 选取b，发送$g^b(mod\,p)$给 Alice;

Alice 计算$K=(g^b)^a=g^{ab}(mod\,p)$;

Bob 计算$K=(g^a)^b=g^{ab}(mod\,p)$;

这样,Alice 和 Bob 便拥有了相同的密钥 K。基于离散对数问题的困难性，Eve 仅通过信道中的$g^a(mod\,p)$和$g^b(mod\,p)$计算 K 是困难的。然而如果能解离散对数问题，那么该协议就毫无安全性可言。

Shor 算法求解离散对数的过程使用 3 个量子寄存器，每个量子寄存器都有m个量子比特，满足：$p\le Q=2^m<2p$。算法具体步骤前文已经详细介绍，在此不再赘述。

然而 Shor 算法对椭圆曲线密码进行攻击相对于 Shor 算法攻击 RSA 来说很少。原因主要有两方面：

Shor 算法是建立在有限域的乘法群上来求解问题的，而椭圆曲线加密算法的椭圆曲线密码是基于有限域下的加法群。虽然有限域下乘法群和加法群都可以归纳为阿贝尔隐含子群，但它们之间还是有很大区别的。

椭圆曲线加密算法相对 RSA 算法具有更难理解、运算更复杂的特征。这就使得研究 Shor 算法攻击椭圆曲线加密算法变得更加困难。

2003 年加拿大的滑铁卢大学做了用 Shor 算法求解椭圆曲线离散对数问题的研究。滑铁卢大学最开始是从数学和 Shor 算法两个方面进行着手分析：首先，分析有限域下各种椭圆曲线的特性并选择了一条特殊的椭圆曲线进行分析；然后，从实现 Shor 算法的模幂运算与量子傅里叶变换的两个模块本身出发，进行对 Shor 算法进行优化。在此基础上，逐步分析 Shor 算法求解整数分解、离散对数、椭圆曲线离散对数问题，理论上做了一个很完整的 Shor 算法求解椭圆曲线离散对数问题的研究，并指出对于 Shor 算法攻击 n 位比特椭圆曲线密码，需要的量子比特数为 6nQubits。但是，仅限于理论分析没有给出实验模拟的过程。

2017 年美国微软研究院对使用 Shor 算法求阶椭圆曲线的离散对数问题所需要的量子资源进行了估算，得出在 n 比特素数域上定义的椭圆曲线上的离散对数可以在量子计算机上用至多$448n^3\log_2 n+4090n^3$ Toffoli 门的量子电路计算，其量子比特数最多为$9n+2\lceil\log_2 n\rceil+10$。虽然提出通过量子电路来实现 shor 算法解决 ECDLP，分析了电路所需资源但没有通过实验证明。

2018 年，上海大学陈宇航等人提出可以利用小量子比特数来破解椭圆曲线加密的 Shor 量子攻击方法，对当前安全曲线构成威胁，其通用性更强。

根据上面简单分析，可以看出 Shor 算法可以推广至一般有限阿贝尔群的隐含子群问题，

所以通过微小的修改，Shor 算法可以应用于与椭圆曲线相关的群，从而打破椭圆曲线 Diffie-Hellman 密钥交换和椭圆曲线数字签名算法。受到这一成果的鼓舞，许多研究人员试图在各种非阿贝尔群体上设计“隐藏子群问题”的量子算法[12]，例如对称群，二面体群和有限域上的一般线性群。这些问题与许多其他众所周知的问题有关，如图同构问题，基于格的最短向量问题，以及多变量密码系统安全性的某些问题。迄今为止，量子算法在解决这些困难问题上仍没有大的突破，但仍有一些有趣的结果，例如 Kuperberg 算法，它在次指数时间内解决了二面体隐含子群问题[13]。

参考文献

[1] Rivest R L, Shamir A, Adleman L M. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems[J]. Communications of the ACM, 1978, 21(2):120-126.

[2] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. Foundations of Computer Science, 1994 Proceedings. Symposium on. IEEE, 2002: 124-134.

[3] Miquel, César, Paz J P , Perazzo R . Factoring in a Dissipative Quantum Computer[J]. Physical Review A, 1996, 54(4):2605-2613.

[4]Vandersypen L M K, Steffen M, Breyta G, et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance[J]. Nature, 2001, 414(6866): 883-887.

[5]Vartiainen J J, Niskanen A O, Nakahara M, et al. Implementing Shor’s algorithm on Josephson charge qubits[J]. Physical Review A, 2004, 70(1): 012319.

[6]García-Mata I, Frahm K M, Shepelyansky D L. Effects of imperfections for Shor’s factorization algorithm[J]. Physical Review A, 2007, 75(5): 052311.

[7] Lu C Y , Browne D E , Yang T , et al. Demonstration of a Compiled Version of Shor’s Quantum Factoring Algorithm Using Photonic Qubits[J]. Physical Review Letters, 2007, 99(25):250504.

[8] Nam Y S, Blümel R. Streamlining Shor's algorithm for potential hardware savings[J]. Physical Review A, 2013, 87(6): 060304.

[9]Gidney C, Ekerå M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits[J]. arXiv preprint arXiv:1905.09749, 2019.

[10]Hosoyamada A, Sasaki Y, Tani S, et al. Quantum algorithm for the multicollision problem[J]. Theoretical Computer Science, 2020, 842: 100-117.

[11] Merkle, Ralph C . Secure communications over insecure channels[J]. Communications of the ACM, 1978, 21(4):294-299.

[12]BanielBoneh and Richard J. Lipton. Quantum cryptanalysis of hiddlen linear functions (extended abstract). In Don Coppersmith, editor, Lecture notes in computer science-Advances in Cryptology-CRTPTO’95, pages 424-437, 1995

[13]]Kuperberg G. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem[J]. SIAM Journal on Computing, 2005, 35(1): 170-188.

第 6 章量子计算机物理实现

量子计算是量子物理和计算科学结合的产物，被认为是在经典计算能力达到极限后，未来计算能力发展的新方向。量子计算的一个重要应用领域即为信息安全，在量子计算机上，基于量子叠加和纠缠而获得的天然并行处理能力，可以实现诸如 Shor 的大整数因子分解算法、求解离散对数算法[1,2]，以及 Grover 量子搜索算法[3,4]等，从而对经典密码协议安全性产生影响。例如，人们一般认为，Shor 的大整数因子分解算法、离散对数算法分别会对目前广泛使用的 RSA、ElGamal 公钥密码算法安全性产生威胁， Grover 量子搜索算法会对 AES 等算法安全性造成影响（导致密钥量需要加倍），等等。目前已经提出了不少量子计算机的实现方案，主要有核磁共振方案、光学方案、量子点方案、腔量子电动力学方案、超导约瑟夫森结方案、冷离子阱方案等等。在这些方案中，冷离子阱方案是最有希望的方案之一。

本讲义主要从原理及装置、初态制备和终态测量、量子门的实现、最初实验、最新进展、场量子化对离子阱量子计算的影响 5 个方面，对离子阱量子计算方案作一介绍。

§6.1 概述

量子计算是以量子力学系统为计算硬件，以量子态编码信息，并根据具体问题算法要求、按照量子力学规律执行计算任务（变换、演化编码量子态），根据量子测量理论提取计算结果的计算机。由于量子态具有相干叠加性质，特别是具有经典物理中没有的量子纠缠特性，使得量子计算具有天然的大规模并行计算能力。目前已经知道，量子计算机在解决大整数因子分解、随机数据库搜索等问题上，相对经典计算机具有加速作用。

量子计算主要通过量子门来实现，单量子比特门和受控非（CNOT）门构成量子计算的一组通用量子门[7]。单量子比特的量子门 U 可由 2×2 矩阵给出，由门操作前后量子态都要满足归一化的要求，可以得到 $U^{+}U=I$，其中 U^{+}是 U 的共轭转置，即取 U 的转置和复共轭所得，I 是 2×2 的单位阵。受控非(controlled-NOT,CNOT)门有两个输入量子比特，分别称为控制量子比特和目标量子比特。此门的作用是：若控制量子比特为 0，则目标量子比特不变；若控制量子比特为 1，则目标量子比特翻转。用方程表示有

$$|00\rangle \to |00\rangle, |01\rangle \to |01\rangle, |10\rangle \to |11\rangle, |11\rangle \to |10\rangle.$$

受控非门还有一种矩阵表示方法

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \tag{6.1.1}$$

其第一列表示对|00>的变换，第二、三、四列分别表示对|01>、|10>、|11>的变换。

量子计算发展至今，主要有离子阱、超导、线性光学、核磁共振等物理实现方案。其中，离子阱方案由 Cirac 和 Zoller 于 1995 年提出**错误！未找到引用源。**量子比特是阱中离子的电子状态（如基态和激发态）；同时，轴向量子化振动模（声子）在离子间传递相互作用，为“总线（bus）”量子比特。逻辑门通过相干场（如激光）驱动来实现。超导约瑟夫森结方

案由 Nakamura、Pashkin、Tsai 于 1999 年首次实现[9]。量子比特是电荷相位等。单量子比特门通过约瑟夫森结等来实现。量子比特间耦合通过电容或电感来实现，从而实现多量子比特门。线性光学方案由 Knill，Laflamme，Miburn 于 2001 年提出[10]。量子比特为单光子极化方向。单量子比特门通过极化旋转来实现。量子比特间通过测量实现耦合，从而实现多量子比特门。核磁共振方案由 Gershenfeld 和 Chuang 于 1997 年提出[11]。量子比特是分子中原子核自旋。逻辑门通过相应射频脉冲实现。

近年来，国际上许多著名研究机构、企业都投入巨大人力、物力来研制量子计算机，并取得了稳步进展。2016 年，马里兰大学与美国国家标准与技术研究院发布 5 个量子比特的可编程离子阱量子计算机。2017 年，中科院宣布中国建造了世界上第一台超越早期经典计算机的 10 量子比特光量子计算机，清华大学上线了基于核磁共振的量子计算云平台。2018 年，谷歌宣布推出名为“Bristlecone”的 72 超导量子比特芯片，创造了新纪录。2019 年，我国科研团队开发出具有 20 个超导量子比特的量子芯片，并成功操控其实现全局纠缠，刷新了固态量子器件中生成纠缠态的量子比特数目的世界纪录。

目前，离子阱系统和超导系统实验技术发展水平最为领先，是最有可能率先实现的方案。2018 年底美国颁布《国家量子计划法》，正式启动国家量子计划，该计划在量子计算机方面主要面向的就是离子阱和超导电路两个方案。

§6.2 离子阱量子计算机原理及装置

冷离子阱方案的思想是 J. I. Cirac 和 P. Zoller 在 1995 年首先提出的[8]，作者讨论了离子阱方案的特点、原理、装置、量子门的实现以及终态测量等问题，奠定了离子阱量子信息处理的理论基础。在该方案中，量子计算机可以用冷离子完成，这些离子被限制在线性阱中，而且和激光束作用，包含任意两个、三个或者更多离子的量子门可以通过把离子用集体量子化运动耦合起来实现。在这个系统中，退相干可以忽略，而且测量可以以高效率完成。

6.2.1 原理

离子阱量子计算机的基本元素（即量子比特）是离子自身。第 n 个量子比特的两个状态用相应离子的两个内部能级来表征。例如，基态和激发态。在这个系统中，每个量子比特的独立操作是通过用不同激光束照射不同离子来实现的。量子 CNOT 门可通过用激光激发集体的量子化运动来实现（这在后文中会详细讲述）。离子运动的耦合由库仑斥力提供，它在离子间距为几个光学波长时，比其它的相互作用都强得多。

离子阱的退相干源于内部原子能级的自发辐射和离子运动损耗，存储的离子在极高精度光谱和时间频率标准下的实例表明，这个退相干时间可以相当长，比实现很多操作需要的时间长得多。自发辐射可用亚稳跃迁（metastable transitions）抑制。与背景原子的碰撞可可在足够低的压强下在相当长时间内避免，其他影响运动电荷的耦合都可以足够小。此外，量子寄存器的最终读出可以用量子跃迁技术（quantum jumps technique）以高效率完成。

6.2.2 实验装置

实验装置即是对上述原理的实际实现。首先给出离子阱量子计算机的框图（见图 6.2-1），四个被束缚的离子，处在四根柱形电极产生的势场的中心。该设备通常置于高度真空中，离子是从附近的炉内载入的。从真空室的窗口入射的调制后的激光，在原子状态上完成运算并用于读出原子状态。

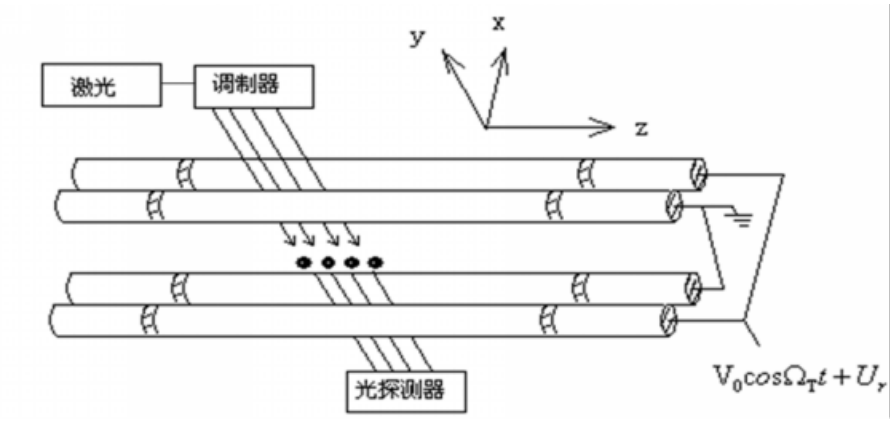
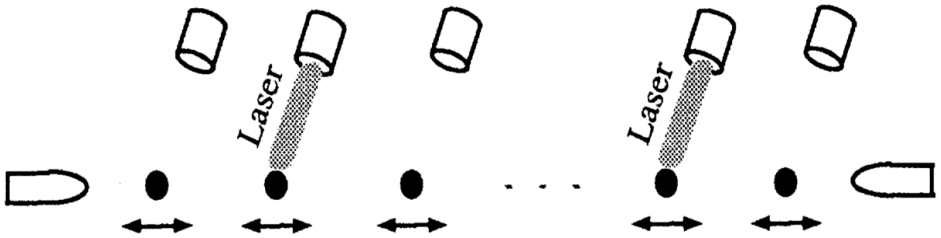


图 6.2-1 离子阱量子计算机框图

下面给出离子与激光束作用的示意图（图 6.2-2）。可看出，N 个离子被限制在线性阱中，分别和不同驻波激光束作用。X，Y 和 Z 方向的运动限制可以用（各向异性的）谐振势描述$v_x << v_y, v_z$。离子事先用激光在三个方向上冷却，所以它们在平衡位置附近作非常小的振动。在这种情形下，离子运动用简正模式来描述。此外，假设边带冷却已经使得所有简



正模式在它们相应的基态上。为使这成为可能，需要假设对所有简正模式 Lamb-Dicke 极限（LDL）都适用，即所有简正模式的频率比用于冷却的光子反冲频率大。简正模式中，频率最小（能量最低）的模式是在 X 方向的质心（CM）模式，它的频率为v_x。

图 6.2-2 离子与激光束作用示意图

6.2.3 量子比特

具体来说，离子阱中的量子比特分为两类，一类是 N 个离子，它们提供 N 个量子比特，$|0\rangle$和$|1\rangle$为离子中电子的内部能态，通常是由原子内的超精细作用或外加磁场的塞曼作用从基态分离出来的低位能级。下面给出一个碱土金属的典型能级图（见图 6.2-3），选择作为

量子比特的能级用粗线标出（$|g\rangle$和$|e_0\rangle$），$|e_1\rangle$是辅助能级。根据 A. Steane 的观点[9]，作为量子比特的离子需要满足以下条件：需为稳定的同位素，有长的退相干时间，基态有超精细结构，产生用于冷却和计算的激光的难度较低，有大的反冲能量（光子入射所引起）。

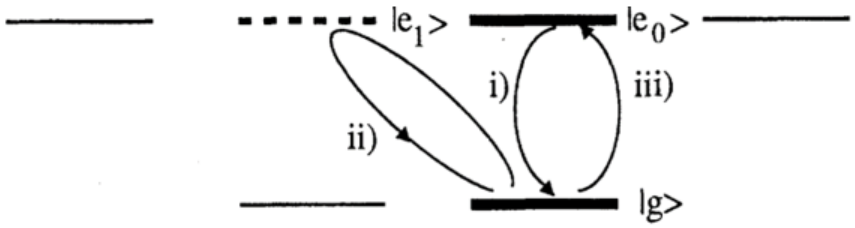


图 6.2-3 原子能级图

第二类量子比特是整个离子链的振动声子，它们作为第（N+1）个量子比特，一般选用质心模式的基态和第一激发态。它为整个离子链所共享，在各离子间（不一定相邻）传递相互作用，从而实现任意两量子位间的控制转动操作，又被称为总线比特（bus bit）。

§6.3 初态制备与终态测量

6.3.1 初态制备

为使离子的一维谐振子近似有效，需要将离子冷却到质心模式的基态。如何才能做到这点？首先，如果调节激光，使得它只被迎面而来的原子吸收，那么原子就因光子的反向冲击而变慢，这种方法称为 Doppler 冷却，可把原子冷却到极限$k)BT \approx \eta\Gamma/2$，其中$\Gamma$是用于冷却的跃迁的辐射宽度。要超过这个极限进一步冷却，常用另一种称为边带冷却的方法，使能达到$k_BT << \eta\omega_x$的极限。

边带冷却的原理是这样的（见图 6.3-1）： g/e 是电子能级，$0/1/\cdots$是表示离子运动状态的声子能级。激光被调整到具有比电子跃迁少一个声子的能量。比如，状态跃迁到状态，然后原子自发地衰变为较低能量的 g 状态（波浪线），随机地（以基本相同的概率）进入$|g,1\rangle$，$|g,2\rangle$或$|g,3\rangle$状态，整个过程不影响$|g,0\rangle$态，并且原子最终会停留在这个状态。简单来说就是向最低的振动量子数进行光学抽运。

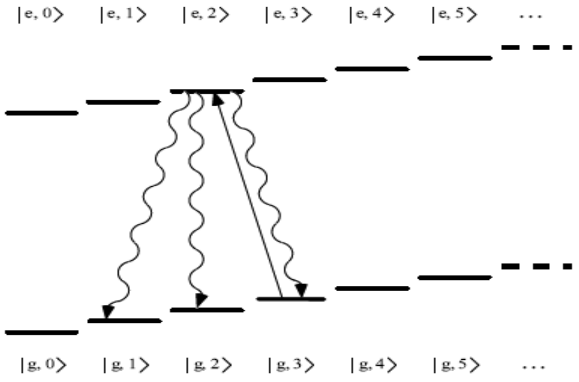


图 6.3-1 边带冷却示意图

6.3.2 终态测量

离子所表示的量子比特可以这样测量（见图 6.3-2）：若体系处于态，体系将吸收光子并从基态 a 跃迁到激发态 b，然后再从 b 态跃迁到基态并发射光子，这一荧光将被检测器检测；若体系处于|0⟩与|1⟩正交的态，由于体系不能吸收所照射的光，检测器探测不到任何信息；若处于叠加态，需要将态矢量进行旋转以后再观测就能确定波函数。如果要测量声子所表示的量子比特，只需要将离子和声子的信息交换，然后测量离子的状态即可。

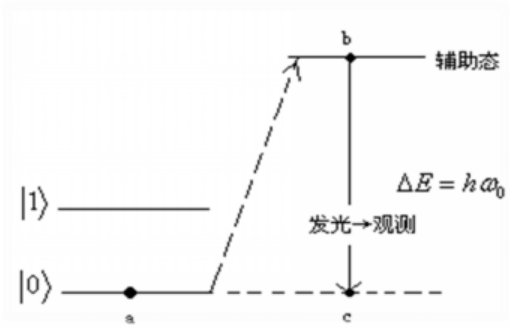


图 6.3-2 终态测量示意图

§6.4 量子门的实现

任何一个量子计算机的实现方案中，如何实现一组通用量子门都是其核心内容。冷离子阱方案也不例外。在离子阱量子门的实现中，激光有着决定性的作用，当一束激光束作用在一个离子上时，它导致离子内部基态与激发态之间的跃迁，而且可以改变集体简正模式的状态。

下面以原始文章[1]中的方案为例，介绍受控非（CNOT）门及单量子比特门的实现，而这两个门构成量子计算的一组通用量子门。具体地，令$\hat{H}_0$为系统没有激光场时的哈密顿量。考虑第 n 个离子上的激光被打开，显然，它不会影响其他离子的内部状态。调整激光频率使得失谐$\delta_n = -v_x$，v_x如前所述，是 CM 模式的频率。同时，令激光驻波波节和离子平衡位置重合。相互作用表象下这种情形的哈密顿量是（$\eta = 1$）

$$\hat{H}_{n,q} = \frac{\eta}{\sqrt{N}}\frac{\Omega}{2}\left[|e_q\rangle_n\langle g|ae^{-i\Phi} + |g\rangle_n\langle e_q|a^{\dagger}e^{i\Phi}\right] \tag{6.4.1}$$

这里a^{+}和a分别是声子的产生和湮灭算符，Ω是拉比频率,Φ是激光相位，$\eta = [\eta k_\theta/(2Mv_x)]^{1/2}$是 LDL 参数（$k_{theta} = k\cos(\eta)$，k 是激光波矢，$\theta$是激光传播方向和 X 轴夹角）。下标 q=0,1 代表依赖于激光极化的跃迁。方程（6.4.2）可以看作是线性阱中单个离子哈密顿量在多个离子时的推广。

如果激光束照射一定时间$t = k\pi/(\Omega\eta/\sqrt{N})$ (即用一个$k\pi$脉冲)，系统的演化用以下酉算符描述（通过$\hat{U}_n^{k,q} = exp(-i\,\hat{H}_{n,q}\,t)$计算得出）

$$\hat{H}_n^{k,q}(\Phi) = exp[-ik\frac{\pi}{2}(\quad |e_q\rangle_n\langle g|ae^{-i\Phi+H.c.})] \tag{6.4.2}$$

这里 H.c.代表厄米共轭。容易证明此变换不改变$|g\rangle_n|0\rangle$，然而

$$\begin{aligned}|g\rangle_n|1\rangle &\longrightarrow \cos(k\pi/2)|g\rangle_n|1\rangle - ie^{i\phi}\sin(k\pi/2)|e_q\rangle_n|0\rangle,\\ |e\rangle_n|0\rangle &\longrightarrow \cos(k\pi/2)|e_q\rangle_n|0\rangle - ie^{-i\phi}\sin(k\pi/2)|g\rangle_n|1\rangle\end{aligned} \tag{6.4.3}$$

这里$|0\rangle$（$|1\rangle$）代表 CM 模式没有（有一个）声子的状态。下面展示如何完成一个双量子比特门。考虑以下三个步骤：(1)极化 q=0 且$\Phi=0$的脉冲激发第 m 个离子，相应演化可用$\hat{U}_m^{1,0}=\hat{U}_m^{1,0}(0)$描述。(2) 打开第 n 个离子对应的激光，调整激光使其是$q=1,\Phi=0$的2π脉冲。相应的演化算符$\hat{U}_n^{2,1}$改变$|g\rangle_n|1\rangle$的符号，但不改变其他态。(3)与(1)相同。因此整个过程的酉演化是$\hat{U}_{m,n}=\hat{U}_m^{1,0}\,\hat{U}_n^{2,1}\,\hat{U}_m^{1,0}$，可用下面形式表示:此相互作用的结果是只当两个离子初始时都是激发态时才改变态的符号。注意到 CM 模式的状态在整个过程之后恢复到$|0\rangle$。上面方程和 CNOT 门等同。为了说明这点，令$|\pm\rangle=(|g\rangle\pm|e_0\rangle)/\sqrt{2}$，则有$|g\rangle_m|\pm\rangle_n\rightarrow|g\rangle_m|\pm\rangle_n$，$|e_0\rangle_m|\pm\rangle_n\rightarrow|e_0\rangle_m|\mu\rangle_n$。用一个合适的对第 n 个离子的单量子比特旋转，这个

$$\begin{array}{ccccccccc}
 & & \hat{U}_m^{1,0} & & & \hat{U}_n^{2,1} & & \hat{U}_m^{1,0} & \\
|g\rangle_m|g\rangle_n|0\rangle & \longrightarrow & |g\rangle_m|g\rangle_n|0\rangle & \longrightarrow & |g\rangle_m|g\rangle_n|0\rangle & \longrightarrow & |g\rangle_m|g\rangle_n|0\rangle, \\
|g\rangle_m|e_0\rangle_n|0\rangle & \longrightarrow & |g\rangle_m|e_0\rangle_n|0\rangle & \longrightarrow & |g\rangle_m|e_0\rangle_n|0\rangle & \longrightarrow & |g\rangle_m|e_0\rangle_n|0\rangle, \\
|e_0\rangle_m|g\rangle_n|0\rangle & \longrightarrow & -i|g\rangle_m|g\rangle_n|1\rangle & \longrightarrow & i|g\rangle_m|g\rangle_n|1\rangle & \longrightarrow & |e_0\rangle_m|g\rangle_n|0\rangle, \\
|e_0\rangle_m|e_0\rangle_n|0\rangle & \longrightarrow & -i|g\rangle_m|e_0\rangle_n|1\rangle & \longrightarrow & -i|g\rangle_m|e_0\rangle_n|1\rangle & \longrightarrow & -|e_0\rangle_m|e_0\rangle_n|0\rangle
\end{array}$$

过程就成为 CNOT。

这个单个离子上的旋转可以用和内部跃迁谐振的激光（$\delta_n=0$）完成，使激光极化$\Phi=0$，且驻波波腹和离子平衡位置重合。此种情形下哈密顿量为

$$\hat{H}_n\,(\Omega/2[|e_0\rangle_n\langle g|e^{-i\Phi}+|g\rangle_n\langle e_0|e^{i\Phi}]) \tag{6.4.4}$$

对于相互作用时间$t=k\pi/\Omega$(即用一个$k\pi$脉冲)，这个过程可用以下酉演化算符描述

$$\hat{V}_n^k(\Phi)=exp[-ik\frac{\pi}{2}(|e_0\rangle_n\langle g|e^{-i\Phi}+H.c.)] \tag{6.4.5}$$

因此，

$$\begin{aligned}|g\rangle_n &\rightarrow \cos(k\pi/2)|g\rangle_n - ie^{i\Phi}\sin(k\pi/2)|e_0\rangle_n,\\ |e_0\rangle_n &\rightarrow \cos(k\pi/2)|e_0\rangle_n - ie^{i\Phi}\sin(k\pi/2)|g\rangle_n,\end{aligned} \tag{6.4.6}$$

所以对于状态$|\epsilon_m\rangle|\epsilon_n\rangle$（$\epsilon_{m,n}=g,e_0$），完整的 CNOT 门由$\hat{C}_{mn}-\hat{V}_n^{1/2}(\frac{\pi}{2})\,\hat{U}_{m,n}\,\hat{V}_n^{1/2}(-\frac{\pi}{2})$给出。

到这里，虽然看起来差不多是实现了 CNOT 门，但为了验证，分别对$|g\rangle_m|g\rangle_n|0\rangle$、$|g\rangle_m|e_0\rangle_n|0\rangle$、$|e_0\rangle_m|g\rangle_n|0\rangle$、$|e_0\rangle_m|e_0\rangle_n|0\rangle$态，按$\hat{C}_{m,n}=\hat{V}_n^{1/2}(\frac{\pi}{2})\,\hat{U}_{m,n}\,\hat{V}_n^{1/2}(-\frac{\pi}{2})$给出的脉冲顺序进行作用，看其结果是否和 CNOT 门结果一致。这里以$\left|e_0\right\rangle_m\left|g\right\rangle_n\left|0\right\rangle$为例进行计算：

$$\left|e_0\right\rangle_m\left|g\right\rangle_n\left|0\right\rangle\xrightarrow{\hat{V}_n^{1/2}(-\frac{\pi}{2})}\left|e_0\right\rangle_m\frac{\sqrt{2}}{2}(\left|g\right\rangle_n-\left|e_0\right\rangle_n)\left|0\right\rangle\xrightarrow{\hat{U}_{m,n}}\frac{\sqrt{2}}{2}\left|e_0\right\rangle_m(\left|g\right\rangle_n+\left|e_0\right\rangle_n)\left|0\right\rangle$$

$$\xrightarrow{\hat{V}_n^{1/2}(\frac{\pi}{2})} \frac{1}{2}|e_0\rangle_m[(|g\rangle_n+|e_0\rangle_n)+(|e_0\rangle_n-|g\rangle_n)]|0\rangle=|e_0\rangle_m|e_0\rangle_n|0\rangle \quad (6.4.7)$$

而$|e_0\rangle_m|g\rangle_n|0\rangle \xrightarrow{CNOT} |e_0\rangle_m|e_0\rangle_n|0\rangle$，因此，确实对$|e_0\rangle_m|g\rangle_n|0\rangle$实现了 CNOT，其他三个态的验证类似。

通过上面具体描述可以看出，用五个特定的脉冲，可以实现 CNOT 门；而且单量子比特旋转操作也可以容易实现。因此利用量子信息理论中的可分解定理，理论上任何门操作都可以实现。

§6.5 冷离子阱方案的首次实验实现

关于冷离子阱方案，最早的实验实现是由 C.Monroe 等人完成的[13]，他们在 J.I.Cirac 和 P.Zoller 提出离子阱量子计算思想的同年就实现了其方案的重要内容。作者指出，他们展示了两比特受控非量子逻辑门的操作。两个量子比特存储在阱中单个离子的内部和外部自由度中，离子起初用激光冷却到零点能。他们还确定了操作的退相干影响。有希望把此系统扩展到更多的量子比特。

6.5.1 量子比特的选择

在他们的实验方案中，目标比特$|S\rangle$由 $^9Be^+$的两个 $^2S_{1/2}$ 超精细基态张成（即$|F=2,m_F=2\rangle$和$|F=1,m_F=1\rangle$态，简写为$|\uparrow\rangle$和$|\downarrow\rangle$），它们的频率差是$\omega_0/2\pi \approx 1.250GHz$。控制比特$|n\rangle$由离子量子化谐振子态的前两个能级张成（$|0\rangle$和$|1\rangle$），频率差为离子做简谐振动的频率$\omega_x/2\pi \approx 11MHz$。作者给出了具体能级图（见图 6.5-19）四个基态本征态（$|n\rangle|S\rangle = |0rangle|\downarrow\rangle, |0rangle|\downarrow\rangle, |0\rangle|\uparrow\rangle, |1\rangle|\downarrow\rangle, |1\rangle|\uparrow\rangle$）之间的操作是通过一对失谐激光实现的，它在计算基态之间引起受激拉曼跃迁。两束的频率差δ不同，引起的跃迁就不同。$\delta \approx \omega_0$时，为载波跃迁（carrier transition），即引起离子本身能级的跃迁而保持$|n\rangle$；类似地，$\delta \approx \omega_x - \omega_x$时，为红边带跃迁，引起$|1\rangle|\downarrow\rangle$和$|0\rangle|\uparrow\rangle$之间的跃迁；$\delta \approx \omega_0 + \omega_x$时，为蓝边带跃迁，引起$|0\rangle|\downarrow\rangle$和$|1\rangle|\uparrow\rangle$之间的跃迁。可以注意到当$\delta$调整到任一个边带的时候，受激拉曼跃迁把$|S\rangle$和$|n\rangle$纠缠起来，这是量子 CNOT 门的关键环节。

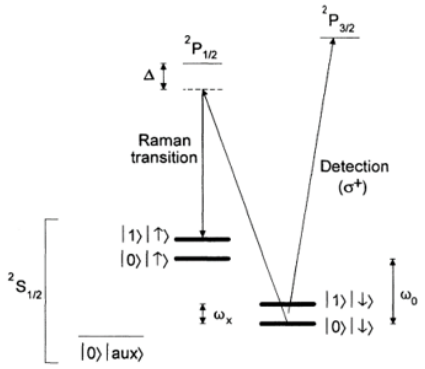


图 6.5-19Be+能级图

6.5.2 CNOT 门实现

他们通过以下三步完成 CNOT 操作：(1)载波跃迁，用$\pi/2$脉冲，作用可用文献[1] 中的$V^{1/2}(\pi/2)$描述。(2)$|\uparrow\rangle$和辅助能级$|aux\rangle$间的蓝边带跃迁，用2π脉冲。(3) 载波跃迁，用$\pi/2$脉冲，用文献[1] 中的$V^{1/2}(-\pi/2)$描述。第(1)、(3)步中的$\pi/2$脉冲使得自旋$|S\rangle$分别经历一个完整拉比振荡的+1/4 和-1/4，$|n\rangle$不变。步骤(2)中的辅助跃迁只通过引入一个完整的拉比振荡$|1\rangle|\uparrow\rangle \rightarrow |0\rangle|aux\rangle \rightarrow -|1\rangle|\uparrow\rangle$，来改变$|1\rangle|\uparrow\rangle$态的符号。辅助能级$|aux\rangle$是 $^2S_{1/2}|F=2, m_F=0\rangle$基态，是从$|\downarrow\rangle$态塞曼分裂而来。在步骤(2)中，量子寄存器中任意$|n\rangle=|0\rangle$态不受影响，两个$\pi/2$脉冲的作用抵消。而$|1\rangle|\uparrow\rangle$态改变符号，两个$\pi/2$脉冲有效地使目标比特翻转。

为便于理解，将以上关于实现 CNOT 门的过程逐步写出：

$$|0\rangle|\downarrow\rangle \xrightarrow{①} |0\rangle\frac{\sqrt{2}}{2}(|\downarrow\rangle+|\uparrow\rangle) \xrightarrow{②} |0\rangle\frac{\sqrt{2}}{2}(|\downarrow\rangle+|\uparrow\rangle) \xrightarrow{③} |0\rangle\frac{1}{2}[(|\downarrow\rangle-|\uparrow\rangle)+(|\downarrow\rangle+|\uparrow\rangle)]=|0\rangle|\downarrow\rangle$$

$$|0\rangle|\uparrow\rangle \xrightarrow{①} |0\rangle\frac{\sqrt{2}}{2}(|\uparrow\rangle-|\downarrow\rangle) \xrightarrow{②} |0\rangle\frac{\sqrt{2}}{2}(|\uparrow\rangle-|\downarrow\rangle) \xrightarrow{③} |0\rangle\frac{1}{2}[(|\downarrow\rangle+|\uparrow\rangle)-(|\downarrow\rangle-|\uparrow\rangle)]=|0\rangle|\uparrow\rangle$$

$$|1\rangle|\downarrow\rangle \xrightarrow{①} |1\rangle\frac{\sqrt{2}}{2}(|\downarrow\rangle+|\uparrow\rangle) \xrightarrow{②} |1\rangle\frac{\sqrt{2}}{2}(|\downarrow\rangle-|\uparrow\rangle) \xrightarrow{③} |1\rangle\frac{1}{2}[(|\downarrow\rangle-|\uparrow\rangle)-(|\downarrow\rangle+|\uparrow\rangle)]=|1\rangle|\downarrow\rangle$$

$$|1\rangle|\uparrow\rangle \xrightarrow{①} |1\rangle\frac{\sqrt{2}}{2}(|\uparrow\rangle-|\downarrow\rangle) \xrightarrow{②} |1\rangle\frac{\sqrt{2}}{2}(-|\uparrow\rangle-|\downarrow\rangle) \xrightarrow{③} |1\rangle\frac{1}{2}[-(|\downarrow\rangle+|\uparrow\rangle)-(|\downarrow\rangle-|\uparrow\rangle)]=|1\rangle|\uparrow\rangle$$

§6.6 最近进展

6.6.1 大规模量子计算与芯片化

一般认为，离子阱量子计算的主要限制和瓶颈在于如何实现可扩展与大规模化，因此近年来，科学家们在这方面做了许多努力，取得了一定进展。

单个量子比特寻址对于可扩展量子计算是一重要先决条件。一般来说，用单个或数个量子比特实现量子门会影响所有其他量子比特。这种整个寄存器保真度下降可能会阻碍量子纠错协议实现，进而阻碍大规模化。Warring 等人[14]实现了微表面电极阱中的精细寻址，描述了 4 种可能在量子信息实验中使用的方法。作者实现了相距 4.36565μm的 2 个 Mg 离子的分别控制，错误率为10^{-3}量级。Piltz 等人[15] 演示在 8 量子比特寄存器中定位单个量子比特，测量对于其他量子比特引入的错误率，测量到的“串音”（错误率）为10^{-5}数量级，低于公认的阈值。Craik 等人 2017 年在微型表面阱中，使用近场微波控制，实现了 43Ca+离子的高精度空间和极化寻址[16]。

大规模离子阱量子计算的一种方案是使用相互连接的子系统，但此方案的前提条件是在子系统间可靠传送量子信息。Kaufmann 等人实现了$99.9994(+6/-7)\%$的单次离子传送正确率[17]。同时，为减少时间成本，需要对量子比特进行快速移动和分离。Walther 等人[18]实现了对于多区微结构 Paul 阱中离子的快速移动。离子在短短 5 个阱周期内，在比其基态波函数长度大10^4倍的距离穿梭（即 3.6 微秒内 280 微米）。离子初始时冷却到基态，移动

结束时，能量只增加了 0.1±0.01 声子能量。Bonler 等人研究了单个或多个离子在不同位置间移动或分离过程中的动力学[19]。结果是在 2MHz 谐振阱中单个 Be 离子，8 微秒内被传送了 370 微米，对应于 16 个振荡周期；对于双离子传送情形，可在 55 微秒内完成。

Allcock 等人曾于 2013 年设计、制造和测试了一个表面电极离子阱[20]，该阱整合了微波波导、谐振器、耦合单元，以使用近场微波操纵阱中离子量子比特。他们对阱进行了优化，使其具有大的微波场梯度，以允许对于离子运动自由度的操纵，而这是多量子比特纠缠的必备要素。Craik 等人[21]也给出表面离子阱设计，使用微波控制电极来进行单量子比特控制；使用标准光刻和电镀技术，制造了具有 2 个区域的原理验证电极阵列。讨论了对于微波驱动系统的要求，以及扩展到大型二维阱阵列的可能性。

Khromova 等人[22]曾于 2012 年，将核磁共振实验和离子阱量子计算优势结合，开拓了一个大规模量子计算新路径。Monroe 等人在 2013 年也指出，实用化的可扩展量子计算机硬件，需要不同类型量子系统的“混搭”[23]。他们设计了一个模块化离子阱量子计算机架构，其具有层次化相互作用，该相互作用可以扩展到非常大量的量子比特上。对于同一寄存器中不同量子比特存储器间局部纠缠量子门，是通过量子比特间自然相互作用实现；不同寄存器间纠缠是通过不同寄存器中量子比特间（即使量子比特间相距甚远）概率光子干涉实现的。展示该架构可容错实现，并且展示其用于中等规模量子线路容错执行的可行性。Lekitsch 等人在 2017 年给出一个基于离子阱的，模块化的可扩展量子计算机设计[24]，他们运用微波驱动量子门，利用阱间离子传送技术实现可扩展性。

6.6.2 纠缠及量子门实现

Slodicka 等人[25]曾在 2012 年，实现了 Cabrillo 等人提出的远距离离子间的纠缠[26]。协议基于单光子量子干涉和探测，该单光子是从两个相距 1 米的离子中散射出来的。实验探测到单光子预示着束缚离子内部两能态之间的以高概率纠缠，其正确率主要受限于离子运动。实验通过改变单光子干涉仪的路径长度，演示了对于纠缠态相位的控制。

Harty 等人[27]2014 年实现了对于单量子比特的制备、读取等所有操作，正确率大大高于容错量子计算的最小阈值。具体是使用 43Ca+超精细“原子钟”里存储的离子阱量子比特，测量到量子比特状态制备、读取联合正确率为99.93%，存储相干时间为 50s，门操作正确率99.9999%。Akerman 等人[28]2015 年在光学量子比特（量子比特的 2 个能级差为光学跃迁量级）上，基于$88Sr^+$离子，实现了高精度的通用门集合，包括单比特门和M${\o}$lmer-S${\o}$rensen 双比特门。

Ballance 等人 2014 年使用 43Ca+超精细离子实现双量子比特相位门，门精度97.1（2）% − 99.9（1）%[29]。2016 年他们进一步发展了实验结果，实现了激光驱动单、双量子比特门[30]，正确率分别为 99.9934 （3）、99.9 （1），远高于最小阈值。他们研究了双量子比特门的速度与正确率关系，实验中门作用时间为 3.85-520 微秒。

Cohen 等人 2015 年给出基于“包装态”（dresseed state）的相位门和M${\o}$lmer-S${\o}$rensen 门实现[31]，使用微波场作为驱动场。此门有望成为高精度微波多量子比特门的理想候选；此方案也可用激光实现。Wölk 等人 2017 年研究了动态梯度场中“ 包装态”囚禁离子的量子动力学[32]，研究结果可用于满足动态梯度场离子阱量子计算实验要求。

2017 年，Kaufmann 等人通过快速交换离子物理位置，实现了分区微离子阱中交换门[33]。Arrazola 等人在微波驱动离子阱中，实现了快速高精度双量子比特门，门操作时间为几十微秒，正确率高于99.9%[34]。Bermudez 等人[35]利用之前不受欢迎的离子晶体微运动，在某些参数条件下，提高了基于相位门的纠缠门操作方案速度，同时降低了错误率。

6.6.3 相干来源研究

Häffner 等人曾指出，离子阱量子计算中的退相干来源可以分为以下三类[36]: （1）比特翻转；（2）相位错误；（3）不够完美的控制。比特翻转主要来源于自发辐射，通过选择合适的量子比特能级，可以有效地减少此种退相干。相位错误主要来源于外部磁场的涨落，以及激光频率的起伏。不够完美的控制来源于有涨落的控制参数。如激光的频率和强度涨落、激光（对离子的）指向误差，以及特定离子上的脉冲可能会对离子本身（AC-Stark 位移或失谐跃迁）或相邻离子有非预想的作用。

近年来，对于离子阱中退相干的研究主要集中于对于离子运动加热所导致错误率。如，Hite 等人[37]研究了离子阱电极上吸附物对于离子加热速率的作用，发现去除吸附物后，离子加热速率降低到之前的 1/100。

6.6.4 量子算法实现

近年来，人们已在离子阱中实现了许多量子算法，包括 Deutsch-Jozsa 算法、密度编码、量子隐形传态、量子纠错、纠缠协助探测、量子傅里叶变换、Grover 搜索算法、纠缠交换、Toffoli 门等等。其中，Deutsch-Jozsa 算法是在 2003 年实现的[38]，运用在核磁共振中的复合脉冲技术，用单个 Ca 离子的电子和运动状态作为量子比特。2004 年实现了量子纠错算法[39]，用的是三个处于线性、多分区阱中的 Be 原子离子，一个编码单量子比特态被保护免受自旋翻转错误，这是通过一个三量子比特量子纠错码实现的。原则上，此方案允许通过重复纠错保持量子态，这对于实现可扩展容错离子阱量子计算来说是重要的一步。纠缠交换[40]和 Toffoli 门[41]分别于 2008、2009 年实现。Brickman 等人于 2005 年首次在离子阱量子计算机上实现了 2 量子比特的 Grover 算法[42]；2017 年，Figgatt 等人实现了完整 3 量子比特 Grover 搜索算法[33]。

Monz 等人 2016 年[44]提出可扩展 Shor 算法的实现（相应算法由 Kitaev[45]提出）。通过有效使用和控制 7 个量子比特和 4 个“缓冲量子比特”，以及实现通用算数操作，完成了对 15 的分解。该算法可在离子阱量子计算机上可扩展地执行，返回正确结果，正确率超过99%。

6.6.5 容错量子计算

Knill 在 2005 年提出了一个量子容错计算的简单模型[46]，提出了10^{-2}这一目前最大的容错量子计算阈值：证明在每个门的错误概率（EPG）达到3%时，精确量子计算是可能的，但是为了避免过多的资源消耗，需要更低的错误率。假设有像今天计算机的数字资源这么多的量子资源，作者提出 EPG 为1%的非平凡的量子计算可以实现。2009 年，Aliferis 和 Preskill[47]通过严格分析（而不是数值模拟）Knill 的 Fibonacci 量子容错计算方案，证明了对于局域随机噪声，阈值为0.67×10^{-3}，对于独立极化噪声，阈值为1.25×10^{-3}。虽然此结果比 Knill 自己的数值模拟结果低一个数量级，但和其他已证明具有类似精度的阈值的方案相比，Fibonacci 方案的成本大大减少。Fowler 等人 2012 年提出表面编码[48]，可用于大规模容错量子计算。

离子阱中快速高效的量子比特状态探测对于量子纠错等至关重要。Noek 等 2013 年对于 171Yb+超精细原子量子比特，提出一个简单的量子比特状态探测协议[49]，对于不同光强下的平均探测时间$10.5\mu s, 28.1\mu s$和$99.8\mu s$，探测正确率分别达到$99\%, 99.856(8)\%$和$99.915(7)\%$。

6.6.6 超导量子计算

超导量子计算方案自提出至今已有 20 年。起初，相干时间较短（仅几纳秒），但经过数年发展，逐渐形成多种可用的量子比特，如通量量子比特（flux qubit）、相位量子比特、quantronium 库伯电子对（CPB）等。下一个重要进展是在超导微波谐振器中嵌入量子比特，引入线路量子电动力学（cQED）概念。

之后，使用二维超导共面微波谐振器实现了开创性的进展，一方面是微波量子比特的操控、量子比特与谐振器间的强耦合、分散式结果读出[50]；另一方面是 CPB 量子比特和交换激发（swapping excitation）耦合，实现通用$\sqrt{iSWAP}$ 门[51]。

Transmon 量子比特于 2007 年提出[52]，其为可扩展多量子比特系统及场相干时间打下了基础。2011 年，嵌入三维腔的 transmon 相干时间增长至 100 微秒[53]。如今研究多集中于二维和三维多量子比特超导线路，其中量子比特和谐振器寿命较长，可实现大量高精度量子门。

目前，超导量子线路已扩展至数十量子比特规模，可据此研究量子计算和量子模拟中的实际问题[54-68]。

§6.7 量子计算机物理性质对量子计算的影响

6.7.1 容许逻辑深度

对大规模量子计算而言，错误的累积不可避免，这也是对于量子计算物理实现的巨大挑战。相干场驱动量子计算机（如离子阱）中，有一种特殊的错误率来源：在原始计算方案（如[8]）中，用于控制进行量子门操作的光场被认为是经典的，即不具量子性，但光场实际上是量子系统。量子化的激光场是不同粒子数态的相干叠加，而不同数态会导致被驱动的离子量子位产生不同的振荡，在多次操作下将失去协同性（uncorrelated），全量子理论下离子量子比特演化与经典平面波驱动下情况不同。而量子门操作步骤是依据经典场驱动下离子比特演化情况给出的，因此实际操作结果将可能与基于经典处理的期望结果不同，这将导致量子逻辑门出现与技术改进无关的错误。经过多次操作，此种错误累积将可能导致对量子计算不可忽略的影响。

基于此种考虑，科学家们在这方面做了一定的探索，如 Enk 和 Kimble 考虑相干场驱动量子计算机中，由于光场量子化，使得光场和量子比特纠缠（导致错误），并具体计算了纠缠度[69]。基于类似的出发点，Gea-Banacloche 计算了 Hadamard 门（量子计算中重要的单量子比特门）出现的附加错误率**错误！未找到引用源。**。但是他们的方法只是在光场的经典处理之上添加了量子“涨落”（fluctuations），而且并未考虑该量子性对于量子计算和量子算法实现的影响。回想场-原子相互作用理论的发展史，所谓“半经典”处理将光场视作经典的，可以解释拉比振荡的存在，但是它不能预测“崩塌-恢复（collapse and revival）”现

象，该现象是个纯量子效应，需要用 Jaynes-Cummings 模型才能解释，该模型中光学腔中光场是量子化的。同样道理，对于离子阱量子计算，许多二能级系统在进行脉冲串驱动的拉比振荡，一定存在无法用仅仅通过在经典处理上添加量子涨落来解释的现象，需要一个更为准确的全量子模型。

杨理和陈玉福在[71]中初步讨论了该问题，建立离子阱量子计算全量子模型的困难性主要体现在以下两个方面：一是对于量子计算系统及其多次门操作后的时间演化给出精确描述，二是以任意精度求解全量子处理中出现的三角级数求和。在杨理等人 2013 年文章[72]中，对于量子化脉冲串驱动下的二能级系统拉比振荡（其的一个直接应用便是相干场驱动量子计算），发展了一个模型来处理该二能级系统，提出一个以任意精度求解上述求和的算法，得到关于这个基本物理相互作用的一些有意义结果，结合容错量子计算的阈值定理，提出了量子计算机容许逻辑深度理论。此概念针对量子计算机物理实现方案，给出一个纠错周期内单个物理量子比特上操作数上限。它会对量子算法的单纠错周期逻辑深度给出限制。若一个量子算法在单纠错周期内容错线路中，某一物理量子比特上操作数超过了量子计算机的容许逻辑深度，即可认为量子计算机无法执行此算法。这为设计量子算法和分析量子攻击可行性提供了重要的依据。

之后，杨碧瑶、杨理等人发展了[72]中的结果，将场-原子相互作用的全量子理论应用于离子阱量子计算方案，首次给出了受控非门的全量子操作结果，进而给出多次受控非门操作后的错误率，最终给出离子阱容错量子计算的容许逻辑深度，在给定条件下，约为10^2量级。

6.7.2 容错量子计算

由于量子计算机实质上是一个物理系统，其具体实现过程中，会受到很多物理因素的影响，这些因素有可能会破坏相干性（即所谓退相干），从而导致计算的错误。要对抗这种退相干，容错量子计算（Fault-tolerant quantum computation, FTQC）应运而生，它使得大规模量子计算变得可行。在 FTQC 中，量子线路中的每一量子比特被运用纠错码编码后的逻辑比特取代，逻辑门用容错门取代。通过周期性地进行纠错，可以阻止量子态上差错的积累。但 FTQC 所能纠正的错误率有一定的限制，具体由阈值定理给出。

FTQC 中，对于单个量子比特而言，对它自身进行纠错编解码的算法有一定深度；中间量子算法线路所用的容错逻辑门进一步增大了单个物理量子比特上的物理门操作数，尤其是考虑到物理上实现任一单量子比特门是由若干个 Hadamard 门和 T 门以任意精度近似，同一物理位上会有大量门操作；再加上 FTQC 中需要运用容错地纠错和级联码，这使得 FTQC 中作用在单个量子比特上的物理门操作数更为增加。可以想见，前述由于量子计算机物理性质导致的错误率，经过多次门操作的累积，可能使得错误率超过允许的阈值，量子计算便可能无法正常进行。

6.7.3 量子算法运行时间下限估计

杨理和周瑞瑞从另一个角度考虑了量子计算机的物理局限[74]。Shor 算法在解决离散对数问题时需要用到大量的量子比特，需要在许多量子位之间进行 CNOT 门操作，而相距较远的量子位之间的 CNOT 操作是利用声子等集体激发粒子来传递相互作用的。这使得操作的效率受到声子等媒介运动速度的限制，由于上述物理原理约束，Shor 算法解决离散对数问题所用的时间是有下限的。

杨理等人基于可实现的参数对该时间下限首次给出了估计，论证了加密密钥交换（EKE）协议的后量子安全性，并提出了具有后量子安全性的无密钥协议。该 EKE 协议同时采用对称加密和非对称加密，使用一个短的口令来生成一个长的会话密钥。对于此类密钥交换方案的主要攻击方式为字典攻击，即敌手可以通过穷举所有可能的口令来获得其会话密钥，但由于经典计算机能力的局限性，同时在限定使用环境的条件下，可以在一定程度上确保其被安全使用。假设敌手的计算能力进一步提升，即敌手拥有一台量子计算机，其实际破解 EKE 的能力主要取决于其运行求解离散对数算法等量子算法所需时间，而这又取决于单个门的操作时间和门操作数。

§6.8 基于主动防御思想的后量子密码设计

目前后量子密码的安全性基本是基于已有量子算法来分析的，其安全性建立在尚没有有效量子算法可以将其攻破的基础之上，这是一种被动的防御。随着新的量子算法的提出，这些密码体制的安全性随时可能受到威胁。因此，为了设计抗量子的密码体制，需要深入到量子计算机内部，考察量子计算机作为物理系统本身存在的局限性，进而研究量子计算机计算能力上的理论极限，并基于这些理论极限给出量子计算环境下的密码设计准则，构造安全的密码体制。这样构造的对称密码体制的安全性不受新的量子算法提出的影响。称这个思路为“主动防御”。

举例来说，基于格编码、多变量等的密码协议近年来取得了很好的发展，达到了实用化程度，对于实现抗量子的保密通信具有较大现实意义。然而，这些密码协议的安全性是基于已有量子算法来确定的，即现有的量子算法无法攻破，将来的量子算法能否攻破则是不确定的。随着量子算法的发展，上述密码协议安全性曾受到过威胁。如，2016 年 11 月，L. Eldar 和 P. Shor 声称提出了一个量子算法能够解决格上的最短向量问题[75]，引起了整个密码学界的震动。虽然该量子算法最终被发现存在错误，但这说明了量子算法已向基于格编码的密码协议发起了冲击。又如，2001 年，E.Farhi 等人将绝热量子计算应用于求解 NP 完全问题[76]，他们的绝热量子算法对于规模较小的情形有很好的结果，这对于多变量密码算法构成威胁，此种采用绝热量子计算的方案受到 P. Shor 的认可。基于格编码、多变量等的密码协议是否能抗击量子攻击将不确定。

基于前述量子计算机的物理性质，得到了其本身的局限性，进而得出量子计算机计算能力上的理论极限，从而可构造抗量子攻击的密码协议。如根据[73]，对于目前最有可能率先实现的离子阱量子计算机，一般同一量子比特上的物理操作数不能超过10^2；若某一量子算法执行过程中，同一量子比特上的物理操作数会超过10^2，则该算法不能成功执行。故而可构造有关密码协议，使得可能攻击其的量子算法不能在量子计算机上成功执行。此种后量子密码不随未来量子算法发展而失去安全性，能达到真正“主动防御”的效果，构筑起真正牢固的信息安全防线。

参考文献

[1] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In Proc. 35th IEEE Symposium on the Foundations of Computer Science-FOCS 1994, pages 124-134, 1994.

[2] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. COMPUT., 26(5):1484-1509, 1997.
[3] Lov K. Grover. A fast quantum mechanical algorithm for database search. In STOC 1996, pages 212-219, 1996.
[4] Lov K. Grover. Quantum mechanics helps in searching for a needle in a haystack. PHYSICAL REVIEW LETTERS, 79:325-328, 1997.
[5] Li Y, Yang B, Chen Y. Full Quantum Treatment of Rabi Oscillation Driven by a Pulse Train and Its Application in Ion-Trap Quantum Computation[J]. IEEE Journal of Quantum Electronics, 2013, 49(8):641-651.
[6] Liang M, Li Y. A note on threshold theorem of fault-tolerant quantum computation[J]. Physics, 2010.
[7] Nielsen, M. A. and Chuang, I. L. Quantum Computation and Quantum Information. 2010. Cambridge University Press.
[8] J.I. Cirac and P.Zoller, “Quantum computations with cold trapped ions,” Phys. Rev. Lett., vol. 74, no. 20,pp. 4091–4094, May. 1995.
[9] Y. Nakamura , Y. A. Pashkin , and J. S. Tsai . "Coherent control of macroscopic quantum states in a single-Cooper-pair box." Nature 398. 1999.
[10] E. Knill, R. Laflamme , and G. J. Milburn . "A scheme for efficient quantum computation with linear optics. " Nature 409.6816(2001):46-52.
[11] N. A. Gershenfeld , I. L. Chuang "Bulk Spin-Resonance Quantum Computation." Science 275.5298(1997):350-356.
[12] Steane, A. (1997). "The ion trap quantum information processor". Appl. Phys. B. 64: 623–643.
[13] [13]C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, “Demonstration of a fundamental quantum logic gate,” Phys. Rev. Lett., vol. 75, no. 25,pp. 4714–4717, December. 1995.
[14] [14]Warring, U., Ospelkaus, C., Colombe, Y., Jördens, R., Leibfried, D., Wineland, D. J. (2013) Individual-ion addressing with microwave field gradients.?Physical Review Letters,?110(17), 173002.
[15] [15]Piltz, C., Sriarunothai, T., Varón, A. F., Wunderlich, C. (2014) A trapped-ion-based quantum byte with 10^{-5} next-neighbour cross-talk.?Nature Communications,?5,4679.
[16] [16]Aude Craik, D. P. L.,Linke, N. M.,Sepiol, M. A.,Harty, T. P., Goodwin, J. F.,Ballance, C. J., Stacey, D. N.,Steane, A. M., Lucas, D. M., and D. T. C. Allcock (2017) High-fidelity spatial and polarization addressing of 43Ca+ qubits using near-field microwave control.?Physical Review A,?95,022337.
[17] [17]Kaufmann, P., Gloger, T. F., Kaufmann, D., Johanning, M., and Wunderlich, C. (2017). High-fidelity preservation of quantum information during trapped ion transport.arXiv:quant-ph1704.02141.
[18] [18]Walther, A., Ziesel, F., Ruster, T., Dawkins, S. T., Ott, K., Hettrich, M., et al. (2012) Controlling fast transport of cold trapped ions.?Physical Review Letters,?109(8), 080501.
[19] [19]Bowler, R., Gaebler, J., Lin, Y., Tan, T. R., Hanneke, D., Jost, J. D., et al. (2012) Coherent diabatic ion transport and separation in a multizone trap array.?Physical Review Letters,?109(8), 080502.
[20] [20]Allcock, D. T. C., Harty, T. P., Ballance, C. J., Keitch, B. C., Linke, N. M., Stacey, D. N., et al. (2013) A microfabricated ion trap with integrated microwave circuitry.?Applied Physics Letters,?102(4), 175.
[21] [21]Craik, D. P. L. A., Linke, N. M., Harty, T. P., Ballance, C. J., Lucas, D. M., Steane, A. M., et al. (2014) Microwave control electrodes for scalable, parallel, single-qubit operations in a

surface-electrode ion trap.?Applied Physics B,?114, 3-10.
[22] [22]Khromova, A., Piltz, C., Scharfenberger, B., Gloger, T. F., Johanning, M., Varón, A. F., et al. (2012) Designer spin pseudomolecule implemented with trapped ions in a magnetic gradient.?Physical Review Letters,?108(22), 220502.
[23] [23]Monroe, C., Raussendorf, R., Ruthven, A., Brown, K. R., Maunz, P.,Duan, L. M., et al. (2012) Large scale modular quantum computer architecture with atomic memory and photonic interconnects.?Physical Review A,?89(2)
[24] [24]Lekitsch, B., Weidt, S., Fowler, A. G., M${\o}$lmer, K., Devitt, S. J., Wunderlich, C., et al. (2017)Blu for a microwave trapped ion quantum computer.?Science Advances,?3(2), e1601540.
[25] [25]Slodička, L., Hétet, G., Röck, N., Schindler, P., Hennrich, M., Blatt, R. (2013) Atom-atom entanglement by single-photon detection.?Physical Review Letters,?110(8), 083603.
[26] [26]Cabrillo, C., Cirac, J. I., Garciafernandez, P.,Zoller, P. (1998) Creation of entangled states of distant atoms by interference.?Physical Review A,?59(2), 1025-1033.
[27] [27]Harty, T. P., Allcock, D. T., Ballance, C. J., Guidoni, L., Janacek, H. A.,Linke, N. M., et al. (2014) High-fidelity preparation, gates, memory, and readout of a trapped-ion quantum bit.?Physical Review Letters,?113(22), 220501.
[28] [28]Akerman, N., Navon, N., Kotler, S., Glickman, Y.,Ozeri, R. (2015) Universal gate-set for trapped-ion qubits using a narrow linewidth diode laser.?New Journal of Physics,?17(11), 113060.
[29] [29]Ballance, C. J., Harty, T. P., Linke, N. M., Lucas, D. M. (2014) High-fidelity two-qubit quantum logic gates using trapped calcium-43 ions.?arXiv: quant-ph/1406.5473.
[30] [30]Ballance, C.J.,Harty, T.P.,Linke, N.M., Sepiol, M.A., Lucas. D.M. (2016) High-fidelity quantum logic gates using trapped-ion hyperfine qubits. Physical Review Letters,?117(6), 060504.
[31] [31]Cohen, I., Weidt, S., Hensinger, W. K., Retzker, A. (2015) Multi-qubit gate with trapped ions for microwave and laser-based implementation.?New Journal of Physics,?17(4).
[32] [32]Wölk, S., Wunderlich, C. (2017). Quantum dynamics of trapped ions in a dynamic field gradient using dressed states.?New Journal of Physics,?19.
[33] [33]Kaufmann, H., Ruster, T., Schmiegelow, C. T., Luda, M. A., Kaushal, V., and Schulz, J., et al. (2017). Fast ion swapping for quantum-information processing.?Physical Review A,?95, 052319.
[34] [34]Arrazola, I., Casanova, J., Pedernales, J. S., Wang, Z. Y., Solano, E., andPlenio, M. B. (2017). Fast and robust two-qubit gates with microwave-driven trapped ions.arXiv:quant-ph/1706.02877.
[35] [35]Bermudez, A., Schindler, P., Monz, T., Blatt, R., and Müller, M. (2017). Micromotion-enabled improvement of quantum logic gates with trapped ions. ?arXiv:quant-ph/1705.02456.
[36] [36]H?ffner, H., Roos, C. F., Blatt, R. (2008) Quantum computing with trapped ions.?Physics Reports,?469(4), 155-203.
[37] [37]Hite, D. A., Colombe, Y., Wilson, A. C., Brown, K. R., Warring, U.,Jördens, R., et al. (2012) 100-fold reduction of electric-field noise in an ion trap cleaned with in situ argon-ion-beam bombardment.?Physical Review Letters,?109(10), 103001.
[38] [38]Gulde S., Riebe M., Lancaster G. P. T., Becher C., Eschner J., Häffner H., Schmidt-Kaler F., Chuang I. L. and Blatt R.(2003) Implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer. Nature, 421(2):48-50.
[39] [39]Chiaverini J., Leibfried D., Schaetz T., Barrett, M. D.Blakestad R. B., Britton J.,

ItanoW.M., Jost J. D., Knill E., Langer C., et al.(2004) Realization of quantum error correction.Nature, 432(2):602-605,.

[40] [40]Riebe M., Monz T., Kim K., Villar A. S., Schindler P., Chwalla M., Hennrich M., Blatt R. (2008)Deterministic entanglement swapping with an ion trap quantum computer. Nature Physics 4, 839.

[41] [41]Monz T., Kim K., Hänsel W., Riebe M., Villar A., Schindler P., Chwalla M., Hennrich M., Blatt R. (2009) Realization of the quantum Toffoli gate with trapped ions. Physical Review Letters,?102, 040501.

[42] [42]Brickman, K. A., Acton, M., Deslauriers, L., Haljan, P. C., Lee, P. J., Monroe, C., et al. (2005). Implementation of Grover's quantum search algorithm in a scalable system.?Physical Review A,?72,050306.

[43] [43]Figgatt, C., Maslov, D., Landsman, K. A., Linke, N. M., Debnath, S., and Monroe, C. (2017). Complete 3-qubit grover search on a programmable quantum computer.?Nature Communications,?8.

[44] [44]Monz, T., Nigg, D., Martinez, E. A., Brandl, M. F., Schindler, P.,Rines, R., et al. (2016) Realization of a scalable shor algorithm.?Science,351(6277), 1068.

[45] [45]Kitaev, A. Y. (1995) Quantum measurements and the abelian stabilizer problem.?arXiv:quant-ph/9511026

[46] [46]Knill, E. (2005) Quantum computing with realistically noisy devices.?Nature,?434(7029), 39.

[47] [47]Aliferis, P., Preskill, J. (2009)Thefibonacci scheme for fault-tolerant quantum computation.?Physical Review A,?79(20)，012332.

[48] [48]Fowler, A. G., Mariantoni, M., Martinis, J. M., Cleland, A. N. (2012) Surface codes: towards practical large-scale quantum computation.?,86(3), 6691-6699.

[49] [49]Noek, R., Vrijsen, G., Gaultney, D., Mount, E., Kim, T., Maunz, P., et al. (2013) High speed, high fidelity detection of an atomic hyperfine qubit.?Optics Letters,?38(22), 4735.

[50] [50]Wallraff A, Schuster D I, Blais A, Frunzio L, Huang R-S, Majer J, Kumar S, Girvin S M and Schoelkopf R J 2004 Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics Nature 431 162–7.

[51] [51]Majer J et al 2007 Coupling superconducting qubits via a cavity bus Nature 449 443–7.

[52] [52]Koch J et al 2007 Charge insensitive qubit design from optimizing the cooper-pair box Phys. Rev. A 76 042319.

[53] [53] Paik H et al 2011 Observation of high coherence in Josephson junction qubits measured in a threedimensional circuit QED architecture Phys. Rev. Lett. 107 240501.

[54] [54]Chow J M et al 2014 Implementing a strand of a scalable fault-tolerant quantum computing fabric Nat. Commun. 5 4015.

[55] [55]Córcoles A D, Magesan E, Srinivasan S J, Cross A W, Steffen M, Gambetta J M and Chow J M 2015.Demonstration of a quantum error detection code using a square lattice of four superconducting qubits Nat. Commun. 6 6979.

[56] [56]Takita M, Córcoles A D, Abdo B, Brink M, Cross A, Chow J M and Gambetta J M 2016 Demonstration of weight-four parity measurements in the surface code architecture Phys. Rev. Lett. 117 210505.

[57] [57]Takita M, Cross A W, Córcoles A D, Chow J M and Gambetta J M 2017 Experimental demonstration of faulttolerant state preparation with superconducting qubits (arXiv:1705.09259v1) Rep. Prog. Phys. 80 (2017) 106001.

[58] [58]Versluis R, Poletto S, Khammassi N, Haider N, Michalak D J, Bruno A, Bertels K and DiCarlo L 2016 Scalable quantum circuit and control for a superconducting surface code (arXiv:1612.08208v1).

[59] [59]Barends R et al 2014 Superconducting quantum circuits at the surface code threshold for fault tolerance Nature 508 500–3.
[60] [60]Saira O-P, Groen J P, Cramer J, Meretska M, de Lange G and DiCarlo L 2014 Entanglement genesis by Ancilla–Based parity measurement in 2D circuit QED Phys. Rev. Lett. 112 070502.
[61] [61]Riste D, Poletto S, Huang M-Z, Bruno A, Vesterinen V, Saira O-P and DiCarlo L 2015 Detecting bit-flip errors in a logical qubit using stabilizer measurements Nat. Commun. 6 6983.
[62] [62]Kelly J et al 2015 State preservation by repetitive error detection in a superconducting quantum circuit Nature 519 66–9.
[63] [63]Barends R et al 2015 Digital quantum simulation of fermionic models with a superconducting circuit Nat. Commun. 6 7654.
[64] [64]Barends R et al 2016 Digitized adiabatic quantum computing with a superconducting circuit Nature 534 222–6.
[65] [65]O'Malley P J J et al 2016 Scalable quantum simulation of molecular energies Phys. Rev. X 6 031007.
[66] [66]Asaad S, Dickel C, Poletto S, Bruno A, Langford N K, Rol M A, Deurloo D and DiCarlo L 2016 Independent, extensible control of same-frequency superconducting qubits by selective broadcasting npj Quantum Inf. 2 16029.
[67] [67] Song C et al 2017 10-qubit entanglement and parallel logic operations with a superconducting circuit (arXiv:1703.10302v1).
[68] [68]Kandala A, Mezzacapo A, Temme K, Takita M, Chow J M and Gambetta J M 2017 Hardware-efficient quantum optimizer for small molecules and quantum magnets hardwareefficient quantum optimizer for small molecules and quantum magnets (arXiv:1704.05018).
[69] [69]Enk V, S. J, Kimble, et al. On the classical character of control fields in quantum information processing[M]. Rinton Press, Incorporated, 2002.
[70] [70]J. Gea-Banacloche, Some implications of the quantum nature of laser fields for quantum computations. Phys. Rev. A, 65, 022308 (2002).
[71] [71]Li Yang and Yufu Chen, A decoherence limit of fault-tolerant quantum computation driven by coherent fields, Proceedings of SPIE 6827, pp. 6827081-6827086, Conference of Quantum Optics and Application in Computing and Communications, SPIE Photonics Asia 2007, 11-15 November 2007, Beijing
[72] [72]Li Yang, Biyao Yang and Yufu Chen. Full Quantum Treatment of Rabi Oscillation Driven by a Pulse Train and Its Application in Ion-Trap Quantum Computation[J]. IEEE Journal of Quantum Electronics, 2013, 49(8):641-651.
[73] [73]Biyao Yang and Li Yang. Effect on ion-trap quantum computers from the quantum nature of the driving field. Sci China Inf Sci, 2020, 63(10): 202501,.
[74] [74]Yang L , Zhou R R . On the post-quantum security of encrypted key exchange protocols (arXiv:1305.5640).
[75] [75]*Lior Eldar*, *Peter W. Shor*. An Efficient Quantum Algorithm for a Variant of the Closest Lattice-Vector Problem. *arXiv:1611.06999* ,2016.
[76] [76]E Farhi , J Goldstone, S Gutmann. et. al., A Quantum Adiabatic Evolution Algorithm Applied to Random Instances of an NP-complete Problem. Science, , 2001 , 292 (5516) :472.

第 7 章 纠错码与容错量子计算

§7.1 简介

噪声对信息处理系统有着很大的危害，因此在建立信息系统时要尽量避免噪声。现在很多在广泛使用的系统就遭受着实质性的噪声问题。调制解调器和 CD 就利用了误差纠错码来防止噪声污染。在实际中，用来防止噪声的技术细节往往是十分复杂的，但是基本原理是容易理解的。核心思想就是如果想要保护信息免受噪声污染，就需要往信息中添加冗余信息。这样的话，即便在编码后的消息中的信息会被噪声影响，在编码后的消息中仍然有足够多的冗余度使得能够恢复或者解码消息，这样在原始消息中的信息就会得到恢复。

比如，假设希望在有噪声的经典信道中从一个地方到另一个地方发送一个比特的信息。在信道中噪声的作用是以p的概率使得被传送的比特翻转，而以$1-p$的概率使比特无差错传输。这种信道叫做二元对称信道。针对二元对称信道中噪声的影响来保护比特的一个简单手段是，把想要保护的比特替换为其自身的三份备份。$0 \to 000, 1 \to 111$。这个比特串 000 和 111 有时被叫做逻辑 0 和逻辑 1，因为它们分别扮演 0 和 1 的角色。现在通过信道发送所有这三个比特，在信道的接收方三个比特均为输出，且接收方必须确定原来的比特值是什么。假设得到信道的输出为 001.规定一个比特翻转的概率p不太高，则非常有可能是第三比特被信道翻转，而 0 是所发送的比特。

这种类型的解码方式叫做多数判决，因为信道的解码输出不论是 1 还是 0，在实际信道输出都占多数。如果通过信道发送的比特中两个或多个被翻转，那么多数判决失败，否则多数判决成功。所有比特中两个或者多个被翻转的概率为$3p^2(1-p)+p^3$，所以差错的概率为$p_e = 3p^2 - 2p^3$。要是没有编码，出现一个差错的概率为p，所以只要$p_e < p$这种编码就会使得传输更为可靠，而$p < 1/2$就是这种情况。

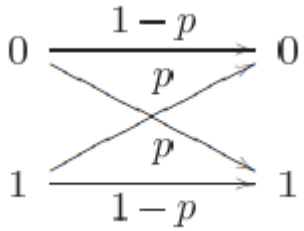


图 7.1-1 二元对称信道

上面所述是通过将发送的消息重复多次来对其编码的，这类码叫做重复码。类似的思想在经典中用了很多，核心思想都是通过加入足够的冗余来编码消息，使得有噪声的编码消息仍可以恢复原有的消息，至于需要添加的冗余量则依赖于信道中噪声的严重程度。

§7.2 编码理论基本概念

7.2.1 编译码概念

编码过程是m位二进制数到n位二进制数的转换：$\mathcal{E}: B^m \to B^n$；译码过程刚好相反，表示为$\mathcal{D}: B^n \to B^m$。

$W = (w_1, w_2, \cdots w_n)$是$n$位二元码，即$w_i \in \{0,1\}$，接收端收到的是$R = (r_1, r_2, \cdots, r_n)$，设$R = W \oplus E$，其中$E = (e_1, e_2, \cdots e_n)$，显然：

$$e_i = \begin{cases} 0, w_i = r_i \\ 1, w_i \neq r_i \end{cases} \tag{7.2.1}$$

易知：$W = R \oplus E$，其中$E = W \oplus R$为错误矢量。

设$A = (a_1, a_2, \cdots a_n) \in B^n, B = (b_1, b_2, \cdots, b_n) \in B^n$。令$W(A)$为$A$的权重，即为 1 的分量的个数。

$d(A,B) = w(A \oplus B)$称为A与B的Hamming距离。关于Hamming距离有如下几个引理。

引理 7.2.1：若$A, B, C \in B^n$，则

（1）$d(A,B) = d(B,A)$

（2）$d(A,C) \leq d(A,B) + d(B,C)$

7.2.2 码字的检错和纠错

关于码字的检错和纠错有如下两个定理。

定理 7.2.1：一组码可以检出k个错误的充要条件是这组码的码字间最短距离至少为$k+1$。

证明：$\mathcal{E}: B^m \to B^n$，$A \in B^n$是码字，传输后接收到R，$E = A \oplus R$，$w(E) = d(A,R)$。错误E可被检出的充要条件：R不是码字。因此，$w(E) \leq k$的所有误差可被检出的充要条件是不存在码字$B \neq A$满足$d(A,B) \leq k$，即：任意两个不同码字间的距离d至少为$k+1$。

定理 7.2.2：已知一组编码的任意两码字的最短距离为$2k+1$，则所有权不超过k的误差可得到纠正。

证明：设A是一个码字，在传输过程中发生误差，接收到的为R，$d(A,R) \leq k$。如果有码字B在传输过程中也接收到R，且$d(B,R) \leq k$，则有$d(A,B) \leq d(A,R) + d(B,R) \leq k + k < 2k+1$。即两码字$A$和$B$之间的距离小于$2k+1$，与定理假设矛盾。故知：不可能在权不超过$k$的误差下，两不同码字在接收端相同。所以，所有权不超过k的误差可以得到纠正。

7.2.3 线性码

取矩阵$G = \left(g_{ij}\right)_{mn}$，取编码过程为$W = AG$，其中$A = \left(a_1, a_2, \ldots, a_m\right) \in B^m$，则成$G$为生成矩阵。例如：

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}, A = \left(011\right) \tag{7.2.2}$$

对应有码字：

$$W=(011)\begin{pmatrix}1&0&0&1&1&0\\0&1&0&0&1&1\\0&0&1&1&0&1\end{pmatrix}=(011110) \tag{7.2.3}$$

特别是，若取生成矩阵

$$G=\begin{pmatrix}1&0&0&\cdots&0&g_{1,m+1}&g_{1,m+2}&\cdots&g_{1,n}\\0&1&0&\cdots&0&g_{2,m+1}&g_{2,m+2}&\cdots&g_{2,n}\\0&0&1&\cdots&0&g_{3,m+1}&g_{3,m+2}&\cdots&g_{3,n}\\\vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&\cdots&1&g_{m,m+1}&g_{m,m+2}&\cdots&g_{m,n}\end{pmatrix} \tag{7.2.4}$$

则有码字：

$$\begin{aligned}W=AG&=(a_1,a_2,...,a_m)\begin{pmatrix}1&0&\cdots&0&g_{1,m+1}&\cdots&g_{1,n}\\0&1&\cdots&0&g_{2,m+1}&\cdots&g_{2,n}\\\vdots&\vdots&\ddots&\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&1&g_{m,m+1}&\cdots&g_{m,n}\end{pmatrix}\\&=(w_1,w_2,...,w_n)\end{aligned} \tag{7.2.5}$$

显然有：

（1）$w_1=a_1,w_2=a_2,\cdots,w_m=a_m$

（2）$w_j=a_1g_{1,j}+\cdots+a_mg_{m,j}$

由（1）（2）有：$w_{m+j}=g_{1,m+j}w_1+g_{2,m+j}w_2+\cdots+g_{m,m+j}w_m,j=1,\cdots,n-m$

码字的各位满足上述关系，可以用于校验。故码字可以表示为：n 位=m 位（信息位）+n-m 位（校验位，偶校验）

比如，

$$G=\begin{pmatrix}1&0&0&1&1&0\\0&1&0&0&1&1\\0&0&1&1&0&1\end{pmatrix},(a_1,a_2,a_3)G=(w_1,w_2,\cdots,w_6) \tag{7.2.6}$$

则有：

$$\begin{cases}w_1+w_3+w_4=0\\w_1+w_2+w_5=0\\w_2+w_3+w_6=0\end{cases} \tag{7.2.7}$$

可得：

$$G=\begin{pmatrix}1&0&0&1&1&0\\0&1&0&0&1&1\\0&0&1&1&0&1\end{pmatrix},(a_1,a_2,a_3)G=(w_1,w_2,\cdots,w_6) \tag{7.2.8}$$

可得：

$$\begin{pmatrix}1&0&1&1&0&0\\1&1&0&0&1&0\\0&1&1&0&0&1\end{pmatrix}\begin{pmatrix}w_1\\w_2\\\vdots\\w_6\end{pmatrix}=\begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix}$$

一般情况有

$$\begin{aligned}g_{1,m+1}w_1+g_{2,m+1}w_2+\cdots+g_{m,m+1}w_m+w_{m+1}=0\\g_{1,m+2}w_1+g_{2,m+2}w_2+\cdots+g_{m,m+2}w_m+w_{m+2}=0\\g_{1,n}w_1+g_{2,n}w_2+\cdots+g_{m,n}w_m+w_n=0\end{aligned} \tag{7.2.9}$$

可写成$HW^T=0$，其中$W=AG$

$$H=\begin{pmatrix}g_{1,m+1}&g_{2,m+1}&\cdots&g_{m,m+1}&1&0&0&\cdots&0\\g_{1,m+2}&g_{2,m+2}&\cdots&g_{m,m+2}&0&1&0&\cdots&0\\&\cdots&\cdots&&\vdots&&&\ddots&0\\g_{1,n}&g_{2,n}&\cdots&g_{m,n}&0&0&0&\cdots&1\end{pmatrix}_{(n-m)\times n}$$

H称为对应于生成矩阵G的校验矩阵。已知G可求得H，反之亦然。

校验矩阵H可用于纠正一位错误，例如：

$$H=\begin{pmatrix}1&0&1&1&0&0\\1&1&0&0&1&0\\0&1&1&0&0&1\end{pmatrix},R=\begin{pmatrix}1&0&0&1&0&1\end{pmatrix} \tag{7.2.10}$$

则$HR^T=\begin{pmatrix}0\\1\\1\end{pmatrix}\neq\begin{pmatrix}0\\0\\0\end{pmatrix}$，$R$不是码字，设$R=W+E$，则：

$$HR^T=HW^T+HE^T=HE^T\text{。} \tag{7.2.11}$$

若$E=(0\cdots010\cdots0)$，则HE^T必是矩阵H的第i列

故根据$HE^T=\begin{pmatrix}0\\1\\1\end{pmatrix}$，知第二位出错，纠正得$W=(110101)$，取信息位得$A=(110)$，

若出现两个错误，则不能正确译码。

译码步骤：接收到$R=(r_1,r_2,\cdots,r_n)$

（1） 计算校正子$s=HR^T$

（2） 若$s=0$，确认原信息即为$(r_1,r_2,\cdots,r_m)$；若$s\neq 0$，则进行（3）

（3） 若s是H的第i列，则认为R在第i位出错，可纠正得到R_1，取R_1的前m位作为信息。

若s不为H的某一列，则认为至少出现两个错误，不能正确译码。

下面给出有关校验矩阵和生成矩阵的定理。

定理 7.2.3：校验矩阵$H=(h_{ij})_{(n-m)\times n}$能纠正一个错误的充要条件是$H$的各列互不相同且非零。

证明：充分性显然成立，现在证明必要性。

①若H的第i列为零向量，对于第i位出错的情形，有$H(W+E)^T=HE^T=0$

②若H的第i列和第j列相同，则第i位和第j位的错误将无法区分，而且，两位都出错时，将误以为传输正确。

定理 7.2.4：设$A=(a_{ij})_{m\times(n-m)}$是$(0,1)$矩阵，若以矩阵$G=(I_m\vdots A)$为生成矩阵，则对应的校验矩阵为$H=(A^T\vdots I_{n-m})$，其中$I_m$是$m$维的单位矩阵。

7.2.4 Hamming 码

首先介绍几个编码理论的基本概念。

（1）完全码：一个极小距离为$2k+1$的码称为完全码，如果每个向量都恰与一个码字之间的距离$\leq k$。本节介绍的 Hamming 码就是一种完全码。

（2）线性码：一个线性码C是一个线性子空间。若C的维数是m，则说C是一个$[n,m]$码。

线性码的生成矩阵G是一个$m\times n$矩阵，其行向量是C的一组基。如果$G=(I_m,A)$，则称G是标准型的。

（3）对偶码：设C是$[n,m]$码，定义对偶码$C^{\perp}$为：

$$C^{\perp}\equiv\left\{y\mid y\in F_2^{(n)}satisfies:\ for\ any\ x\in C,x_1y_1\oplus x_2y_2\oplus\cdots\oplus x_ny_n=0\right\}$$

当$C=C^{\perp}$时，称C是自对偶码。

若$G=\left(I_m,A\right)$是码C的标准型生成矩阵，那么$H=\left(A^T,I_{n-m}\right)$是$C^{\perp}$的生成矩阵。

接下来简单介绍 Hamming 码的构造。

编译码器简单，构造容易，使用普遍。构造$\left(n-m\right)\times n$校验矩阵$H=\left(h_{ij}\right)$如下：令$l=n-m$为列向量的维数（即行数），则可得到2^l-1个不同的非零列向量，将其排成$\left(n-m\right)\times n$矩阵H_l，使后面l列恰好构成I_l。这种校验矩阵对应的纠错码即为 Hamming 码。例如：

$$H_3=\begin{pmatrix}0&1&1&1&1&0&0\\1&0&1&1&0&1&0\\1&1&0&1&0&0&1\end{pmatrix},A_{4\times3}\to G_{4\times7} \tag{7.2.12}$$

可以将 4 位编码成 7 位。

$$H_4=\begin{pmatrix}1&1&1&0&0&0&1&1&1&0&1&1&0&0&0\\1&0&0&1&1&0&1&1&0&1&1&0&1&0&0\\0&1&0&1&0&1&1&0&1&1&1&0&0&1&0\\0&0&1&0&1&1&0&1&1&1&1&0&0&0&1\end{pmatrix},A_{11\times4}\to A_{11\times15} \tag{7.2.13}$$

可以将 11 位编码成 15 位。

§7.3 三量子比特的量子纠错码

7.3.1 三量子比特的比特翻转码

下面引入量子纠错码，经典信息和量子信息之间存在着一些重要的区别，这就需要引入一种新的思想以使得这样的量子纠错码成为可能。在这个过程中，将会涉及三个重大的困难问题。

（1）不可克隆：有人可能试图通过将量子状态复制三次或者多次，用量子力学方式来实现类似于经典中的重复码。然而根据量子不可克隆定理，这是不可能的。即使复制是可能的，也不可能来度量和比较来自信道的三个量子状态输出。

（2）差错是连续的：连续的不同差错可能出现在单量子比特上。为了纠正差错就必须确定哪个差错，这需要无限精度也就需要无限的资源。

（3）测量会破坏量子信息：在经典纠错中，会观测来自信道的输出，并决定采用什么样的解码步骤，量子力学中的观测一般会破坏所观测的量子状态并使恢复成为不可能。

然而，这三个困难问题并不是致命的。设通过一个信道发送量子比特，信道以概率$1-p$保持量子比特不变，以概率p使量子比特翻转。即，以概率p状态$|\psi\rangle$被取代为$X|\psi\rangle$，其中X为通常的 Pauliσ_x算子或者比特翻转算子。这种信道叫做比特翻转信道。现在来解释比特翻转码，这种码可以被用来针对来自这种信道的噪声的影响来保护量子比特。

设将单量子比特状态$a|0\rangle+b|1\rangle$用三个量子比特编码为$a|000\rangle+b|111\rangle$。一个方便的做法是把这个编码写成$|0\rangle\rightarrow|0_L\rangle\equiv|000\rangle, |1\rangle\rightarrow|1_L\rangle\equiv|111\rangle$。

其中可以理解，基状态的叠加被取为相应编码状态的叠加，符号$|0_L\rangle, |1_L\rangle$表示逻辑$|0\rangle$和逻辑$|1\rangle$状态，而不是物理的 0 和 1 状态，执行这种编码的线路如图所示

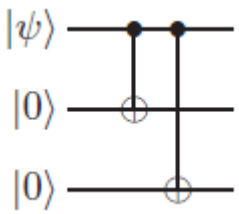


图 7.3-1 三量子比特的比特翻转码的编码线路

设初始工作状态$a|0\rangle+b|1\rangle$已被完美地编码为$a|000\rangle+b|111\rangle$。这三个量子比特中的每一个都通过一个比特翻转信道的独立备份。设一个或更少的量子比特出现了一个比特翻转。有一种简单的两阶段纠错方法，可用于恢复和纠正这种情况中的量子状态。

（1）差错检测：执行一次测量，结果会显示什么差错将出现在量子状态上，这个测量结果叫做差错症状。对于比特翻转信道，对应于四个投影算子可有如下四种差错症状。

$$P_0\equiv|000\rangle\langle000|+|111\rangle\langle111|\textit{没有差错}$$
$$P_1\equiv|100\rangle\langle100|+|011\rangle\langle011|\textit{第一量子比特上比特翻转}$$
$$P_2\equiv|010\rangle\langle010|+|101\rangle\langle101|\textit{第二量子比特上比特翻转}$$
$$P_3\equiv|001\rangle\langle001|+|110\rangle\langle110|\textit{第三量子比特上比特翻转}$$

设举例来说，比特翻转出现在第一个量子比特，所以破坏后的状态为$a|100\rangle+b|011\rangle$。注意到在这种情况中，$\langle\psi|P_1|\psi\rangle=1$，所以测量结果的输出肯定为 1。进而，差错症状测量不会引起状态的任何改变，在差错症状测量之前和之后的状态都为$a|100\rangle+b|011\rangle$。值得注意的是，差错症状所包含的只是有关什么差错的信息，而不允许推断有关a或者b的任何信息，即它不包含所被保护状态的信息。这是差错症状测量的一个普遍特征。

（2）恢复：采用差错症状的值来了解采用什么方法来恢复初始状态。举例来说，如果差错症状为 1，指示第一个量子比特上比特翻转，则只要再一次翻转那个量子比特，就以完全准确地恢复到原状态$a|000\rangle+b|111\rangle$。这四种可能的差错症状和每种情况中的恢复方法为：0（没有差错）——什么也不用做；1（第一量子比特上比特翻转）——再一次翻转第一量子比特；2（第二量子比特翻转）——再一次翻转第二量子比特；3（第三量子比特上比特翻转）——再一次翻转第三量子比特。对于差错症状中的每个值，在给定相应所出现的差错后很容易可以看出原状态可得以完全准确的恢复。

如下图 7.3-2 译码线路图所示，译码线路实现了：

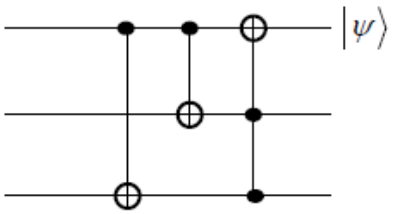


图 7.3-2 三量子比特比特翻转译码线路图

第一位错误：$\alpha|100\rangle+\beta|011\rangle\rightarrow\alpha|011\rangle+\beta|111\rangle=(\alpha|0\rangle+\beta|1\rangle)|11\rangle$

第二位错误：$\alpha|010\rangle+\beta|101\rangle\rightarrow\alpha|010\rangle+\beta|110\rangle=(\alpha|0\rangle+\beta|1\rangle)|10\rangle$

第三位错误：$\alpha|001\rangle+\beta|110\rangle\rightarrow\alpha|001\rangle+\beta|101\rangle=(\alpha|0\rangle+\beta|1\rangle)|01\rangle$

无错误：$\alpha|000\rangle+\beta|111\rangle\rightarrow\alpha|000\rangle+\beta|100\rangle=(\alpha|0\rangle+\beta|1\rangle)|00\rangle$

这种纠错方法要求：在三个量子比特出现不超过一个的比特翻转。这种情况以概率$(1-p)^3+3p(1-p)^2=1-3p^2+2p^3$出现。剩下一个差错没有纠正的概率为$3p^2-2p^3$。同之前研究的经典中的重复码相同，同样，$p<1/2$，编码和解码会改善量子状态的存储可靠性。

7.3.2 三量子比特相位翻转码

下面介绍带噪声量子信道的单量子比特的相位翻转差错模型。在该模型中，量子比特以概率$1-p$保持不变，状态$|0\rangle$和状态$|1\rangle$的相对相位以概率p被翻转。更确切的说，相位翻转算子Z以概率$p>0$作用于量子比特，所以在相位翻转下状态$a|0\rangle+b|1\rangle$变成状态$a|0\rangle-b|1\rangle$。在经典中相位翻转信道没有等价物，因为经典信道不具有任何相位的等价性质。不过，可以将相位翻转信道转化成比特翻转信道。设考虑量子比特基$|+\rangle\equiv\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$和$|-\rangle\equiv\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$。关于这个基，算子$Z$将$|+\rangle$变成$|-\rangle$。因此，使用状态$|0_L\rangle=|+++\rangle,|1_L\rangle=|---\rangle$作为逻辑 0 状态和逻辑 1 状态来解决相位翻转差错问题。这时，相位翻转纠错所需要的所有运算—编码、差错检测和恢复都同比特翻转信道中一样进行。所不同的只是，要以$|+\rangle$、$|-\rangle$来代替$|0\rangle$、$|1\rangle$。为了实现这样基的转换，只需要在纠错过程的适当位置上应用 Hadamard 门及其逆即可。

对相位翻转信道的编码可以按两步进行：第一，完全准确地对三个量子比特按比特翻转信道那样编码；第二，对每个量子比特作用 Hadamard 门。如图所示。差错检测可以通过如前相同的投影测量来达到，但要由 Hadamard 门取共轭：$P_j\rightarrow P_j'\equiv H^{\otimes3}P_jH^{\otimes3}=X_1X_2$。等价地，差错症状测量可以通过测量观测量$H^{\otimes3}Z_1Z_2H^{\otimes3}=X_1X_2$和$H^{\otimes3}Z_2Z_3H^{\otimes3}=X_2X_3$来执行。按照比特翻转码$Z_1Z_2$和$Z_2Z_3$的测量的类似思路，可对这些测量做出解释。对观测量$X_1X_2$和$X_2X_3$的测量，分别对应于比较第一和第二量子比特，以及比较第二和第三量子量子比特的正负号。其含义是，在X_1X_2的测量例如对形如$|+\rangle|+\rangle\otimes(\ \ )$或$|-\rangle|-\rangle\otimes(\ \ )$的状态给出+1，而对形如$|+\rangle|-\rangle\otimes(\ \ )$或$|-\rangle|+\rangle\otimes(\ \ )$的状态给出-1。最后纠错可以用恢复运算来完成，这种运算就是从比特翻转码导出的 Hadamard 共轭恢复运算。比如，在第一量子比特的符号中检测到了一个从$|+\rangle$到$|-\rangle$的翻转，那么就可以通过对第一量子比特作用$HX_1H=Z_1$来恢复，对其他的差错症状可以应用类似的方法。

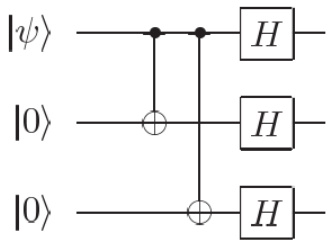


图 7.3-3 相位翻转码的编码线路

纠正相位错误的过程：

（1）作用$H^{\otimes 3}$，状态变为

$$\alpha|000\rangle+\beta|111\rangle \rightarrow \frac{1}{2\sqrt{2}}[\alpha(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle) +\beta(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)]$$

（2）送入信道，第一相位反转后，状态变为：

$$\frac{1}{2\sqrt{2}}[\alpha(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)+\beta(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)]$$

（3）作用$H^{\otimes 3}$，状态变为：$\alpha|100\rangle+\beta|011\rangle$

（4）进行译码，状态变为：$(\alpha|0\rangle+\beta|1\rangle)|11\rangle$

§7.4 Shor 码

Shor 码能针对单量子比特上的任意差错的影响进行保护。Shor 码是三量子比特相位翻转码和三量子比特比特翻转码的组合。首先用相位翻转码来编码量子比特：$|0\rangle\rightarrow|{+}{+}{+}\rangle, |1\rangle\rightarrow|{-}{-}{-}\rangle$。其次用三量子比特比特翻转码来编码这些量子比特中的每个。$|+\rangle$编码为$\frac{(|000\rangle+|111\rangle)}{\sqrt{2}}$，$|-\rangle$编码为$\frac{(|000\rangle-|111\rangle)}{\sqrt{2}}$。这个结果为 9 量子比特码，其码字为：

$$|0\rangle\rightarrow|0_L\rangle\equiv\frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}},$$
$$|1\rangle\rightarrow|1_L\rangle\equiv\frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

编码 Shor 码的量子线路如图 7.4-1 所示

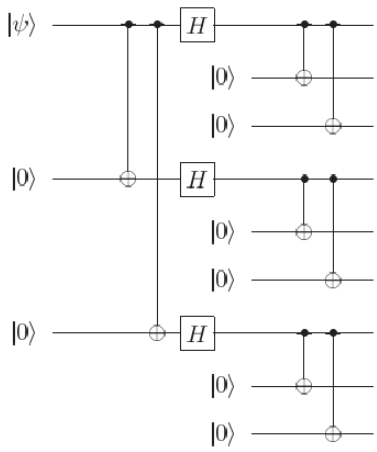


图 7.4-1 9 量子比特 Shor 码的编码线路

Shor 码能对任意量子比特上的相位翻转差错和比特翻转差错进行保护。设比特翻转出现在第一个量子比特上，就比特翻转码来说，执行对Z_1Z_2的一次测量并比较前两个量子比特，发现他们不同。基于此得出结论，比特翻转差错出现在第一或第二量子比特上。下一步，通过执行对Z_2Z_3的一次测量来比较第二和第三量子比特。若发现他们相同，则第二量子比特不可能出现翻转。据此得出结论，第一量子比特一定出现了翻转。所以，只要对第一量子比特再执行一次翻转就可以从差错中恢复，回到原来的状态。按类似的方法，就能从这个码中检测和恢复出 9 个量子比特的任意一个受比特翻转差错影响的比特。

可以使用类似的方式来处理量子比特上的相位翻转。设相位翻转出现在第一个量子比特上，这个相位翻转使得第一量子比特块中的符号翻转，变$|000\rangle + |111\rangle$为$|000\rangle - |111\rangle$。纠错过程开始于比较第一和第二量子比特块的符号。举例来说，$(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$在两个量子比特块中具有相同的符号（-），$(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)$在两个量子比特块中具有不同的符号。当相位翻转出现在前三个量子比特中任意一个上时，很容易可以发现第一和第二量子比特块的符号不同。接着进行第二和第三量子比特块的符号比较，发现这些符号相同，并得到结论在第一个三量子比特块中必有翻转。通过对第一个三量子比特块翻转符号，就能恢复到它原来的值。以类似的方式，还可以恢复 9 个量子比特中任意一个上的相位翻转。

假设比特翻转和相位翻转差错两者同时出现在第一量子比特上，也即算子Z_1X_1作用于该量子比特上。很容易可以看出，检测比特翻转差错的方法可以用来检测第一量子比特上的比特翻转并进行纠正，检测相位翻转差错的方法可以用来检测第一个三量子比特块上的相位翻转并对其进行纠正。因此，可以说，Shor 码也能用来纠正单量子比特上比特翻转和相位翻转的组合差错。

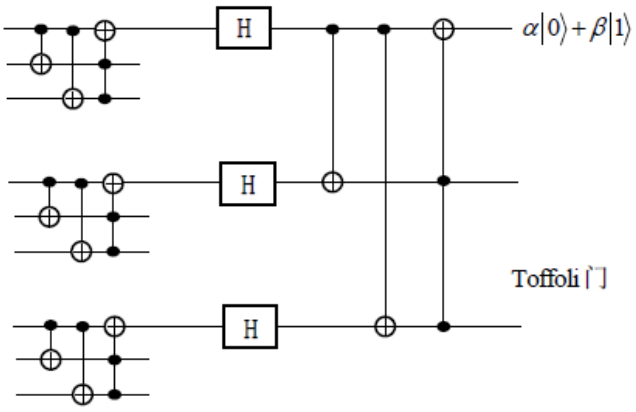


图 7.4-2 Shor 码的译码线路

§7.5Calderbank-Shor-Steane 码

量子纠错码大类中的第一个例子就是 Calderbank-Shor-Steane 码，通常更多地被称为 CSS 码。这是稳定子码的重要子类。

7.5.1 定理

定理 7.5.1：在一组基下经典线性纠错码C的所有码字的等权重叠加态，是其共轭基下C的对偶码$C^{\perp}$的所有码字的等权重叠加态。

在基$\{|0\rangle,|1\rangle\}$下码C等权重叠加$|C\rangle=\frac{1}{2^{m/2}}\sum_{v\in C}|v\rangle$

在共轭基$\{|\bar{0}\rangle，|\bar{1}\rangle\}$下，

$$\begin{aligned}|s\rangle&=H^{(n)}|C\rangle=\frac{1}{2^{m/2}}\sum_{v\in C}H^{(n)}|v\rangle\\&=\frac{1}{2^{m/2}}\sum_{v\in C}\frac{1}{2^{n/2}}\sum_{w=0}^{2^n-1}(-1)^{v\cdot w}|w\rangle\\&=\frac{1}{2^{(n+m)/2}}\sum_{w=0}^{2^n-1}\sum_{a=0}^{2^m-1}(-1)^{(aG)\cdot w}|w\rangle\end{aligned}\tag{7.5.1}$$

$$(aG)\cdot w=a(Gw^T)^T\tag{7.5.2}$$

由于G是$C^{\perp}$的校验矩阵，故知$Gw^T=\begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix}$，当且仅当$w\in C^{\perp}$。所以有

$$|s\rangle=\frac{1}{2^{\frac{(n+m)}{2}}}\sum_{w\in C^{\perp}}2^m|w\rangle=\frac{1}{2^{\frac{(n-m)}{2}}}\sum_{w\in C^{\perp}}|w\rangle\tag{7.5.3}$$

即：$|s\rangle$在共轭基下看是$C^{\perp}$中各码字的等权重叠加。

7.5.2 CSS 码构造

$C_2 \subset C_1$，C_1和C_2为线性码，C_2为C_1的K阶子码，即C_2在C_1中不同陪集的数目有2^K个.

对偶码：由校验矩阵作为生成矩阵所生成的码。维数是$n-m$。

构造 CSS 码，涉及四个经典纠错码

$$\begin{aligned} &C_2(n, m-K, \geq d_1) \subset C_1(n, m, d_1) \\ \Leftrightarrow\ &C_2^{\perp}(n, n-m+K, d_2) \supset C_1^{\perp}(n, n-m, \geq d_2) \end{aligned} \tag{7.5.4}$$

可用来编码K量子位

$$|C_w\rangle = \frac{1}{2^{(n-m)/2}} \sum_{v \in C_1^{\perp}} |w+v\rangle, w \in C_2^{\perp} \backslash C_1^{\perp} \tag{7.5.5}$$

①由于$\{|C_w\rangle\}$都是由$C_2^{\perp}$中的码字对应的量子态叠加而成，故可以纠正$\frac{1}{2}(d_2-1)$个位反转错误；只有当$w=(0,\cdots,0)$时，$|C_w\rangle$才是由$C_1^{\perp}$中元素对应的量子态叠加而成，其他情况都是$C_1^{\perp}$的某个陪集中的元素所对应的量子态叠加而成。

②由于在共轭基下$|C_w\rangle = \frac{1}{2^{m/2}} \sum_{v \in C_1} (-1)^{w \cdot v} |v\rangle$。故在共轭基下$\{|C_w\rangle\}$又可以看成是由$C_1$中码字对应的量子态叠加而成，故可纠正$\frac{1}{2}(d_1-1)$个相位反转错误。

很容易可以得到，$C_2 \subset C_1 \Rightarrow C_2^{\perp} \supset C_1^{\perp}$

证明：由$C_2 \subset C_1$知$H_1(aG_2)^T = 0$即：$H_1 G_2^T a^T = 0$ ，

由a的任意性，知$H_1 G_2^T = 0$，而$C_1^{\perp}$中码字都属于$C_2^{\perp}$，$C_1^{\perp}$是$C_2^{\perp}$的子码。

故$C_2[7,3,4] \subset C_1[7,4,3] \Leftrightarrow C_2^{\perp}[7,3,4] \supset C_1^{\perp}[7,4,3]$，当$C_2^{\perp} = C_1, C_1^{\perp} = C_2$，可纠一位错。

偶重码字对应的量子态之和为：

$$|\bar{0}\rangle = \frac{1}{2^{3/2}} \begin{pmatrix} |0000000\rangle + |0011101\rangle + |0100111\rangle + |0111010\rangle \\ +|1001110\rangle + |1010011\rangle + |1101001\rangle + |1110100\rangle \end{pmatrix} \tag{7.5.6}$$

奇重码字对应的量子态之和（做关于$w=(1111111)$的陪集）为：

$$|\bar{1}\rangle = \frac{1}{2^{3/2}} \begin{pmatrix} |1111111\rangle + |1100010\rangle + |1011000\rangle + |1000101\rangle \\ +|0110001\rangle + |0101100\rangle + |0010110\rangle + |0001011\rangle \end{pmatrix} \tag{7.5.7}$$

所以，在共轭基下有：

$$|0\rangle_L = \frac{1}{4}\left(\sum_{v \in C_1, 偶重} |v\rangle + \sum_{v \in C_1, 奇重} |v\rangle\right) \tag{7.5.8}$$

$$|1\rangle_L = \frac{1}{\sqrt{2^4}} \sum_{v \in C_1} (-1)^{w \cdot v} |v\rangle = \frac{1}{4} \sum_{v \in C_1} (-1)^{\sum_i v_i} |v\rangle = \frac{1}{4}\left(\sum_{v \in C_1, 偶重} |v\rangle - \sum_{v \in C_1, 奇重} |v\rangle\right)$$

即：$|0\rangle_L = \frac{1}{\sqrt{2}}(|\bar{0}\rangle_L + |\bar{1}\rangle_L), |1\rangle_L = \frac{1}{\sqrt{2}}(|\bar{0}\rangle_L - |\bar{1}\rangle_L)$

7.5.3 Steane 码

Steane 码的编码线路图如下图 7.5-1 所示

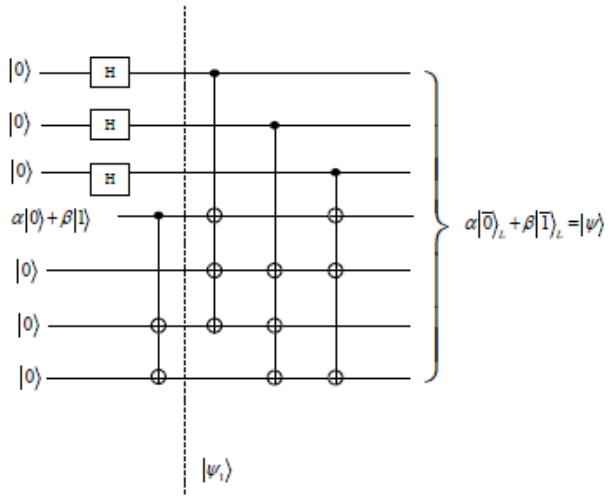


图 7.5-1 Steane 码编码线路图

编码线路原理为：

$$\begin{aligned}&|000\rangle(\alpha|0\rangle+\beta|1\rangle)|000\rangle\\&\rightarrow\frac{1}{2\sqrt{2}}\alpha|(0+1)(0+1)(0+1)0000\rangle\\&+\tfrac{1}{2\sqrt{2}}\beta|(0+1)(0+1)(0+1)1011\rangle\\&\rightarrow\alpha|\bar{0}\rangle_L+\beta|\bar{1}\rangle_L\end{aligned}\tag{7.5.9}$$

编码线路的解释：

$$\begin{aligned}|\psi\rangle&=\alpha\left|\overline{0}\right\rangle_L+\beta\left|\overline{1}\right\rangle_L\\&=\alpha\sum_{v\in C[7,3,4]}|v\rangle+\beta\sum_{v\in C[7,3,4]在C[7,4,3]中的陪集}|v\rangle\end{aligned}\tag{7.5.10}$$

因此，必须生成一个在$C[7,4,3]$中但不在$C[7,3,4]$中的码字。线路的后三列控制变换对应于

$$G[7,3,4]=\begin{bmatrix}1&0&0&1&1&1&0\\0&1&0&0&1&1&1\\0&0&1&1&1&0&1\end{bmatrix}\tag{7.5.11}$$

的三行，将态$(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)|0\rangle|0\rangle|0\rangle|0\rangle$变换为$\sum_{v\in C[7,3,4]}|v\rangle$，将态$(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)|1011\rangle$变换为

$$\sum_{v\in C[7,3,4]}|v\oplus(0001011)\rangle=\sum_{v\in C[7,3,4]在C[7,4,3]中的由0001011生成的陪集}|v\rangle\tag{7.5.12}$$

下面给出 Steane 码的译码线路图（不考虑容错问题）。

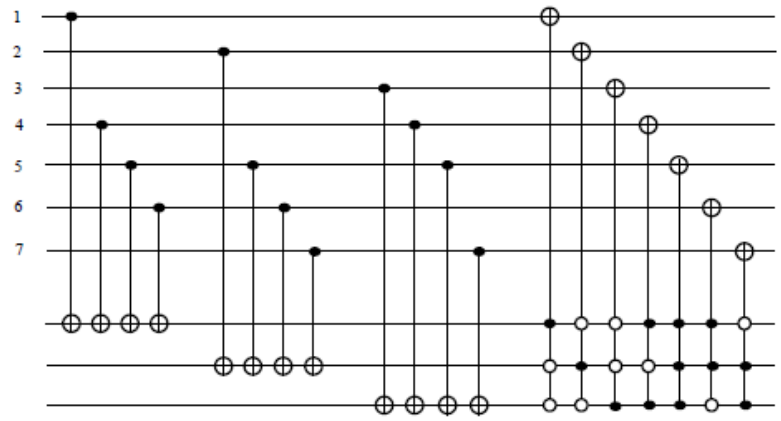


图 7.5-2 Steane 码译码线路图

具体译码过程如下：

（1） 在基$\{|0\rangle,|1\rangle\}$下，纠正比特反转错误。利用C_1码，

$$H(7,4,3)=\begin{bmatrix}1&0&0&1&1&1&0\\0&1&0&0&1&1&1\\0&0&1&1&1&0&1\end{bmatrix} \tag{7.5.13}$$

（2） 在共轭基下，纠正相位反转错误：

利用$C_2^{\perp}[7,4,3]$的$H(7,4,3)=\begin{bmatrix}1&0&0&1&1&1&0\\0&1&0&0&1&1&1\\0&0&1&1&1&0&1\end{bmatrix}$

（3） 编码线路逆用：

$$G(7,3,4)=\begin{bmatrix}1&0&0&1&1&1&0\\0&1&0&0&1&1&1\\0&0&1&1&1&0&1\end{bmatrix} \tag{7.5.14}$$

$$\begin{aligned}
&|C_w\rangle=\frac{1}{2^{(n-m)/2}}\sum_{v\in C_1^{\perp}}|w+v\rangle\\
&\rightarrow H^{(n)}|C_w\rangle=\frac{1}{2^{(n-m)/2}}\sum_{v\in C_1^{\perp}}\frac{1}{2^{n/2}}\sum_{w'=0}^{2^n-1}(-1)^{(w+v)\cdot w'}|w'\rangle\\
&=\frac{1}{2^{(n-m)/2}}\cdot\frac{1}{2^{n/2}}\sum_{w'=0}^{2^n-1}(-1)^{w\cdot w'}\sum_{a=0}^{2^{(n-m)}-1}(-1)^{(aH_1)\cdot w'}|w'\rangle\\
&=\frac{1}{2^{(n-m)/2}}\cdot\frac{1}{2^{n/2}}\cdot\sum_{w'\in C_1}(-1)^{w\cdot w'}2^{n-m}|w'\rangle\\
&=\frac{2^{\frac{(n-m)}{2}}}{2^{n/2}}\sum_{v\in C_1}(-1)^{w\cdot v}|v\rangle=\frac{1}{2^{m/2}}\sum_{v\in C_1}(-1)^{w\cdot v}|v\rangle
\end{aligned} \tag{7.5.15}$$

上式推导中利用了H_1为$C_1^{\perp}$的生成矩阵；H_1为C_1的校验矩阵；$(aH_1)\cdot w'=aH_1w'^T=a\cdot(w'H_1^T)$.

在共轭基下为：$|C_w\rangle = \frac{1}{2^{m/2}}\sum_{v\in C_1}(-1)^{w\cdot v}|v\rangle$，等概率但不是等系数。

① 当$w=0$时：

$$|C_0\rangle = \frac{1}{2^{m/2}}\sum_{v\in C_1}|v\rangle$$
$$= \frac{1}{\sqrt{2}}\left(\frac{1}{2^{(n-m)/2}}\sum_{v\in C_1,\text{偶重}}|v\rangle + \frac{1}{2^{(n-m)/2}}\sum_{v\in C_1,\text{奇重}}|v\rangle\right) \quad (7.5.16)$$

② 当$w=|1111111\rangle$时：

$$|C_w\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{2^{(n-m)/2}}\sum_{v\in C_1,\text{偶重}}|v\rangle - \frac{1}{2^{(n-m)/2}}\sum_{v\in C_1,\text{奇重}}|v\rangle\right) \quad (7.5.17)$$

§7.6 容错量子计算

7.6.1 容错量子计算的通用门组

定义 7.6.1（合法操作）一个公正操作如果能将码空间映射到自身，就称为合法操作。

定义 7.6.2（容错操作）一个合法操作如果能够通过逐位操作实现，就称为容错操作。

容错计算的意义：概率p与p^2问题，避免错误的关联。（两位同时出错概率应为p^2）

容错量子计算的通用门组表示为：$\{\bar{I},\bar{x},\bar{y},\bar{z}\}\to\{\bar{H},\bar{P},\overline{CNOT}\}$，其中$\bar{P}=\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$称为相位门（或位相门），$\{\bar{H},\bar{P},\overline{CNOT}\}$可被经典计算机有效模拟，Shor 建议添加 Toffoli 门，故通用门组为：$\{\bar{H},\bar{P},\overline{CNOT},\overline{Toff}\}$.

7.6.2 基于 Steane 码的容错量子计算

$$|0\rangle_L = \frac{1}{2^{\frac{3}{2}}}(|0000000\rangle + |0011101\rangle + |0100111\rangle + |0111010\rangle$$
$$+|1001110\rangle + |1010011\rangle + |1101001\rangle + |1110100\rangle) \quad (7.6.1)$$

$$|1\rangle_L = \frac{1}{2^{\frac{3}{2}}}(|1111111\rangle + |1100010\rangle + |1011000\rangle + |1000101\rangle$$
$$+|0110001\rangle + |0101100\rangle + |0010110\rangle + |0001011\rangle) \quad (7.6.2)$$

经过 H 转动后，有

$$|\bar{0}\rangle_L = \frac{1}{\sqrt{2}}(|0\rangle_L + |1\rangle_L),\ |\bar{1}\rangle_L = \frac{1}{\sqrt{2}}(|0\rangle_L - |1\rangle_L) \quad (7.6.3)$$

可实现的容错逻辑门：

$$\overline{NOT}:\begin{cases}|0\rangle\to|1\rangle\\ |1\rangle\to|0\rangle\end{cases}\Rightarrow\begin{cases}|\bar{0}\rangle_L\to|\bar{1}\rangle_L\\ |\bar{1}\rangle_L\to|\bar{0}\rangle_L\end{cases} \quad (7.6.4)$$

$$\bar{P}\colon P^{-1}=\begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix}=P^3=ZP \tag{7.6.5}$$

故$\bar{P}$可通过逐位执行P^{-1}实现，并且有$\begin{cases}W(|0\rangle_L)=0(mod4)\\ W(|1\rangle_L)=3(mod4)\end{cases}$，故有$\begin{cases}\bar{P}|0\rangle_L=|0\rangle_L\\ \bar{P}|1\rangle_L=i|1\rangle_L\end{cases}$.

$$\bar{H}\colon \begin{cases}|\bar{0}\rangle_L=\bar{H}|0\rangle_L\\ |\bar{1}\rangle_L=\bar{H}|1\rangle_L\end{cases}\Rightarrow\begin{cases}\bar{H}|0\rangle_L=|\bar{0}\rangle_L=\frac{1}{\sqrt{2}}(|0\rangle_L+|1\rangle_L)\\ \bar{H}|1\rangle_L=|\bar{1}\rangle_L=\frac{1}{\sqrt{2}}(|0\rangle_L-|1\rangle_L)\end{cases} \tag{7.6.6}$$

$$\overline{CNOT}\colon\begin{cases}|0\rangle_L=\dfrac{1}{2^{\frac{3}{2}}}\displaystyle\sum_{w\in c}|w\rangle\\ |1\rangle_L=\dfrac{1}{2^{\frac{3}{2}}}\displaystyle\sum_{w'\in c}|w'+a\rangle\end{cases}\Rightarrow\begin{cases}|0\rangle_L|0\rangle_L\xrightarrow{\overline{CNOT}}|0\rangle_L\dfrac{1}{2^{\frac{3}{2}}}\displaystyle\sum_{w\in c}|w+w'\rangle=|0\rangle_L|0\rangle_L\\ |0\rangle_L|1\rangle_L\xrightarrow{\overline{CNOT}}|0\rangle_L\dfrac{1}{2^{\frac{3}{2}}}\displaystyle\sum_{w'\in c}|w+w'+a\rangle=|0\rangle_L|1\rangle_L\\ |1\rangle_L|0\rangle_L\xrightarrow{\overline{CNOT}}|1\rangle_L\dfrac{1}{2^{\frac{3}{2}}}\displaystyle\sum_{w'\in c}|w+a+w'\rangle=|1\rangle_L|1\rangle_L\\ |1\rangle_L|1\rangle_L\xrightarrow{\overline{CNOT}}|1\rangle_L\dfrac{1}{2^{\frac{3}{2}}}\displaystyle\sum_{w'\in c}|w+a+w'+a\rangle=|1\rangle_L|0\rangle_L\end{cases}$$

对于$\overline{Toff}$门而言，

（1）构造辅助态

$|A\rangle=\frac{1}{2}(|000\rangle_L+|010\rangle_L+|100\rangle_L+|111\rangle_L)$，可通过$\bar{H}$使每个辅助块都处于状态$\frac{1}{\sqrt{2}}(|0\rangle_L+|1\rangle_L)$来实现，这时有$|\text{辅助块态}\rangle=\frac{1}{\sqrt{2}}(|A\rangle+|B\rangle)$，其中$|B\rangle=\frac{1}{2}(|001\rangle_L+|011\rangle_L+|101\rangle_L+|110\rangle_L)$，易见$|A\rangle=\overline{NOT}^{(3)}|B\rangle$.

另一辅助态处于猫态

$$\frac{1}{\sqrt{2}}(|0\ldots0\rangle+|1\ldots1\rangle)\triangleq\frac{1}{\sqrt{2}}(|0\rangle_c+|1\rangle_c) \tag{7.6.7}$$

对于$\frac{1}{2}(|0\rangle_c+|1\rangle_c)(|A\rangle+|B\rangle)$的每一叠加分量同时进行逻辑位操作：

$$|a_i\rangle|b_i\rangle|c_i\rangle|d_i\rangle\to(-1)^{a_i(b_ic_i+d_i)}|a_i\rangle|b_i\rangle|c_i\rangle|d_i\rangle \tag{7.6.8}$$

可得：

$$\frac{1}{2}(|0\rangle_c+|1\rangle_c)|A\rangle+\frac{1}{2}(|0\rangle_c-|1\rangle_c)|B\rangle \tag{7.6.9}$$

测量第一个辅助块处于$|0\rangle_c+|1\rangle_c$还是$|0\rangle_c-|1\rangle_c$即可知后三个辅助块处于$|A\rangle$还是$|B\rangle$.

（2）实现$\overline{Toff}$

Toffoli 的线路图为

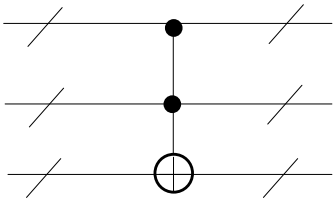


Figure 7.6-1　Toffoli 门线路图

首先，令第一辅助块对第一数据块，第二辅助块对第二数据块执行$\overline{CNOT}$，有

$$|00\rangle_L|A\rangle \to \frac{1}{2}(|00000\rangle_L + |01010\rangle_L + |10100\rangle_L + |11111\rangle_L),$$
$$|01\rangle_L|A\rangle \to \frac{1}{2}(|01000\rangle_L + |00010\rangle_L + |11100\rangle_L + |10111\rangle_L),$$
$$|10\rangle_L|A\rangle \to \frac{1}{2}(|10000\rangle_L + |11010\rangle_L + |00100\rangle_L + |01111\rangle_L),$$
$$|11\rangle_L|A\rangle \to \frac{1}{2}(|11000\rangle_L + |10010\rangle_L + |01100\rangle_L + |00111\rangle_L).$$

其次，测量第一、第二数据块，测量结果为$|00\rangle_L$则知已制备出正确的数据块，三辅助块状态与两辅助块状态的对应关系为

数据块　辅助块

$$|00\rangle_L \leftrightarrow |000\rangle_L$$
$$|01\rangle_L \leftrightarrow |010\rangle_L$$
$$|10\rangle_L \leftrightarrow |100\rangle_L$$
$$|11\rangle_L \leftrightarrow |111\rangle_L$$

测量结果为$|10\rangle_L$，得

数据块　辅助块　　辅助块

$$\left.\begin{aligned}|00\rangle_L &\leftrightarrow |010\rangle_L\\ |01\rangle_L &\leftrightarrow |000\rangle_L\\ |10\rangle_L &\leftrightarrow |111\rangle_L\\ |11\rangle_L &\leftrightarrow |100\rangle_L\end{aligned}\right\} \xrightarrow[\overline{NOT}(2)]{\overline{CNOT}(1\to 3)} \left\{\begin{aligned}&|000\rangle_L\\ &|010\rangle_L\\ &|100\rangle_L\\ &|111\rangle_L\end{aligned}\right.$$

测量结果为$|01\rangle_L$，使用$\overline{CNOT}(1\to 3), \overline{NOT}(1)$;

测量结果为$|11\rangle_L$，使用$\begin{cases}\overline{NOT}(1), \overline{NOT}(2)\\ \overline{CNOT}(1\to 3), \overline{CNOT}(2\to 3)\end{cases}$;

皆可得到$\{|000\rangle_L, |010\rangle_L, |100\rangle_L, |111\rangle_L\}$.

再次，以三辅助块为前三块，以第三数据块为第四块，执行$\overline{CNOT}(4\to 3)$和$\overline{H}(4)$，有

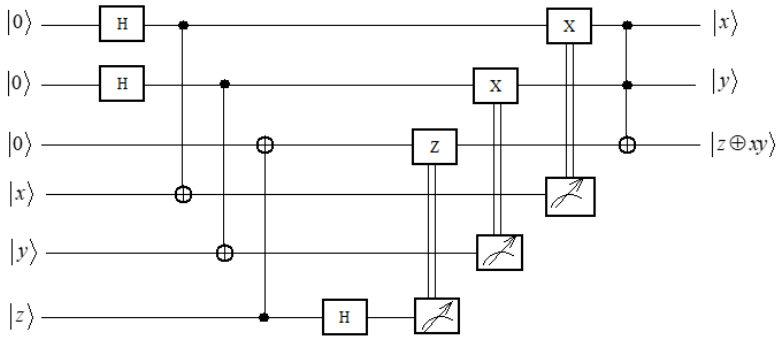
$$
\begin{aligned}
&|000\rangle_L|0\rangle_L \to |000\rangle_L|0\rangle_L \to \frac{1}{\sqrt{2}}|000\rangle_L\left(|0\rangle_L+|1\rangle_L\right)\\
&|010\rangle_L|0\rangle_L \to |010\rangle_L|0\rangle_L \to \frac{1}{\sqrt{2}}|010\rangle_L\left(|0\rangle_L+|1\rangle_L\right)\\
&|100\rangle_L|0\rangle_L \to |100\rangle_L|0\rangle_L \to \frac{1}{\sqrt{2}}|100\rangle_L\left(|0\rangle_L+|1\rangle_L\right)\\
&|111\rangle_L|0\rangle_L \to |111\rangle_L|0\rangle_L \to \frac{1}{\sqrt{2}}|111\rangle_L\left(|0\rangle_L+|1\rangle_L\right)\\
&|000\rangle_L|1\rangle_L \to |001\rangle_L|1\rangle_L \to \frac{1}{\sqrt{2}}|001\rangle_L\left(|0\rangle_L-|1\rangle_L\right)\\
&|010\rangle_L|1\rangle_L \to |011\rangle_L|1\rangle_L \to \frac{1}{\sqrt{2}}|011\rangle_L\left(|0\rangle_L-|1\rangle_L\right)\\
&|100\rangle_L|1\rangle_L \to |101\rangle_L|1\rangle_L \to \frac{1}{\sqrt{2}}|101\rangle_L\left(|0\rangle_L-|1\rangle_L\right)\\
&|111\rangle_L|1\rangle_L \to |110\rangle_L|1\rangle_L \to \frac{1}{\sqrt{2}}|110\rangle_L\left(|0\rangle_L-|1\rangle_L\right).
\end{aligned}
$$

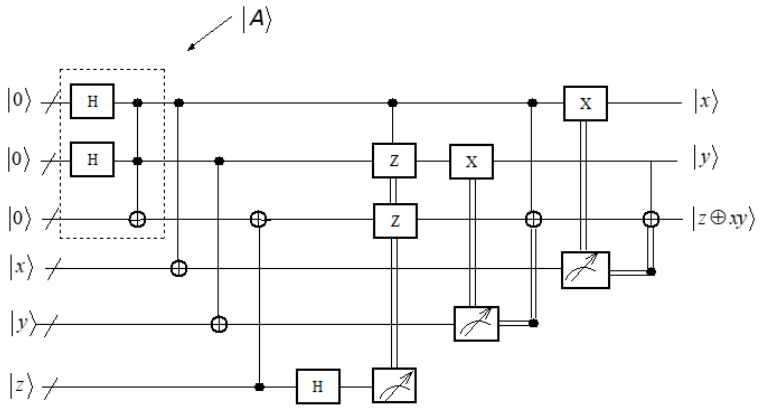
最后，测量第四块（原数据块的第三块），结果为$|0\rangle_L$，则可知三个辅助块正是三个数据块执行 Toffoli 门后的输出，结果为$|1\rangle_L$，则第三辅助块的状态与 Toffoli 门输出的第三量子位差一个相位，可通过执行下述逐位变换加以修正：

$$|a_i\rangle|b_i\rangle|c_i\rangle \to (-1)^{a_ib_i}(-1)^{c_i}|a_i\rangle|b_i\rangle|c_i\rangle \tag{7.6.10}$$

7.6.3 容错 Toffoli 门线路的构造

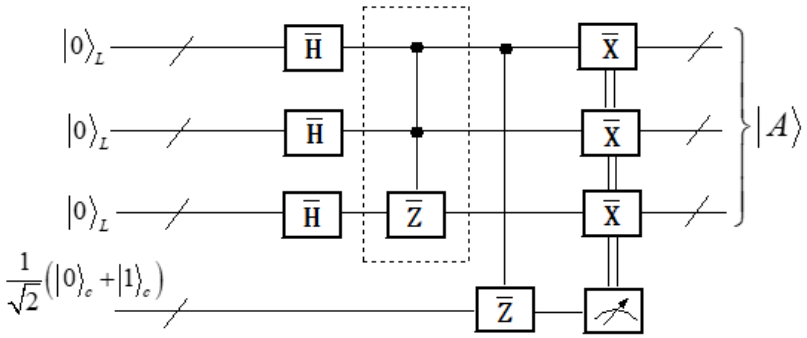
（1）构造 1





（2）构造 2

1) 辅助态$|A\rangle$的制备



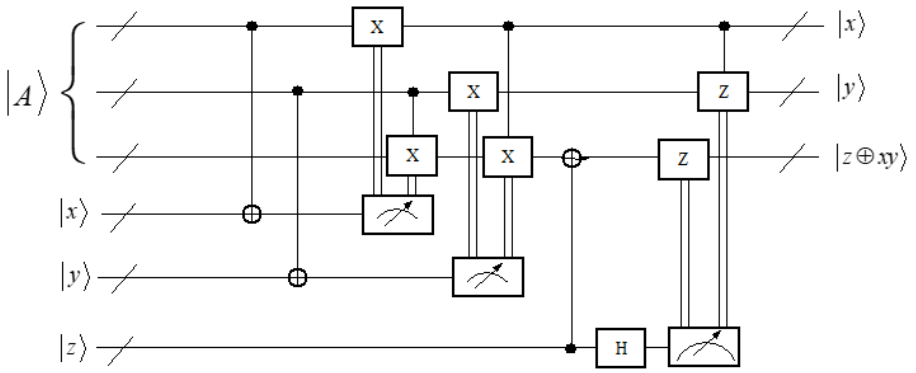
其中测量是区分两个正交态；

2) 两组条件操作的可交换性

$$\left.\begin{array}{l}|00\rangle_L \leftrightarrow |111\rangle_L\\ |01\rangle_L \leftrightarrow |100\rangle_L\\ |10\rangle_L \leftrightarrow |010\rangle_L\\ |11\rangle_L \leftrightarrow |000\rangle_L\end{array}\right\} \xrightarrow[\overline{NOT}(2)]{\overline{CNOT}(1\to 3)} \left\{\begin{array}{l}|100\rangle_L\\ |111\rangle_L\\ |000\rangle_L\\ |010\rangle_L\end{array}\right. \xrightarrow[\overline{NOT}(1)]{\overline{CNOT}(2\to 3)} \left\{\begin{array}{l}|000\rangle_L\\ |010\rangle_L\\ |100\rangle_L\\ |111\rangle_L\end{array}\right.$$

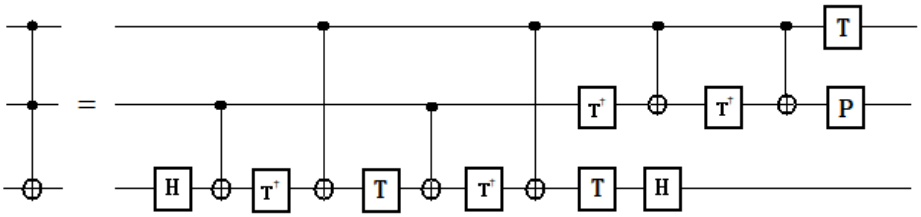
$$\left.\begin{array}{l}|00\rangle_L \leftrightarrow |111\rangle_L\\ |01\rangle_L \leftrightarrow |100\rangle_L\\ |10\rangle_L \leftrightarrow |010\rangle_L\\ |11\rangle_L \leftrightarrow |000\rangle_L\end{array}\right\} \xrightarrow[\overline{NOT}(1)]{\overline{CNOT}(2\to 3)} \left\{\begin{array}{l}|010\rangle_L\\ |000\rangle_L\\ |111\rangle_L\\ |100\rangle_L\end{array}\right. \xrightarrow[\overline{NOT}(2)]{\overline{CNOT}(1\to 3)} \left\{\begin{array}{l}|000\rangle_L\\ |010\rangle_L\\ |100\rangle_L\\ |111\rangle_L\end{array}\right.$$

3) 线路图



（3）构造 3

Toffoli 门：由 H、CNOT、P、T 门实现，共 16 个基本门操作，具体线路图如下：

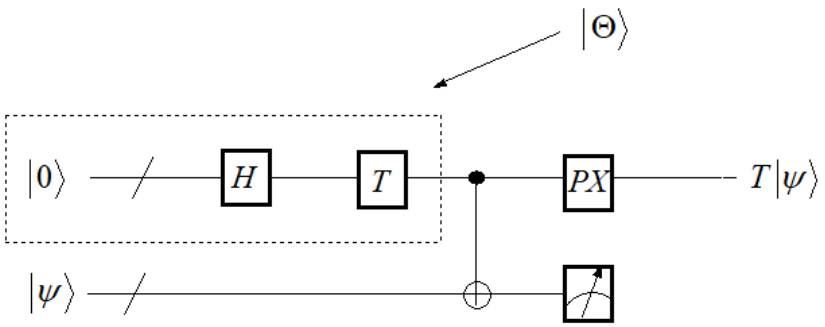


其中

$$T^{\dagger}=\begin{bmatrix}1 & 0\\ 0 & \left(e^{\frac{i\pi}{4}}\right)^{*}\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & e^{\frac{i\pi}{4}}\end{bmatrix}=T^{7}=ZPT \qquad (7.6.11)$$

如果 H、CNOT、P、T 皆可容错实现，容错 Toffoli 门即可按上述方案实现。

T 的容错实现方案：



其中$|\Theta\rangle=\frac{|0\rangle+e^{i\pi/4}|1\rangle}{\sqrt{2}}$.

第 8 章 量子信息理论基础

经典信息论主要关心通过经典信道传送经典信息。如果考虑经典信息或量子信息在量子信道中传送，会遇到新的问题。经典信息是量子态信息的特殊形式，量子信息是经典信息的拓展。因此，量子信息论是经典信息论的拓展，量子信息论在本质上比经典信息论更普适、更丰富、更深刻。

§8.1 量子操作

量子操作（quantum operation）是描述量子系统演化的工具。已经知道一个闭量子系统的演化由酉算子刻画。而开系统，即与外界环境有相互作用的系统的演化则用更一般的量子操作来刻画。一个自然的描述开量子系统演化的方法是，把演化看成是感兴趣的量子系统（称为主系统）和外界（称为环境）相互作用导致的。这个环境与主系统一起构成了闭系统。如图 8.1-1 所示，假设一开始时主系统初始处于状态ρ，环境处于状态ρ_{env}，系统-环境的状态是直积态$\rho \otimes \rho_{env}$。主系统与环境一起经过酉演化后，对环境取偏迹得到的约化后的态即为主系统的输出态。所以量子操作$\mathcal{E}$表示为:

$$\mathcal{E}(\rho) = tr_{env}[U(\rho \otimes \rho_{env})U^{\dagger}] \tag{8.1.1}$$

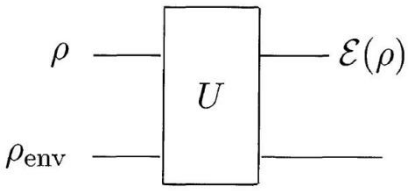


图 8.1-1 主系统与环境一起经过酉演化线路图

量子操作除了可以从与系统耦合的角度刻画，还有另一种等价的刻画，即量子操作的算子和表示。假设主系统为 Q，环境为 R，$\{e_k\}$是 R 的一组标准正交基，则：

$$\begin{aligned} \mathcal{E}(\rho) &= tr_{env}[U(\rho \otimes \rho_{env})U^{\dagger}] \\ &= \sum_k \langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^{\dagger}|e_k\rangle \\ &= \sum_k E_k \rho E_k^{\dagger} \end{aligned} \tag{8.1.2}$$

其中$E_k \equiv \langle e_k|U|e_0\rangle$为 Q 上的算子。(8.1.2)式称为量子操作的算子和表示。$\{E_k\}$称为操作元。通常要求量子操作是保迹的，即对任意的密度算子ρ，$\mathcal{E}(\rho)$的迹等于 1。

$$\begin{aligned} 1 = \ & tr(\mathcal{E}(\rho)) \\ &= tr(\textstyle\sum_k E_k \rho E_k^{\dagger}) \\ &= tr(\textstyle\sum_k E_k^{\dagger} E_k \rho) \end{aligned} \tag{8.1.3}$$

由ρ的任意性可以得到：

$$\sum_k E_k^\dagger E_k = I。 \tag{8.1.4}$$

这个等式称为算子元的完备性关系。满足这个式子的量子操作称为是保迹的。当$\sum_k E_k^\dagger E_k \le I$时称为非保迹的量子操作。算子和表示的物理解释如下：

$$\mathcal{E}(\rho) = \sum_k tr(E_k \rho E_k^\dagger) \frac{E_k \rho E_k^\dagger}{tr(E_k \rho E_k^\dagger)} \tag{8.1.5}$$

对于输入态ρ，以几率$tr(E_k \rho E_k^\dagger)$变为状态$E_k \rho E_k^\dagger / tr(E_k \rho E_k^\dagger)$例如一个十分重要的量子操作，被称为去极化信道：

$$\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z) \tag{8.1.6}$$

对于输入态ρ，以几率$(1-p)$保持不变，各以几率$\frac{p}{3}$变为$X\rho X$，$Y\rho Y$，$Z\rho Z$。

$$(R_1^\mu R_2^{1-\mu})^{1/2} (R_1^\eta R_2^{1-\eta})^{1/2} \tag{8.1.7}$$

既然量子操作具有算子和表示，一个自然的问题即是这种表示是唯一的吗？考虑作用在单量子比特上的量子操作$\mathcal{E}$、$\mathcal{F}$。算子和表示分别为$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$、$\mathcal{F}(\rho) = \sum_k F_k \rho F_k^\dagger$，其中算子元定义如下

$$\begin{aligned} E_1 &= \frac{I}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad E_2 = \frac{Z}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\ F_1 &= |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \qquad F_2 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned} \tag{8.1.8}$$

这两组操作元看起来很不同，但事实上它们所对应的量子操作是完全一样的。

$$\begin{aligned} \mathcal{F}(\rho) &= \frac{(E_1+E_2)\rho(E_1^\dagger+E_2^\dagger)+(E_1-E_2)\rho(E_1^\dagger-E_2^\dagger)}{2} \\ &= E_1 \rho E_1^\dagger + E_2 \rho E_2^\dagger \\ &= \mathcal{E}(\rho) \end{aligned} \tag{8.1.9}$$

这个例子说明量子操作的算子元不是唯一的。更一般地，有如下定理：

定理 8.1.1（算子和表示的酉自由度）假设算子元$\{E_1, \cdots, E_m\}$和$\{F_1, \cdots, F_n\}$分别对应量子操作$\mathcal{E}$、$\mathcal{F}$。通过添加适当的零算子可以使得$m = n$。则$\mathcal{E} = \mathcal{F}$当且仅当存在复数$u_{ij}$使得$E_i = \sum_j u_{ij} F_j$，$u_{ij}$是$m \times m$酉阵的矩阵元。

证明若$\sum_i E_i \rho E_i^\dagger = \sum_j F_j \rho F_j^\dagger$，引入系统 R 和 Q，R 的维数与 Q 相等。$\{i_R\}$，$\{i_Q\}$分别为 R 和 Q 的一组标准正交基。定义：

$$\begin{aligned} |e_i\rangle &\equiv \sum_k |k_R\rangle (E_i |k_Q\rangle) \\ |f_j\rangle &\equiv \sum_k |k_R\rangle (F_j |k_Q\rangle) \end{aligned} \tag{8.1.10}$$

并且令$|\alpha\rangle = \sum_k |k_R\rangle |k_Q\rangle$，简单计算有：

$$\begin{aligned}\sum_i |e_i\rangle\langle e_i| &= (I\otimes\mathcal{E})(|\alpha\rangle\langle\alpha|)\\ &= (I\otimes\mathcal{F})(|\alpha\rangle\langle\alpha|)\\ &= \sum_j |e_j\rangle\langle e_j|\end{aligned} \tag{8.1.11}$$

又存在酉阵u_{ij}满足：

$$|e_i\rangle = \sum_j u_{ij}\,|f_j\rangle \tag{8.1.12}$$

对任意的态$|\psi\rangle = \sum_k a_k\,|k_Q\rangle$，定义$|\widetilde{\psi}\rangle \equiv \sum_k a_k^*\,|k_R\rangle$，则有：

$$\begin{aligned}E_i|\psi\rangle &= \langle\widetilde{\psi}\,|e_i\rangle\\ &= \sum u_{ij}\langle\widetilde{\psi}\,|f_j\rangle\\ &= \sum_j u_{ij}\,F_j|\psi\rangle\end{aligned} \tag{8.1.13}$$

因此$E_i = \sum_j u_{ij}\,F_j$，从而定理的必要性得证。

定理的充分性证明比较容易，将作为习题留给读者证明。

§8.2 迹距离与保真度

8.2.1 迹距离

本节要介绍的迹距离和保真度是用于刻画两个量子态有多接近的度量工具。这一小节主要讨论迹距离的定义及性质。而在此之前，了解经典信息中相似的距离度量是很有必要的。

在经典信息中，信息源通常被建模为随机变量，也即某个源字母表上的概率分布。因此比较两个信息源，往往是比较两个概率分布。设$\{p_x\}$和$\{q_x\}$是具有相同指标集x的两个概率分布，它们的迹距离定义为：

$$D(p_x, q_x) \equiv \frac{1}{2}\sum_x |\,p_x - q_x| \tag{8.2.1}$$

迹距离也被称为L_1距离或 Kolmogorov 距离。

概率分布的另一种度量工具是保真度。概率分布$\{p_x\}$和$\{q_x\}$的保真度被定义为：

$$F(p_x, q_x) \equiv \sum_x \sqrt{p_x q_x} \tag{8.2.2}$$

若定义向量$\sqrt{p} \equiv (\sqrt{p_1},\cdots,\sqrt{p_n}),\sqrt{q} \equiv (\sqrt{q_1},\cdots,\sqrt{q_n})$，则有$|\sqrt{p}|^2 = 1$，$|\sqrt{q}|^2 = 1$，且：

$$\sqrt{p}\cdot\sqrt{q} = \sum_x \sqrt{p_x q_x} = F(p_x, q_x)。 \tag{8.2.3}$$

现在定义两个量子态的迹距离，经典迹距离定义中度量的是概率分布的距离，在量子信息中，则用密度算子代替概率分布。两个量子态ρ和σ之间的迹距离定义为：

$$D(\rho,\sigma) \equiv \frac{1}{2}tr|\rho-\sigma|。 \tag{8.2.4}$$

其中运算$|\cdot|$定义为$|A| \equiv \sqrt{A^\dagger A}$。

迹距离具有许多重要的性质。首先会看到当两个密度算子ρ和σ对易时，量子的迹距离将退化为经典的迹距离。由于ρ与σ对易，所以它们可同时谱分解，即存在标准正交的态矢$\{|i\rangle\}$使得：

$$\rho = \sum_i r_i |i\rangle\langle i| \qquad \sigma = \sum_i s_i |i\rangle\langle i| \tag{8.2.5}$$

直接计算有$D(\rho,\sigma) = \frac{1}{2}tr|\sum_i (r_i - s_i)|i\rangle\langle i|| = \frac{1}{2}tr(\sum_i |r_i - s_i|) = \frac{1}{2}\sum_i |r_i - s_i|$.

迹距离的一个很好的性质是，它在酉作用下是不变的：

$$D\left(U\rho U^\dagger, U\sigma U^\dagger\right) = D(\rho,\sigma). \tag{8.2.6}$$

利用对任意的半正定算子 A 和酉算子 U，$\sqrt{UAU^\dagger} = U\sqrt{A}U^\dagger$直接按照定义即可证明上式（留作习题）。

下面定理给出迹距离的另一种等价刻画，这种刻画省去了$|\cdot|$运算，因此在许多时候用起来更加方便。

定理 8.2.1 设ρ、σ为密度算子，则迹距离：

$$D(\rho,\sigma) = \max_P tr(P(\rho - \sigma)) \tag{8.2.7}$$

其中等式右边是在所有可能的投影算子 P 上取极大。

证明$\rho - \sigma$是厄米算子，所以有谱分解$\rho - \sigma = \sum_i d_i |i\rangle\langle i|$，其中

$$d_i = \begin{cases} \lambda_i & i \le \alpha \\ -\lambda_i & i \ge \alpha + 1 \end{cases} \tag{8.2.8}$$

λ_i为非负实数。对$i \le \alpha$，取$q_i = \lambda_i, s_i = 0$；对$i > \alpha$，取$q_i = 0, s_i = \lambda_i$。令$Q = \sum_i q_i |i\rangle\langle i|$，$S = \sum_i s_i |i\rangle\langle i|$。则有：

$$\begin{aligned} |\rho - \sigma| &= |Q - S| \\ &= \sum_i |\lambda_i||i\rangle\langle i| \\ &= \sum_i q_i |i\rangle\langle i| + \sum_i s_i |i\rangle\langle i| \\ &= Q + S \end{aligned} \tag{8.2.9}$$

所以：

$$D(\rho,\sigma) = \frac{1}{2}tr|\rho - \sigma| = \frac{1}{2}tr(Q + S) \tag{8.2.10}$$

由因为$trQ - trS = tr(Q - S) = tr(\rho - \sigma) = tr\rho - tr\sigma = 0$，所以$trQ = trS$。因此，有$D(\rho,\sigma) = trQ$。设 P 是任意的投影算子，则：

$$\begin{aligned} tr(P(\rho - \sigma)) &= tr(P(Q - S)) \\ &\le tr(PQ) \\ &\le tr(Q) \\ &= D(\rho,\sigma) \end{aligned} \tag{8.2.11}$$

显然当取 P 为到 Q 的支集上的投影时，$tr(P(\rho - \sigma)) = D(\rho,\sigma)$。于是定理得证。

下面定理给出迹距离的另一种等价刻画，它将量子迹距离与经典迹距离密切地联系起来。

定理 8.2.2 令$\{E_m\}$为一个 POVM，且$p_m = tr(\rho E_m)$和$q_m = tr(\sigma E_m)$分别为状态ρ和σ测量输出 m 的几率。则有：

$$D(\rho,\sigma) = \max_{\{E_m\}} D(p_m, q_m) \tag{8.2.12}$$

其中极大是对所有的 POVM$\{E_m\}$取的。

证明利用谱分解可以得到具有正交支集的半正定算子 Q、S，满足$\rho - \sigma = Q - S$，且$|\rho - \sigma| = Q + S$。由经典的迹距离的定义：

$$D(p_m, q_m) = \frac{1}{2}\sum_m |\, tr(E_m(\rho - \sigma))| \tag{8.2.13}$$

又：

$$\begin{aligned} |tr(E_m(\rho-\sigma))| &= |tr(E_m(Q-S))| \\ &\le tr(E_m(Q+S)) \\ &\le tr(E_m|\rho-\sigma|) \end{aligned} \tag{8.2.14}$$

从而

$$\begin{aligned} D(p_m, q_m) &\le \frac{1}{2}\sum_m t\, r(E_m|\rho-\sigma|) \\ &= \frac{1}{2} tr(|\rho-\sigma|) \\ &= D(\rho,\sigma) \end{aligned} \tag{8.2.15}$$

由上面推导可看出，当取 POVM 使得 POVM 元包含到 Q 和 S 的支集的投影时，$D(p_m, q_m) = D(\rho,\sigma)$。于是定理得证。

该定理说明量子的迹距离以经典的迹距离为上界。若在量子的情况下不能区分两个态，则从经典的角度更不能区分。迹距离的这两个等价刻画，有时比直接按迹距离的定义使用起来更方便。例如证明迹距离满足三角不等式：

$$D(\rho,\tau) \le D(\rho,\sigma) + D(\sigma,\tau) \tag{8.2.16}$$

易知存在投影算子 P，使得:

$$\begin{aligned} D(\rho,\tau) &= tr(P(\rho-\tau)) \\ &= tr[P(\rho-\sigma)] + tr[P(\sigma-\tau)] \\ &\le D(\rho,\sigma) + D(\sigma,\tau) \end{aligned} \tag{8.2.17}$$

从而得到了迹距离的三角不等式。

已经知道迹距离在酉算子作用下是不变的，那么它在更一般的量子操作作用下仍是不变的吗？下面定理说明，在保迹量子操作下迹距离是不增的。

定理 8.2.3 假设$\mathcal{E}$是保迹量子操作，ρ和σ是密度算子，则：

$$D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \le D(\rho,\sigma) \tag{8.2.18}$$

证明设$\mathcal{E}$的操作元是$\{E_k\}$，利用谱分解可以得到具有正交支集的半正定算子 Q、S，满足$\rho-\sigma=Q-S$，且$|\rho-\sigma|=Q+S$。存在投影算子 P，使得$D(\mathcal{E}(\rho),\mathcal{E}(\sigma))=tr[P(\mathcal{E}\rho-\mathcal{E}(\sigma))]$。因为$trQ=trS$，且

$$\begin{aligned} tr(\mathcal{E}(Q)) &= tr(\textstyle\sum_k E_k\, Q E_k^{\dagger}) \\ &= \textstyle\sum_k t\, r(E_k Q E_k^{\dagger}) \\ &= \textstyle\sum_k t\, r(E_k^{\dagger} E_k Q) \\ &= tr(\textstyle\sum_k E_k^{\dagger}\, E_k Q) \\ &= trQ \end{aligned} \tag{8.2.19}$$

所以$tr(\mathcal{E}(Q))=tr(\mathcal{E}(S))$。于是：

$$\begin{aligned} D(\rho,\sigma) &= \tfrac{1}{2} tr|\rho-\sigma| \\ &= \tfrac{1}{2} tr|Q-S| \\ &\tfrac{1}{2} tr(Q)+\tfrac{1}{2} tr(S) \\ &= \tfrac{1}{2} tr(\mathcal{E}(Q))+\tfrac{1}{2} tr(\mathcal{E}(S)) \\ &= tr(\mathcal{E}(Q)) \\ &\geq tr(P\mathcal{E}(Q)) \\ &\geq tr(P(\mathcal{E}(Q)-\mathcal{E}(S))) \\ &= tr(P(\mathcal{E}(\rho)-\mathcal{E}(\sigma))) \\ &= D(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \end{aligned} \tag{8.2.20}$$

从而定理得证。

由于偏迹是一种量子操作，且对量子态取偏迹后迹距离不增。即若ρ^{AB}和σ^{AB}是复合系统 AB 的两个量子态，$\rho^A=tr_B(\rho^{AB})$，$\sigma^A=tr_B(\sigma^{AB})$，则

$$D(\rho^A,\sigma^A)\leq D(\rho^{AB},\sigma^{AB}) \tag{8.2.21}$$

当把两个物体的一部分遮起来，将使得这两个物体更难区分。在这一小节的最后，证明迹距离的强凸性。

定理 8.2.4（迹距离的强凸性）设$\{p_i\}$和$\{q_i\}$是具有相同指标集的概率分布，ρ_i和σ_i是密度算子，则

$$D(\textstyle\sum_i p_i\,\rho_i,\sum_i q_i\,\sigma_i)\leq D(p_i,q_i)+\sum_i p_i\, D(\rho_1,\sigma_i) \tag{8.2.22}$$

其中$D(p_i,q_i)$是概率分布$\{p_i\}$和$\{q_i\}$的经典迹距离。

证明存在投影算子 P 使得

$$\begin{aligned} D\left(\sum_i p_i\,\rho_i,\sum_i q_i\,\sigma_i\right) &= \sum_i p_i\, tr(P\rho_i)-\sum_i q_i\, tr(P\sigma_i) \\ &= \sum_i p_i\, tr(P(\rho_i-\sigma_i))+\sum_i (p_i-q_i) tr(P\sigma_i) \end{aligned}$$

$$\leq \sum_i p_i D(\rho_i, \sigma_i) + \sum_i (p_i - q_i) tr(P\sigma_i)$$

又因为

$$\begin{aligned} \sum_i (p_i - q_i) tr(P\sigma_i) &\leq \sum_{i|p_i>q_i} (p_i - q_i) tr(P\sigma_i) \\ &\leq \sum_{i|p_i>q_i} (p_i - q_i) \\ &= \frac{1}{2} \sum_i |p_i - q_i| \\ &= D(p_i, q_i) \end{aligned} \tag{8.2.23}$$

综上，得到：

$$D(\sum_i p_i \rho_i, \sum_i q_i \sigma_i) \leq D(p_i, q_i) + \sum_i p_i D(\rho_1, \sigma_i) \tag{8.2.24}$$

推论 8.2.1（联合凸）迹距离是联合凸的，即：

$$D(\sum_i p_i \rho_i, \sum_i p_i \sigma_i) \leq D \sum_i p_i D(\rho_1, \sigma_i) \tag{8.2.25}$$

8.2.2 保真度

在这一小节中，讨论量子态的保真度及相关的性质。量子态ρ和σ的保真度定义如下：

$$F(\rho, \sigma) \equiv tr\sqrt{\rho^{1/2} \sigma \rho^{1/2}} \tag{8.2.26}$$

保真度具有许多和迹距离相似的性质。例如，当ρ和σ对易时，量子保真度将退化为经典的保真度。具体地，ρ和σ对易，则它们可同时对角化，设：

$$\rho = \sum_i r_i |i\rangle\langle i|; \qquad \sigma = \sum_i s_i |i\rangle\langle i| \tag{8.2.27}$$

于是

$$\begin{aligned} F(\rho, \sigma) &= tr\sqrt{\sum_i r_i s_i |i\rangle\langle i|} \\ &= tr(\sum_i \sqrt{r_i s_i} |i\rangle\langle i|) \\ &= \sum_i \sqrt{r_i s_i} \\ &= F(r_i, s_i) \end{aligned} \tag{8.2.28}$$

另一种特殊情况是，当两个量子态之一是纯态。此时

$$\begin{aligned} F(|\psi\rangle, \rho) &= tr\sqrt{\langle\psi|\rho|\psi\rangle |\psi\rangle\langle\psi|} \\ &= \sqrt{\langle\psi|\rho|\psi\rangle} \end{aligned} \tag{8.2.29}$$

所以保真度等于算子ρ在态$|\psi\rangle$下均值的平方根。

保真度在酉变换下同样是不变的。即对酉算子 U，密度算子ρ和σ有：

$$F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma) \tag{8.2.30}$$

上式的推导比较容易，读者可自己进行验证。下面定理给出了保真度的一个十分重要的等价刻画：

定理 8.2.5（Uhlmann 定理）假设ρ和σ是量子系统 Q 的密度算子，引入第二个量子系统 R，与 Q 具有相同的维数，则：

$$F(\rho,\sigma)=\max_{|\psi\rangle,|\varphi\rangle}|\langle\psi|\varphi\rangle| \tag{8.2.31}$$

其中极大是对ρ和σ在系统 RQ 的所有纯化态$|\psi\rangle$、$|\varphi\rangle$取的。

在证明 Uhlmann 定理之前，先要证明一个引理：

引理 8.2.1 设 A 为任意算子，U 是酉算子，则

$$|tr(AU)|\le tr|A| \tag{8.2.32}$$

设 A 有极式分解$A=|A|V$，当取$U=V^{\dagger}$时等号成立。

注意这里的$|A|=\sqrt{AA^{\dagger}}$。

Hilbert-Schmit 内积是定义在作用于 Hilbert 空间的算子空间上的二元运算：

$$<A,B>\equiv tr(A^{\dagger}B) \tag{8.2.33}$$

实质是一种内积，于是利用内积的 Cauchy-Schwarz 不等式有：

$$\begin{aligned}|tr(AU)| &= |tr(|A|VU)|\\ &= |tr(|A|^{1/2}|A|^{1/2}VU)|\\ &\le \sqrt{tr(|A|^{1/2}|A|^{1/2})tr(U^{\dagger}V^{\dagger}|A|^{1/2}|A|^{1/2}VU)}\\ &= tr|A|\end{aligned} \tag{8.2.34}$$

现在证明 Uhlmann 定理。

证明设$|i_Q\rangle$和$|i_R\rangle$分别是 Q 和 R 的标准正交基，令$|m\rangle\equiv\sum_i|i_R\rangle|i_Q\rangle$。简单计算可知，对 R 和 Q 上的任意算子 A 和 B 有：

$$tr(A^{\dagger}B)=\langle m|A^{*}\otimes B|m\rangle \tag{8.2.35}$$

设$|\psi\rangle$是ρ的任意纯化，$|\varphi\rangle$是σ的任意纯化。说明必存在酉算子U_R和U_Q使得

$$|\psi\rangle=(U_R\otimes\sqrt{\rho}U_Q)|m\rangle \tag{8.2.36}$$

这是因为，由 Schmit 分解，存在正交的态矢$|i_R'\rangle$、$|i_Q'\rangle$满足：

$$|\psi\rangle=\sum_i\lambda_i|i_R'\rangle|i_Q'\rangle \tag{8.2.37}$$

其中$\lambda_i\ge 0$，所以$\rho=\rho^{Q}=\sum_i\lambda_i^2|i_Q'\rangle\langle i_Q'|$。由于$|i_Q'\rangle$、$|i_R'\rangle$分别可扩为一组基，所以存在酉算子$U_R$、$U_Q$使得：

$$U_Q|i_Q\rangle\to|i_Q'\rangle\qquad U_R|i_R\rangle\to|i_R'\rangle \tag{8.2.38}$$

于是：

$$\begin{aligned}(U_R \otimes \sqrt{\rho}U_Q)|m\rangle &= \sum_i U_R\,|i_R\rangle \otimes \sqrt{\rho}U_Q|i_Q\rangle \\ &= \sum_i |\,i_R{}'\rangle(\sum_j \lambda_j\,|j_Q{}'\rangle\langle j_Q{}'|)|i_Q{}'\rangle \\ &= \sum_i \lambda_i\,|i_R{}'\rangle\langle j_Q{}'|)|i_R{}'\rangle \\ &= \sum_i \lambda_i\,|i_R{}'\rangle|i_Q{}'\rangle \\ &= |\psi\rangle\end{aligned} \tag{8.2.39}$$

同理，存在酉算子V_R和V_Q满足：

$$|\psi\rangle = (V_R \otimes \sqrt{\sigma}V_Q)|m\rangle \tag{8.2.40}$$

故：

$$\begin{aligned}|\langle\psi|\varphi\rangle| &= |\langle m|(U_R^\dagger V_R \otimes U_Q^\dagger\sqrt{\rho}\sqrt{\sigma}V_Q)|m\rangle| \\ &= |tr(V_R^T U_R^* U_Q^\dagger\sqrt{\rho}\sqrt{\sigma}V_Q)|\end{aligned} \tag{8.2.41}$$

令$U \equiv V_Q V_R^\dagger U_R U_Q^\dagger$，则：

$$|\langle\psi|\varphi\rangle| = |tr(\sqrt{\rho}\sqrt{\sigma}U)| \tag{8.2.42}$$

由引理 8.2.1 可得

$$|\langle\psi|\varphi\rangle| \le tr|\sqrt{\rho}\sqrt{\sigma}| = tr\sqrt{\rho^{1/2}\sigma\rho^{1/2}} \tag{8.2.43}$$

假设$\sqrt{\rho}\sqrt{\sigma} = |\sqrt{\rho}\sqrt{\sigma}|V$为$\sqrt{\rho}\sqrt{\sigma}$的极式分解，则令$U_Q = U_R = V_R = I$，$V_R = V^\dagger$即可取到等号。

利用 Uhlmann 定理可以证明保真度的许多重要性质，其中就包括保真度的强凹性。

定理 8.2.6（保真度的强凸性）设p_i和q_i是具有相同指标集的概率分布，ρ_i和σ_i为密度算子，则

$$F(\sum_i p_i\,\rho_i, \sum_i q_i\,\sigma_i) \ge \sum_i \sqrt{p_i q_i}\,F(\rho_i, \sigma_i) \tag{8.2.44}$$

证明由 Uhlmann 定理存在$|\psi_i\rangle$和$|\varphi_i\rangle$为ρ_i和σ_i的纯化，满足$F(\rho_i, \sigma_i) = \langle\psi_i|\varphi_i\rangle$。引入具有标正基$|i\rangle$的辅助系统。定义：

$$|\psi]\rangle \equiv \sum_i \sqrt{p_i}\,|\psi_i\rangle|i\rangle \qquad |\varphi\rangle \equiv \sum_i \sqrt{q_i}\,|\varphi\rangle|i\rangle \tag{8.2.45}$$

于是$|\psi\rangle$是$\sum_i p_i\,\rho_i$的纯化，$|\varphi\rangle$是$\sum_i q_i\,\sigma_i$的纯化，所以由 Uhlmann 定理：

$$\begin{aligned}F(\sum_i p_i\,\rho_i, \sum_i q_i\sigma_i) &\ge |\langle\psi|\varphi\rangle| \\ &= \sum_i \sqrt{p_i q_i}\,\langle\psi_i|\varphi\rangle \\ &= \sum_i \sqrt{p_i q_i}\,F(\rho_i, \sigma_i)\end{aligned} \tag{8.2.46}$$

从而定理得证。

8.2.3 迹距离与保真度的关系

尽管迹距离与保真度在形式上看起来很不相同，但它们却有密切的关系。具体地有如下定理：

定理 8.2.7 设ρ和σ为密度算子，则

$$1-F(\rho,\sigma)\le D(\rho,\sigma)\le\sqrt{1-F(\rho,\sigma)^2} \tag{8.2.47}$$

证明先证明$D(\rho,\sigma)\le\sqrt{1-F(\rho,\sigma)^2}$。先考虑$\rho$和$\sigma$都是纯态的情况：设$\rho=|a\rangle\langle a|$，$\sigma=|b\rangle\langle b|$。利用 Gram-Schmitdt 过程可以找到正交归一的态矢$|0\rangle$、$|1\rangle$使得$|a\rangle=|0\rangle$，$|b\rangle=\cos\theta|0\rangle+\sin\theta|1\rangle$。直接计算得$F(|a\rangle,|b\rangle)=|\cos\theta|$且：

$$\begin{aligned} D(|a\rangle,|b\rangle) &= \tfrac{1}{2}tr\left|\begin{bmatrix}1-\cos^2\theta & -\cos\theta\sin\theta\\ -\cos\theta\sin\theta & -\sin^2\theta\end{bmatrix}\right| \\ &= |\sin\theta| \\ &= \sqrt{1-F(|a\rangle,|b\rangle)^2}\end{aligned} \tag{8.2.48}$$

对于更一般的情况，ρ和σ为两个任意的量子态。根据 Ulmann 定理，存在它们的纯化态$|\psi\rangle$和$|\varphi\rangle$满足$F(\rho,\sigma)=|\langle\psi|\varphi\rangle|$。所以：

$$F(\rho,\sigma)=|\langle\psi|\varphi\rangle|=F(|\psi\rangle,|\varphi\rangle) \tag{8.2.49}$$

于是：

$$\begin{aligned} D(\rho,\sigma) &\le D(|\psi\rangle,|\varphi\rangle) \\ &= \sqrt{1-F(|\psi\rangle,|\varphi\rangle)^2} \\ &= \sqrt{1-F(\rho,\sigma)^2}\end{aligned} \tag{8.2.50}$$

现证$1-F(\rho,\sigma)\le D(\rho,\sigma)$。令$\{E_m\}$为一个 POVM，满足$F(\rho,\sigma)=\sum_m\sqrt{p_m q_m}$，其中$p_m\equiv tr(\rho E_m)$和$q_m\equiv tr(\sigma E_m)$分别为状态$\rho$和$\sigma$可得结果 m 的概率。于是：

$$\begin{aligned} \sum_m(\sqrt{p_m}-\sqrt{q_m})^2 &= \sum_m p_m+\sum_m q_m-2F(\rho,\sigma) \\ &= 2(1-F(\rho,\sigma))\end{aligned} \tag{8.2.51}$$

另一方面：

$$\begin{aligned} \sum_m(\sqrt{p_m}-\sqrt{q_m})^2 &\le \sum_m|\sqrt{p_m}-\sqrt{q_m}||\sqrt{p_m}+\sqrt{q_m}| \\ &= \sum_m|p_m-q_m| \\ &= 2D(p_m,q_m) \\ &\le 2D(\rho,\sigma)\end{aligned} \tag{8.2.52}$$

故可得$1-F(\rho,\sigma)\le D(\rho,\sigma)$。于是定理得证。

§8.3Von Neumann 熵

8.3.1Shannon 熵

在这一小节中，先学习经典的熵概念。Shannon 熵定义为概率分布的函数。设$p_1,\cdots,p_n$是概率分布，它的 Shannon 熵定义为：

$$H(X)\equiv H(p_1,\cdots,p_n)\equiv-\sum_x p_x\log p_x。 \tag{8.3.1}$$

当$p_x = 0$时，约定$0\log 0 \equiv 0$。Shannon 熵度量在知道随机变量 X 的取值前它所具有的不确定度，或者是在知道 X 的值后所能得到的信息。一个很有用的工具是相对熵。设$p(x)$和$q(x)$是具有相同指标 x 的两个概率分布，$p(x)$对$q(x)$的相对熵定义为：

$$H(p(x) \parallel q(x)) \equiv \sum_x p\,(x)\log\frac{p(x)}{q(x)} = -H(X) - \sum_x p\,(x)\log q(x)。\quad（8.3.2）$$

相对熵可以被看成是刻画两个概率分布之间的距离。下面的定理说明相对熵是非负的。

定理 8.3.1（相对熵的非负性）相对熵是非负的，即$H(p(x) \parallel q(x)) \geq 0$, 等号成立当且仅当对所有的$x$有$p(x) = q(x)$。

证明证明要用到不等式$\log x \ln 2 = \ln x \leq x - 1$，该不等式对所以大于零的$x$成立，且等号成立当且仅当$x = 1$。改写不等式可以得到$-\log x \geq (1 - x)/\ln 2$，于是：

$$\begin{aligned} H(p(x) \parallel q(x)) \quad &= -\sum_x p\,(x)\log\frac{q(x)}{p(x)} \\ &\geq \frac{1}{\ln 2}\sum_x p\,(x)\left(1 - \frac{q(x)}{p(x)}\right) \\ &= \frac{1}{\ln 2}\sum_x (p(x) - q(x)) \\ &\frac{1}{\ln 2}(1 - 1) = 0 \end{aligned} \quad（8.3.3）$$

等号成立当且仅当$q(x)/p(x) = 1$对所有的x成立，也即$p(x)$和$q(x)$是两个相同的分布。于是定理得证。

相对熵可以用于证明 Shannon 熵的许多性质，例如给出 Shannon 熵的上界：

定理 8.3.2 设 X 是共有 d 个取值的随机变量，则$H(X) \leq \log d$，等号成立当且仅当 X 是 d 个取值上的均匀分布。

证明假设 X 的分布为$p(x)$，取$q(x) \equiv 1/d$为相同取值集合上的均匀分布，则：

$$\begin{aligned} H(p(x) \parallel q(x)) \quad &= H(p(x) \parallel 1/d) \\ &= -H(X) - \sum_x p\,(x)\log(1/d) \\ &= \log d - H(X) \end{aligned} \quad（8.3.4）$$

所以$H(X) \leq \log d$，等号成立当且仅当$p(x) = q(x) = 1/d$，即 X 是均匀分布。

接下来介绍两个概念——相对熵和互信息，它们在某种程度上都反映了两个随机变量之间的相关度。在此之前，一个很自然的概念是联合熵。

定义 8.3.1（联合熵）设 X 和 Y 是两个随机变量，它们的联合分布为$p(x, y)$。X 和 Y 的联合熵定义:

$$H(X, Y) \equiv -\sum_{x,y} p\,(x, y)\log p(x, y) \quad（8.3.5）$$

联合熵度量随机变量对(X, Y)总体的不确定度。

定义 8.3.2（条件熵）已知 Y 的下 X 的条件熵定义为：

$$H(X|Y) \equiv H(X, Y) - H(Y) \quad（8.3.6）$$

条件熵度量在已知 Y 的情况下 X 的不确定度。

定义 8.3.3（互信息）X 和 Y 的互信息定义为：

$$H(X:Y) \equiv H(X) + H(Y) - H(X,Y) \tag{8.3.7}$$

互信息度量有多少的公共信息。

利用条件熵的定义有$H(X:Y) = H(X) - H(X|Y)$

Shannon 熵的许多性质都有比较直观地理解，下面定理就列出了其中一部分，这些性质可概括为 Shannon 熵的文氏图（图 8.3-1）。

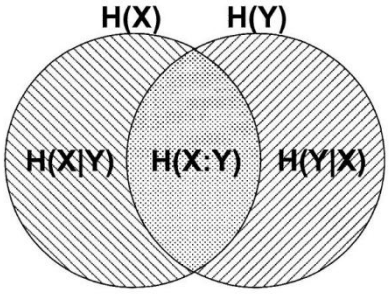


图 8.3-1 Shannon 熵的文氏图

定理 8.3.3（Shannon 熵的基本性质）

(1)$H(X,Y) = H(Y,X), H(X:Y) = H(Y:X)$；

(2)$H(Y|X) \geq 0$，因此$H(x:y) \leq H(y)$，等号成立当且仅当Y是X的函数，$Y = F(X)$；

(3)$H(x) \leq H(X,Y)$，等号成立当且仅当 Y 是 X 的函数；

(4)次可加性：$H(X,Y) \leq H(X) + H(Y)$，等号成立当且仅当 X 与 Y 是独立的随机变量；

(5)$H(Y|X) \leq H(Y)$，因此$H(X:Y) \geq 0$，等号成立当且仅当 X 和 Y 是独立的随机变量；

(6)强次可加性：$H(X,Y,Z) + H(Y) \leq H(X,Y) + H(Y,Z)$，等号成立当且仅当$Z \to Y \to X$构成 Markov 链。

(7)条件减少熵：$H(X|Y,Z) \leq H(X|Y)$。

证明

(1)由定义的对称性可得；

(2)由于$p(x,y) = p(x)p(y|x)$，则：

$$\begin{aligned} H(X,Y) &= -\sum_{x,y} p\,(x,y)\log p(x)p(y|x) \\ &= -\sum_{x} p\,(x)\log p(x) - \sum_{x,y} p\,(x,y)\log p(y|x) \\ &= H(X) - \sum_{x,y} p\,(x,y)\log p(y|x). \end{aligned} \tag{8.3.8}$$

因此$H(Y|X)=-\sum_{xy}p\,(x,y)\log p(y|x)$。由于$-\log p(y|x)\geq 0$，所以$H(Y|X)\geq 0$，等号成立当且仅当 Y 是 X 的确定函数。

(3)由(2)的结论易得。

(4)再次利用不等式$\log x\leq (x-1)/\ln 2$，等号成立当且仅当$x=1$。注意到：

$$\begin{aligned}\sum_{xy}p\,(x,y)\log\frac{p(x)p(y)}{p(x,y)} &\leq \frac{1}{\ln 2}\sum_{x,y}p\,(x,y)\left(\frac{p(x)p(y)}{p(x,y)}-1\right)\\ &=\frac{1}{\ln 2}\sum_{x,y}\left(p(x)p(y)-p(x,y)\right)\\ &=\frac{1-1}{\ln 2}\\ &=0\end{aligned}\qquad (8.3.9)$$

从而得到次可加性。等号成立当且仅当$p(x,y)=p(x)p(y)$对所有的 x 和 y 成立，即 X 与 Y 是独立的随机变量。

(5)由次可加性和条件熵的定义即得。

(6)与次可加性的证明方法类似。注意到：

$$\begin{aligned}&H(X,Y,Z)+H(Y)-H(X,Y)-H(Y,Z)\\ &=-\sum_{xyz}\log p(x,y,z)-\sum_{y}p\,(y)\log p(y)+\sum_{yz}p\,(yz)\log p(y,z)+\sum_{xy}p\,(x,y)\log p(x,y)\\ &=\sum_{xyz}[\log p(y,z)+\log p(x,y)-\log p(y)-\log p(x,y,z)]\\ &=\sum_{xuz}p\,(xyz)\log\frac{p(x,y)p(y,z)}{p(y)p(x,y,z)}\\ &\leq\frac{1}{\ln 2}\sum_{xyz}p\,(x,y,z)\left(\frac{p(x,y)p(y,z)}{p(y)p(x,y,z)}-1\right)\\ &=\frac{1}{\ln 2})\left(\sum_{yz}\frac{p(y)p(y,z)}{p(y)}-1\right)\\ &=0\end{aligned}$$

等号成立当且仅当对任意的x,y,z有$p(x,y)p(y,z)=p(y)p(x,y,z)$，即$p(x|yz)=p(x|y)$对所有$x,y,z$成立，即$Z\to Y\to X$构成 Markov 链。

(7)将不等式改写得到：

$$H(X,Y,Z)-H(Y,Z)\leq H(X,Y)-H(Y),\qquad (8.3.10)$$

由强次可加性知成立。

8.3.2 Von Neumann 熵定义与性质

Shannon 熵度量经典随机变量的不确定度，是概率分布的函数。对应到量子的情况，量子态相当于是经典中的随机变量，其密度算子代替经典的概率分布。现在给出量子态的熵的概念。一个量子态的 Von Neumann 熵定义为：

$$S(\rho) \equiv -tr(\rho \log \rho)。 \tag{8.3.11}$$

若密度算子ρ的本征值标记为λ_x，则：

$$S(\rho) = -\sum_x \lambda_x \log \lambda_x, \tag{8.3.12}$$

这个公式更便于计算。由此公式立刻可得 d 维空间的完全混合态I/d的熵为$\log d$。

与 Shannon 相对熵相似，可以定义量子的相对熵。

定义 8.3.4（量子相对熵）假设ρ和σ是密度算子，ρ对σ的相对熵定义为：

$$S(\rho \parallel \sigma) \equiv tr(\rho \log \rho) - tr(\rho \log \sigma) \tag{8.3.13}$$

与经典的相对熵一样，量子的相对熵也是非负的。有如下定理：

定理 8.3.4（Klein 不等式）量子相对熵是非负的，

$$S(\rho \parallel \sigma) \geq 0, \tag{8.3.14}$$

等号成立当且仅当$\rho = \sigma$.

证明设ρ与σ的谱分解分别为$\rho = \sum_i p_i |i\rangle\langle i|$，$\sigma = \sum_j q_j |j\rangle\langle j|$。由相对熵的定义有：

$$S(\rho \parallel \sigma) = \sum_i p_i \log p_i - \sum_i \langle i|\rho \log \sigma|i\rangle。 \tag{8.3.15}$$

注意到$\langle i|\rho = p_i\langle i|$及

$$\langle i|\log \sigma|i\rangle = \langle i|(\sum_j \log(q_j)|j\rangle\langle j|)|i\rangle = \sum_j \log(q_j) P_{ij}, \tag{8.3.16}$$

其中$P_{ij} \equiv \langle i|j\rangle\langle j|i\rangle \geq 0$。从而：

$$S(\rho \parallel \sigma) = \sum_i p_i (\log p_i - \sum_j P_{ij} \log(q_j))。 \tag{8.3.17}$$

令$r_i \equiv \sum_j P_{ij} q_j$。由于$\sum_i P_{ij} = 1$，$\sum_j P_{ij} = 1$及$\log(\cdot)$的严格凹性，有$\sum_j P_{ij} \log q_j \leq \log r_i$，等号成立当且仅当存在一个 j 使得$P_{ij} = 1$。因此

$$S(\rho \parallel \sigma) \geq \sum_i p_i \log \frac{p_i}{r_i}, \tag{8.3.18}$$

等号成立当且仅当对每个 i 存在一个 j 满足$P_{ij}=1$，也即P_{ij}是一个置换矩阵。上式右端是一个经典熵，由经典熵的非负性得：

$$S(\rho \parallel \sigma) \geq 0。 \tag{8.3.19}$$

等号成立当且仅当对任意 i，$p_i = r_i$且P_{ij}是置换矩阵。也即$\rho = \sigma$。

假设密度算子ρ在很小的范围内变化，相应的熵$S(\rho)$如何变化呢？下面的定理说明熵相对于密度算子具有“连续性”。当密度算子变化不大时，熵也变化不大。

定理 8.3.5（Fannes 不等式）假设ρ与σ是密度算子，它们之间的迹距离满足$T(\rho,\sigma) \leq 1/e$（$T(\rho,\sigma) = 2D(\rho,\sigma)$）。则

$$|S(\rho) - S(\sigma)| \leq T(\rho,\sigma)\log d + \eta(T(\rho,\sigma)), \tag{8.3.20}$$

其中 d 为 Hilbert 空间的维数，$\eta(x) \equiv -x\log x$。

证明

设ρ和σ的本征值分别为$r_1,\cdots,r_d$和$s_1,\cdots,s_d$，且$r_1 \geq r_2 \cdots \geq r_d$，$s_1 \geq s_2 \cdots \geq s_d$，可以构造具有正交支集的半正定算子$Q$和$R$使得$\rho = \sigma = Q - R$。于是有$T(\rho,\sigma) = tr(R) + tr(Q)$。令

$$V \equiv R + \rho = Q + \sigma, \tag{8.3.21}$$

从而$T(\rho,\sigma) = tr(R) + tr(Q) = tr(2V) - tr(\rho) - tr(\sigma)$。设$t_1 \geq t_2 \cdots \geq t_d$为 T 的本征值，由于$t_i \geq \max(r_i, s_i)$，所以$2t_i \geq r_i + s_i + |r_i - s_i|$，于是有：

$$T(\rho,\sigma) \geq \sum_i |r_i - s_i|。 \tag{8.3.22}$$

根据函数η的性质知道当$|r-s| < 1/2$时，$|\eta(r) - \eta(s)| \leq \eta(|r-s|)$（作为习题）。而$|r_i - s_i| \leq 1/2$对所有 i 成立，所以：

$$|S(\rho) - S(\sigma)| = |\sum_i (\eta(r_i) - \eta(s_i))| \leq \sum_i \eta(|r_i - s_i|)。 \tag{8.3.23}$$

令$\Delta \equiv \sum_i |r_i - s_i|$，则：

$$|S(\rho) - S(\sigma)| \leq \Delta \sum \eta(|r_i - s_i|/\Delta) + \eta(\Delta) \leq \Delta \log d + \eta(\Delta),$$

易知$\Delta \leq T(\rho,\sigma)$，所以由$\eta$在$[0,1/e]$内的单调性知：

$$|S(\rho) - S(\sigma)| \leq T(\rho,\sigma)\log d + \eta(T(\rho,\sigma)), \tag{8.3.24}$$

从而定理得证。

Von Neumann 熵有许多有用的性质，下面定理列出了其中的一部分。

定理 8.3.6（Von Neumann 熵的基本性质）

(1)Von Neumann 熵是非负的，熵等于零当且仅当态是纯态;

(2)d 为 Hilbert 空间的熵至多为$\log d$，取到$\log d$当且仅当系统处于完全混合态I/d;

(3)若复合系统 AB 是一个纯态，则$S(A)=S(B)$;

(4)假设p_i是概率分布，态ρ_i有正交的支集。则

$$S(\sum_i p_i\,\rho_i)=H(p_i)+\sum_i p_i\,S(\rho_i); \tag{8.3.25}$$

(5)可加性：ρ和σ分别为系统 A，B 的密度算子，则

$$S(\rho\otimes\sigma)=S(\rho)+S(\sigma); \tag{8.3.26}$$

(6)联合熵定理：假设p_i是概率分布，$|i\rangle$是系统 A 的正交态，ρ_i是系统 B 的密度算子集合。则

$$S(\sum_i p_i\,|i\rangle\langle i|\otimes\rho_i)=H(p_i)+\sum_i p_i\,S(\rho_i)。 \tag{8.3.27}$$

证明

(1)由定义即得;

(2)有 Klein 不等式，$0\le S(\rho\parallel I/d)=-S(\rho)+\log d$;

(3)由 Schmidt 分解知 A 与 B 的密度算子具有相同的本征值，而熵完全由本征值确定，所以$S(A)=S(B)$;

(4)设λ_i^j和$|e_i^j\rangle$是ρ_i的本征矢和相应的本征值，则$p_i\lambda_i^j$和$|e_i^j$是$\sum_i p_i\,\rho_i$的本征矢和本征值。因此：

$$\begin{aligned} S(\sum_i p_i\,\rho_i) &= -\sum_{ij} p_i\,\lambda_i^j\log(p_i\lambda_i^j)\\ &= -\sum_i p_i\log p_i-\sum_i p_i\sum_j\lambda_i^j\log\lambda_i^j\\ &= H(p_i)+\sum_i p_i\,S(\rho_i)\end{aligned} \tag{8.3.28}$$

从而证明了等式。

(5)设ρ与σ的谱分解分别为$\rho=\sum_i\lambda_i\,|i\rangle\langle i|$，$\sigma=\sum_j\mu_j\,|j\rangle\langle j|$。注意到：

$$\begin{aligned}\rho\otimes\sigma &= \sum\lambda_i\mu_j|i\rangle\langle i|\otimes|j\rangle\langle j|\\ &= \sum_{ij}\lambda_i\,\mu_j(|i\rangle\otimes|j\rangle)(\langle i|\otimes\langle j|)\end{aligned} \tag{8.3.29}$$

所以$\lambda_i\mu_j$是$\rho\otimes\sigma$的本征值。因此：

$$S(\rho\otimes\sigma)=-\sum_{ij}\lambda_i\,\mu_j\log(\lambda_i\mu_j)=S(\rho)+S(\sigma); \tag{8.3.30}$$

(6)注意到：

$$
\begin{aligned}
& S(\sum_i p_i |i\rangle\langle i| \otimes \rho_i) \\
&= H(p_i) + \sum_i p_i S(|i\rangle\langle i| \otimes \rho_i) \\
&= H(p_i) + \sum_i p_i \left(S(|i\rangle\langle i|) + S(\rho_i)\right) \\
&= H(p_i) + \sum_i p_i S(\rho_i),
\end{aligned}
\tag{8.3.31}
$$

从而证明了结论。

当对量子态ρ进行测量时，它的熵会如何变化呢？假设对量子系统进行投影测量，相应的正交投影算子即为P_i，且在测量后不得到测量的结果。则测后态为：

$$
\rho' = \sum_i P_i \rho P_i 。 \tag{8.3.32}
$$

下面定理说明这一过程绝不会减少体系的熵，且熵保持不变当且仅当侧后的态与侧前相同。

定理 8.3.7 假设P_i是完备的正交投影算子，ρ是密度算子。则系统的测后态$\rho' \equiv \sum_i P_i \rho P_i$的熵大于等于原来的熵，

$$
S(\rho') \geq S(\rho), \tag{8.3.33}
$$

等号成立当且仅当$\rho = \rho'$。

证明由 Klein 不等式有：

$$
0 \leq S(\rho' \parallel \rho) = -S(\rho) - tr(\rho \log \rho'), \tag{8.3.34}
$$

所以只需证明$-tr(\rho \log \rho') = S(\rho')$。注意到$\rho' P_i = P_i \rho P_i = P_i \rho'$，即$\rho'$与$P_i$可交换，从而$\log \rho'$与$P_i$可交换。又$\sum_i P_i = I$，$P_i^2 = P_i$，所以：

$$
\begin{aligned}
-tr(\rho \log \rho') &= -tr(\textstyle\sum_i P_i \rho \log \rho') \\
&= -tr(\textstyle\sum_i P_i \rho \log \rho' P_i) \\
&= -tr(\textstyle\sum_i P_i \rho P_i \log \rho') \\
&= -tr(\rho' \log \rho') \\
&= S(\rho')
\end{aligned}
\tag{8.3.35}
$$

于是定理得证。

与 Shannon 熵类似，可以定义量子的联合熵和条件熵。设复合系统 AB 的密度算子为ρ^{AB}，则联合熵定义为

$$
S(A,B) \equiv -tr(\rho^{AB} \log(\rho^{AB}))。 \tag{8.3.36}
$$

条件熵和互信息则分别定义如下：

$$
\begin{aligned}
S(A|B) &\equiv S(A,B) - S(B) \\
S(A:B) &\equiv S(A) + S(B) - S(A,B) \\
&= S(A) - S(A|B) = S(B) - S(B|A)
\end{aligned}
\tag{8.3.37}
$$

Shanno 熵的许多性质对 VonNeumann 熵仍然成立，但有的却不成立。例如，当对 Shannon 熵有$H(X) \leq H(X,Y)$成立。且对 Shannon 熵，条件熵都为非负的。这两条对 Von Neumann 熵不成立。考虑两个量子比特的复合系统 AB，处于纠缠态$(|00\rangle + |11\rangle)/\sqrt{2}$。AB

处于纯态，所以 S(A,B)=0。系统 A 的密度算子则为$I/2$，所以$S(A)=1$。由此可见，$S(A,B)\leq S(A)$。另一方面，$S(B|A)=S(A,B)-S(A)$为负的，说明了对 Von Neumann 熵，条件熵有可能为负的。

最后，证明熵的两个重要性质，分别为熵的次可加性和联合凹性。

定理 8.3.8 假设不同的量子系统 A 和 B 具有联合态ρ^{AB}。则两个系统的联合熵满足：

$$\begin{aligned} S(A,B)&\leq S(A)+S(B),\\ S(A,B)&\geq |S(A)-S(B)|。\end{aligned} \tag{8.3.38}$$

其中第一个不等式称为 Von Nuemann 熵的次可加性不等式，等号成立当且仅当 A 与 B 是不相关的，即$\rho^{AB}=\rho^{A}\otimes\rho^{B}$，第二个称为三角不等式。

证明由 Klein 不等式知$S(\rho)\leq -tr(\rho\log\sigma)$。令$\rho\equiv\rho^{AB}$，$\sigma\equiv\rho^{A}\otimes\rho^{B}$，则

$$\begin{aligned} -tr(\rho\log\sigma) &= -tr(\rho^{AB}(\log\rho^{A}+\log\rho^{B}))\\ &= -tr(\rho^{A}\log\rho^{A})-tr(\rho^{B}\log\rho^{B})\\ &= S(A)+S(B)。\end{aligned} \tag{8.3.39}$$

于是得到$S(A,B)\leq S(A)+S(B)$。等号成立当且仅当$\rho=\sigma$，即$\rho^{AB}=\rho^{A}\otimes\rho^{B}$。

为证明三角不等式，引入系统 R 使得系统 ABR 处于纯态。由次可加性得：

$$S(R)+S(A)\geq S(A,R)。 \tag{8.3.40}$$

由于 ABR 处于纯态，$S(A,R)=S(B)$，$S(R)=S(A,B)$。于是有

$$S(A,B)\geq S(B)-S(A), \tag{8.3.41}$$

同理可以得到

$$S(A,B)\geq S(A)-S(B)。 \tag{8.3.42}$$

从而定理得证。

与 Shannon 熵类似，量子熵具有严格凹性。具体有如下定理：

定理 8.3.9 设p_i为密度分布，ρ_i为密度算子，则 Von Neumann 熵满足：

$$S(\textstyle\sum_i p_i\,\rho_i)\geq\sum_i p_i\,S(\rho_i), \tag{8.3.43}$$

等号成立当且仅当对所有$p_i>0$的 i 对于的ρ_i都相同。

证明直观地来看，量子态$\sum_i p_i\,\rho_i$表示系统以概率p_i处于状态ρ_i。对整个混合态的不确定度应该高于每个ρ_i的不确定度的平均。这是因为态$\sum_i p_i\,\rho_i$不仅包含了对态ρ_i的未知，也包含了对指标 i 的未知。

假设ρ_i是系统 A 的态，引进辅助系统 B，B 的态空间有对应指标 i 的标准正交基$|i\rangle$。定义 AB 上的联合态:

$$\rho^{AB}\equiv\textstyle\sum_i p_i\,\rho_i\otimes|i\rangle\langle i| \tag{8.3.44}$$

注意到

$$\begin{aligned} S(A) &= S(\textstyle\sum_i p_i \rho_i) \\ S(B) &= S(\textstyle\sum_i p_i |i\rangle\langle i|) = H(p_i) \\ S(A,B) &= H(p_i) + \textstyle\sum_i p_i S(\rho_i) \end{aligned} \tag{8.3.45}$$

有熵的次可加性$S(A,B) \le S(A) + S(B)$得：

$$\textstyle\sum_i p_i S(\rho_i) \le S(\sum_i p_i \rho_i) \tag{8.3.46}$$

显然等号成立当且仅当对所以大于零的p_i，相应的ρ_i都相同。

8.3.3 强次可加性

强次可加性是次可加性对三系统量子体系的扩展，它是量子信息理论中十分重要和有用的结果。强次可加性的证明过程比较复杂，但学习定理的证明过程对巩固量子信息的知识很有帮助。

强次可加性的证明要用到 Lieb 定理。在证明 Lieb 定理之前，需补充一些基本概念。假设$f(A,B)$是两个矩阵 A，B 的实值函数，则 f 称为关于 A，B 联合凹的，若对任意的$o \le \lambda \le 1$，有：

$$f(\lambda A_1 + (1-\lambda)A_2, \lambda B_1 + (1-\lambda)B_2) \ge \lambda f(A_1,B_1) + (1-\lambda) f(A_2,B_2). \tag{8.3.47}$$

对矩阵 A、B，若 B-A 是半正定阵，记为$A \le B$。对任意一个矩阵 A 定义范数：

$$\| A \| \equiv \max_{\langle u|u\rangle} |\langle u|A|u\rangle| 。 \tag{8.3.48}$$

若 A 有本征值λ_i，λ是$|\lambda_i|$的最大值，则$\| A \| \ge \lambda$。且当 A 为厄米阵时，$\| A \| = \lambda$（证明留作习题）。

假设 A 是半正定阵，可以定义超算子：

$$\mathcal{A}(X) \equiv AX \tag{8.3.49}$$

显然$\mathcal{A}$是线性的。可以证明这样定义的超算子在$Hilbert - Schmidt$内积下是半正定的，即对任意的 X，有$tr(X^\dagger \mathcal{A}(X)) \ge 0$。可类似的定义超算子$\mathcal{A}(X) \equiv XA$。有了这些基本概念，我可以证明 Lieb 定理：

定理 8.3.10（Lieb 定理）设 X 为矩阵，$0 \le t \le 1$，则函数

$$f(A,B) \equiv tr(X^\dagger A^t X B^{1-t}) \tag{8.3.50}$$

关于半正定阵 A，B 是联合凹的。

Lieb 定理的证明基于如下引理：

引理 8.3.1 设$R_1, R_2, S_1, S_2, T_1, T_2$是半正定算子，满足$0 = [R_1, R_2] = [S_1, S_2] = [T_1 . T_2]$，且：

$$\begin{aligned} R_1 &\ge S_1 + T_1 \\ R_2 &\ge S_2 + T_2, \end{aligned} \tag{8.3.51}$$

则对任意的$0 \le t \le 1$，有：

$$R_1^t R_2^{1-t} \ge S_1^t S_2^{1-t} + T_1^t T_2^{1-t}. \tag{8.3.52}$$

证明先证明结论对$t = 1/2$成立。假设R_1和R_2是可逆的，对不可逆的情况只需对证明过程作微小的修改。

这$|x\rangle$和$|y\rangle$是两个向量，利用两次$Cauchy - Schwarz$不等式有：

$$\begin{aligned} & |\langle x|(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})|y\rangle| \\ \le\ & |\langle x|S_1^{1/2}S_2^{1/2}|y\rangle| + |\langle x|T_1^{1/2}T_2^{1/2}|y\rangle| \\ \le\ & \| S_1^{1/2}|x\rangle \| \| S_2^{1/2}|y\rangle \| + \| T_1^{1/2}|x\rangle \| \| T_2^{1/2}|y\rangle \| \\ \le\ & \sqrt{(\| S_1^{1/2}|x\rangle \|^2 + \| T_1^{1/2}|x\rangle \|^2)(\| S_2^{1/2}|y\rangle \|^2 + \| T_2^{1/2}|y\rangle \|^2)} \\ =\ & \sqrt{\langle x|(S_1+T_1)|x\rangle\langle y|(S_2+T_2)|y\rangle}. \end{aligned} \tag{8.3.53}$$

由条件知$S_1 + T_1 \le R_1$，$S_2 + T_2 \le R_2$，所以

$$|\langle x|(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})|y\rangle| \le \sqrt{\langle x|R_1|x\rangle\langle y|R_2|y\rangle}. \tag{8.3.54}$$

设$|u\rangle$是任意的单位向量，将$|x\rangle \equiv R_1^{-1/2}|u\rangle$、$|y\rangle \equiv R_2^{-1/2}|u\rangle$代入式(8.3.54)得：

$$\begin{aligned} & \langle u|R_1^{-1/2}(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})R_2^{-1/2}|u\rangle \\ \le\ & \sqrt{\langle u|R_1^{-1/2}R_1R_1^{-1/2}|u\rangle\langle u|R_2^{-1/2}R_2R_2^{-1/2}|u\rangle} \\ =\ & \sqrt{\langle u|u\rangle\langle u|u\rangle} \\ =\ & 1. \end{aligned} \tag{8.3.55}$$

因此，

$$\| R_1^{-1/2}(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})R_2^{-1/2} \| \le 1. \tag{8.3.56}$$

令，

$$\begin{aligned} A\ & \equiv R_1^{-1/4}r_2^{-1/4}(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})R_2^{-1/2} \\ B\ & \equiv R_2^{1/4}R_1^{-1/4} \end{aligned} \tag{8.3.57}$$

由于 AB 是厄米的，所以

$$\begin{aligned} & \| R_1^{-1/4}R_2^{-1/4}(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})R_2^{-1/4}R_1^{-1/4} \| \\ =\ & \| AB \| \le \| BA \| \\ =\ & \| R_1^{-1/2}(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})r_2^{-1/2} \| \\ \le\ & 1 \end{aligned} \tag{8.3.58}$$

由于 AB 是正定阵，所以

$$R_1^{-1/4}R_2^{-1/4}(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})R_2^{-1/4}R_1^{-1/4} \le I。 \tag{8.3.59}$$

从而

$$S_1^{1/2}S_2^{1/2}+T_1^{1/2}T_2^{1/2}\le R_1^{1/2}R_2^{1/2}。\tag{8.3.60}$$

证明了对$t=1/2$不等式成立，下证对任意的$0\le t\le 1$都成立。

设 I 是所有满足不等式的 t 的集合，假设μ和η是 I 中的任意两个元素，则

$$\begin{aligned}R_1^{\mu}R_2^{1-\mu}&\ge S_1^{\mu}S_2^{1-\mu}+T_1^{\mu}T_2^{1-\mu}\\ R_1^{\eta}R_2^{1-\eta}&\ge S_1^{\eta}S_2^{1-\eta}+T_1^{\eta}T_2^{1-\eta}。\end{aligned}\tag{8.3.61}$$

它们具有条件(3.129)和(3.220)的形式，利用$t=\frac{1}{2}$的结果可以得到

$$(R_1^{\mu}R_2^{1-\mu})^{1/2}(R_1^{\eta}R_2^{1-\eta})^{1/2}\ge(S_1^{\mu}S_2^{1-\mu})^{1/2}(S_1^{\eta}S_2^{1-\eta})^{1/2}+(T_1^{\mu}T_2^{1-\mu})^{1/2}(T_1^{\eta}T_2^{1-\eta})^{1/2}\tag{8.3.62}$$

从而对$\nu\equiv(\mu+\eta)/2$，

$$R_1^{\nu}R_2^{1-\nu}\ge S_1^{\nu}S_2^{1-\nu}+T_1^{\nu}T_2^{1-\nu}。\tag{8.3.63}$$

所以只要μ和η属于I，则$(\mu+\eta)/2$就属于I。由于 0、1 和$1/2$属于 I，所以所有在 0 和 1 之间有有限二元表示的 t 都属于 I，所以 I 在[0,1]稠密，又由 t 得连续性结论得证。

现证明 Lieb 定理：

Lieb 定理证明设$0\le\lambda\le 1$，定义超算子$\mathcal{S}_1,\mathcal{S}_2,\mathcal{T}_1,\mathcal{T}_2,\mathcal{R}_1,\mathcal{R}_2$如下：

$$\begin{aligned}\mathcal{S}_1(X)&\equiv\lambda A_1X\\ \mathcal{S}_2(X)&\equiv\lambda XB_1\\ \mathcal{T}_1(X)&\equiv(1-\lambda)A_2X\\ \mathcal{T}_2(X)&\equiv(1-\lambda)XB_2\\ \mathcal{R}_1&\equiv\mathcal{S}_1+\mathcal{T}_1\\ \mathcal{R}_1&\equiv\mathcal{S}_1+\mathcal{T}_1\end{aligned}\tag{8.3.64}$$

显然$\mathcal{S}_1$与$\mathcal{S}_2$可交换，$\mathcal{T}_1$与$\mathcal{T}_2$可交换，$\mathcal{R}_1$与$\mathcal{R}_2$可交换。这些算子关于 Hilbert-Schmidt 内积可交换。由引理 3.3.1

$$\mathcal{R}_1^t\mathcal{R}_2^{1-t}\ge\mathcal{S}_1^t\mathcal{S}_2^{1-t}+\mathcal{T}_1^t\mathcal{T}_2^{1-t}。\tag{8.3.65}$$

等式两边同时作用到 X 在与 X 内积得到：

$$\begin{aligned}tr[X^{\dagger}(\lambda\quad&A_1+(1-\lambda)A_2)^tX(\lambda B_1+(1-\lambda)B_2)^{1-t}]\\ &\ge tr[X^{\dagger}(\lambda A_1)^tX(\lambda B_1)^{1-t}]+tr[X^{\dagger}((1-\lambda)A_2)^tX((1-\lambda)B_2)^{1-t}]\\ &=\lambda tr(X^{\dagger}A_1^tXB_1^{1-t})+(1-\lambda)tr(X^{\dagger}A_2^tXB_2^{1-t})\end{aligned}\tag{8.3.66}$$

从而定理得证。

利用 Lieb 定理，可以得到一系列有趣的结论，最终证明强次可加性，由相对熵的凸性开始。

定理 8.3.11（相对熵的联合凸性）相对熵$S(\rho\parallel\sigma)$对它的输入时联合凸的。

证明设 A 和 X 是作用在相同空间上的任意矩阵，定义：

$$I_t(A,X) \equiv tr(X^\dagger A^t X A^{1-t}) - tr(X^\dagger X A)。 \tag{8.3.67}$$

由 Lieb 定理，右边第一项关于 A 是凹的，第二项关于 A 线性。所以$I_t(A,X)$关于 A 是凹的。定义：

$$\begin{aligned} I(A,X) &\equiv \frac{d}{dt}|_{t=0} I_t(A,X) \\ &= tr(X^\dagger (\ln A) X A) - tr(X^\dagger X (\ln A) A). \end{aligned} \tag{8.3.68}$$

注意到$I_0(A,X) = 0$且利用$I_t(A,X)$关于 A 的凹性有：

$$\begin{aligned} I(\lambda A_1 + (1-\lambda)A_2, X) &= \lim_{\Delta\to 0} \frac{I_\Delta(\lambda A_1 + (1-\lambda)A_2, X)}{\Delta} \\ &\geq \lambda \lim_{\Delta\to 0} \frac{I_\Delta(A_1,X)}{\Delta} + (1-\lambda)\lim_{\Delta\to 0}\frac{I_\Delta(A_2,X)}{\Delta} \\ &= \lambda I(A_1,X) + (1-\lambda) I(A_2,X). \end{aligned} \tag{8.3.69}$$

因此，$I(A,X)$是 A 的凹函数。定义分块矩阵

$$A \equiv \begin{bmatrix} \rho & 0 \\ 0 & \sigma \end{bmatrix}, \qquad X \equiv \begin{bmatrix} 0 & 0 \\ I & 0 \end{bmatrix}. \tag{8.3.70}$$

简单计算即知$I(A,X) = -S(\rho \| \sigma)$。从而由$I(A,X)$的关于 A 的凹性得到$S(\rho \| \sigma)$的联合凸性。

推论 8.3.1（量子条件熵的凹性）设 AB 是两个子系统 A，B 组成的复合量子系统，则条件熵$S(A|B)$关于密度算子ρ^{AB}是凹的。

证明设系统 A 的维数为 d，注意到

$$\begin{aligned} S(\rho^{AB} \| \frac{I}{d} \otimes \rho^B) &= -S(A,B) - tr(\rho_{AB} \log(\frac{I}{d} \otimes \rho^B)) \\ &= -S(A,B) - tr(\rho^B \log \rho^B) + \log d \\ &= -S(A|B) + \log d. \end{aligned} \tag{8.3.71}$$

因此$S(A|B) = \log d - S(\rho^{AB} \| \frac{I}{d} \otimes \rho^B)$。由相对熵的联合凸性得到$S(A|B)$的凹性。

定理 8.3.12（强次可加性）对任意三系统构成的量子系统 A，B，C，如下不等式成立：

$$\begin{aligned} S(A) + S(B) &\leq S(A,C) + S(B,C) \\ S(A,B,C) + S(B) &\leq S(A,B) + S(B,C)。 \end{aligned} \tag{8.3.72}$$

证明定义系统 A,B,C 的密度算子的函数

$$T(\rho^{ABC}) \equiv S(A) + S(B) - S(A,C) - S(B,C) = -S(C|A) - S(C|B)。$$

由条件熵的凹性知$T(\rho^{ABC})$是ρ^{ABC}的凸函数。设$\rho^{ABC} = \sum_i p_i |i\rangle\langle i|$是$\rho^{ABC}$的谱分解，由 T 的凸性，$T(\rho^{ABC}) \leq \sum_i p_i T(|i\rangle\langle i|)$。但是由于对纯态$S(A,C) = S(B)$，$S(B,C) = S(A)$，所以$T(|i\rangle\langle i|) = 0$，所以$T(\rho^{ABC}) \leq 0$。因此，

$$S(A) + S(B) - S(A,C) - S(B,C) \leq 0, \tag{8.3.73}$$

从而证明了第一个不等式。为了得到第二个不等式，引入辅助系统 R 纯化系统 ABC，利用刚刚证明的不等式得到

$$S(R)+S(B)\leq S(R,C)+S(B,C)。 \tag{8.3.74}$$

由于 ABCR 是纯态，$S(R)=S(A,B,C)$，$S(R,C)=S(A,B)$，所以上式化为

$$S(A,B,C)+S(B)\leq S(A,B)+S(B,C), \tag{8.3.75}$$

从而定理得证。

利用强次可加性可以证明许多结论，下面定理是将强次可加性应用于条件熵和互信息的结果。

定理 8.3.13

(1)（条件减小熵）假设 ABC 是一个复合系统，则$S(A|B,C)\leq S(A|B)$。

(2)（去掉量子系统从不增加互信息）假设ABC是复合量子系统，则$S(A:B)\leq S(A:B,C)$。

(3)（量子操作从不增加互信息）假设系统 AB 是复合系统，$\mathcal{E}$是系统 B 上的保迹量子操作，让$S(A:B)$表示$\mathcal{E}$作用前系统 A 和 B 的互信息，$S(A':B')$是作用后的互信息，则$S(A':B')\leq S(A:B)$。

证明

(1) $S(A|B,C)\leq S(A|B)$ 等价于 $S(A,B,C)-S(B,C)\leq S(A,B)-S(B)$，这等价于$S(A,B,C)+S(B)\leq S(A,B)+S(B,C)$，这即为强次可加性，于是得证。

(2)$S(A:B)\leq S(A:B,C)$等价于$S(A)+S(B)-S(A,B)\leq S(A)+S(B,C)-S(A,B,C)$，这就等价于$S(A,B,C)+S(B)\leq S(A,B)+S(B,C)$，即强此可加性，于是得证。

(3)由量子操作的定义，引入系统 C，使得在 B 上作用$\mathcal{E}$等价于在 BC 上作用酉算子 U 在约去系统 C。由于 C 最初与 AB 处于直积态，所以$S(A:B)=S(A:B,C)$,且$S(A:B,C)=S(A':B',C')$。去掉系统不能增加互信息，所以$S(A':B')\leq S(A':B',C')$，综上得到$S(A':B')\leq S(A:B)$。于是得证。

定理 8.3.14（条件熵的次可加性）设 ABCD 是四个量子系统的复合系统，则条件熵满足：

$$S(A,B|C,D)\leq S(A|C)+S(B|D)。 \tag{8.3.76}$$

设 ABC 是三个量子系统的复合系统，则条件熵满足：

$$\begin{aligned} S(A,B|C) &\leq S(A|C)+S(B|C) \\ S(A|B,C) &\leq S(A|B)+S(A|C)。 \end{aligned} \tag{8.3.77}$$

证明为了证明第一个不等式，注意到由强次可加性有：

$$S(A,B,C,D)+S(C)\leq S(A,C)+S(B,C,D)。 \tag{8.3.78}$$

不等式两边加上$S(D)$得

$$S(A,B,C,D)+S(C)+S(D)\leq S(A,C)+S(B,C,D)+S(D)。 \tag{8.3.79}$$

对不等式右边再用一次强次可加性得：

$$S(A,B,C,D)+S(C)+S(D)\leq S(A,C)+S(B,D)+S(C,D), \quad (8.3.80)$$

适当移项即得到

$$S(A,B|C,D)\leq S(A|C)+S(B|D)。 \quad (8.3.81)$$

第二个不等式由强次可加性的定义可直接得到，现证$S(A|B,C)\leq S(A|B)+S(A|C)$。这等价于证明：

$$S(A,B,C)+S(B)+S(C)\leq S(A,B)+S(B,C)+S(A,C) \quad (8.3.82)$$

由于$S(C)+S(B)\leq S(A,C)+S(A,B)$，所以$S(C)\leq S(A,C)$和$S(B)\leq S(A,B)$至少有一者成立。不妨设$S(C)\leq S(A,C)$，将该不等式加上强次可加性不等式$S(A,B,C)+S(B)\leq S(A,B)+S(B,C)$即得到结论。

在介绍量子条件熵概念时，曾说它某种程度上类似于刻画两个密度矩阵之间的距离。按照这种理解，当去掉体系的一部分时，条件熵应该减小。事实上，接下来的定理说明这是正确的，这一结果称为条件熵的单调性。

定理 8.3.15（条件熵的单调性）设ρ^{AB}和σ^{AB}是复合量子系统的任意两个密度矩阵，则

$$S(\rho^A\parallel\sigma^A)\leq S(\rho^{AB}\parallel\sigma^{AB})。 \quad (8.3.83)$$

证明存在态空间 B 上的酉变换U_j和概率分布p_j使得

$$\rho^A\otimes\frac{I}{d}=\sum_j p_j\,U_j\rho^{AB}U_j^\dagger \quad (8.3.84)$$

对所有ρ^{AB}成立。由条件熵的凸性有：

$$S(\rho^A\otimes\frac{I}{d}\parallel\sigma^A\otimes\frac{I}{d})\leq\sum_j p_j\,S(U_j\rho^{AB}U_j^\dagger)\parallel U_j\sigma^{AB}U_j^\dagger)。 \quad (8.3.85)$$

并且简单计算可知:

$$S(\rho^A\otimes\frac{I}{d}\parallel\sigma^A\otimes\frac{I}{d})=S(\rho^A\parallel\sigma^A)。 \quad (8.3.86)$$

又因为相对熵在酉变换下是不变的，即$S(U_j\rho^{AB}U_j^\dagger\parallel U_j\sigma^{AB}U_j^\dagger)$，所以

$$S(\rho^A\otimes\frac{I}{d}\parallel\sigma^A\otimes\frac{I}{d})\leq\sum_j p_j\,S(\rho^{AB}\parallel\sigma^{AB})=S(\rho^{AB}\parallel\sigma^{AB})。 \quad (8.3.87)$$

综上结论得证。

§8.4 Holevo 界

定理 8.4.1（Holevo 界）设 Alice 以概率$\{\boldsymbol{p_0},\ldots,\boldsymbol{p_n}\}$制备状态$\{\boldsymbol{p_x}|\boldsymbol{x}=\boldsymbol{1},\ldots,\boldsymbol{n}\}$，Bob 进行由 POVM 元$\{\boldsymbol{E_y}\}=\{\boldsymbol{E_0},\ldots,\boldsymbol{E_m}\}$描述的测量，测量结果是$\boldsymbol{Y}$。Holevo 证明，Bob 的任何测量结果都满足：

$$\boldsymbol{H(X:Y)\leq S(\rho)-\sum_x p_x S(\rho_x)\equiv\chi} \quad (8.4.1)$$

其中$\boldsymbol{\rho = \sum_x p_x \rho_x}$。Holevo 界是 J. P. Gordon 1964 年猜想的，Holevo 1973 年给出证明。Holevo 定理是量子信息论的基石。Holevo 界也叫做 Holevo$\boldsymbol{\chi}$量。

证明

三个量子系统：P，Q 和 M.

$$\text{Alice} \xrightarrow{Q} \text{Bob}$$

$$\text{P} \qquad\qquad \text{M}$$

(制备）（测量）

假设系统初始状态为：

$$\rho^{PQM} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x \otimes |0\rangle\langle 0|.$$

Bob 用 POVM 元$\{E_y\}$测量系统 Q，将测量结果存于系统 M：

$$\varepsilon(\sigma \otimes |0\rangle\langle 0|) \equiv \sum_y \sqrt{E_y}\sigma\sqrt{E_y} \otimes |y\rangle\langle y|, \tag{8.4.2}$$

下证ε是迹保留操作：

$$\begin{aligned} tr\big(\varepsilon(\sigma \otimes |0\rangle\langle 0|)\big) &\equiv tr\left(\sum_y \sqrt{E_y}\sigma\sqrt{E_y} \otimes |y\rangle\langle y|\right) \\ &= tr\left(\sum_y \sqrt{E_y}\sigma\sqrt{E_y}\right) tr(|y\rangle\langle y|) \\ &= \sum_y tr(\sqrt{E_y}\sigma\sqrt{E_y}) \cdot 1 \\ &= \sum_y tr\big(E_y\sigma\big) \\ &= tr\left(\left(\sum_y E_y\right)\sigma\right) \\ &= tr\sigma = 1 \end{aligned}$$

$\varepsilon(\rho) = \rho'$，故$\varepsilon$是迹保留操作。

根据定理 8.3.13，对 QM 作ε操作不增加互信息，以及丢掉一系统不增加互信息，因此

$$S(P\colon Q) = S(P\colon Q, M) \geq S(P'\colon Q', M')_M \geq S(P'\colon M') \tag{8.4.3}$$

即

$$S(P'\colon M') \leq S(P\colon Q) \tag{8.4.4}$$

又

$$\rho^{PQ} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x \tag{8.4.5a}$$

$$S(P) = H(p_x), \tag{8.4.5b}$$

$$S(Q) = S(\rho), \rho = \sum_x p_x S(\rho_x), \tag{8.4.5c}$$

以及根据定理 8.3.6 中联合熵定理

$$S(P,Q) = H(p_x) + \sum_x p_x S(\rho_x), \tag{8.4.6}$$

可得

$$\begin{aligned} S(P:Q) &= S(P) + S(Q) - S(P,Q) \\ &= H(p_x) + S(\rho) - H(p_x) - \sum_x p_x S(\rho_x) \\ &= S(\rho) - \sum_x p_x S(\rho_x) \end{aligned} \tag{8.4.7}$$

即得 Holevoχ量。

下计算$S(P':M')$.

由于

$$\rho^{P'Q'M'} = \sum_{x,y} p_x |x\rangle\langle x| \otimes \sqrt{E_y}\rho_x\sqrt{E_y} \otimes |y\rangle\langle y| \tag{8.4.8}$$

且

$$p(x,y) = p_x p(y|x) = p_x tr\left(\rho_x E_y\right) = p_x tr\left(\sqrt{E_y}\rho_x\sqrt{E_y}\right), \tag{8.4.9}$$

$$\begin{aligned} \rho^{P'M'} &= tr_Q\left(\rho^{P'Q'M'}\right) \\ &= \sum_{x,y} p_x |x\rangle\langle x| \otimes tr\left(\sqrt{E_y}\rho_x\sqrt{E_y}\right) \otimes |y\rangle\langle y| \\ &= \sum_{x,y} p(x,y) |x\rangle\langle x| \otimes |y\rangle\langle y| \end{aligned}$$

因此，$S(P':M') = H(X:Y)$.

故，$S(P':M') = H(X:Y) \le S(P:Q) = S(\rho) - \sum_x p_x S(\rho_x)$.

于是定理得证.

§8.5 Schumacher 定理

定理 8.5.1（大数定理）设$X_1, \ldots, X_n$是与随机变量 X 同分布的 n 个独立随机变量，X 具有有限的一阶和二阶矩，则对任意$\varepsilon > 0$，当$n \to \infty$时，有$p(|S_n - E(x)| > \varepsilon) \to 0$，这里$S_n = \sum_{i=1}^n X_i/n$.（证明留给读者练习）

设 i.i.d 信源产生比特$X_1, X_2, \ldots$，每个比特以概率 p 等于 0，以概率 1-p 等于 1。Shannon 定理将这些序列分为两类，同类序列出现概率较大的序列——典型序列，和同类序列出现概率较小的序列——非典型序列。具体而言，当序列长度 n 增大时，包含 pn 个 0、(1-p)n 个 1 的这类序列出现的最多，这些序列就是典型序列。任意给定的一个典型序列出现的概率为

$$\begin{aligned} p(x_1, \ldots, x_n) &= p(x_1)p(x_2) \ldots p(x_n) \\ &\approx p^{np}(1-p)^{(1-p)n} \end{aligned} \tag{8.5.1}$$

两边取对数:

$$-logp(x_1, \ldots, x_n) \approx -nplogp - n(1-p)log(1-p) = nH(X) \tag{8.5.2}$$

所以 $p(x_1, \ldots, x_n) \approx 2^{-nH(X)}$.

由此可知，在概率的意义上，有不超过$2^{nH(X)}$个典型序列。

设 i.i.d 信源产生比特$X_1, X_2, \ldots$，每个比特以概率 p(x)等于 x。对于给定的$\varepsilon > 0$，信源的一串符号$x_1 x_2 \ldots x_n$称为 ε-典型序列，若$2^{-n(H(X)+\varepsilon)} \le p(x_1, \ldots, x_n) \le 2^{-n(H(X)-\varepsilon)}$，用$T(n, \varepsilon)$来代表这些 ε-典型序列的集合。

上述定义等价于要求 ε-典型序列满足：

$$\left|\frac{1}{n}\log\frac{1}{p(x_1,\ldots,x_n)} - H(X)\right| \le \varepsilon. \tag{8.5.3}$$

定理 8.5.2（典型序列定理）

(1) 固定 ε>0，则对任意的 δ>0 和充分大的 n，一个序列为 ε-典型序列的概率至少是 1- δ；

(2) 对任意固定的 ε>0，δ>0，对充分大的 n，ε-典型序列的数目$|T(n, \varepsilon)|$满足

$$(1-\delta)2^{n(H(X)-\varepsilon)} \le |T(n, \varepsilon)| \le 2^{n(H(X)+\varepsilon)}; \tag{8.5.4}$$

(3) 令 S(n)为信源发出的长为 n 的序列的集合，集合的大小至多为2^{nR}的集合，其中$R < H(X)$固定，则对任意的$\delta > 0$和充分大的 n，有$\sum_{x \in S(n)} p(x) \le \delta$

证明

（1）考虑独立同分布随机变量$-logp(X_i)$，由大数定理，对于任意$\varepsilon > 0$，$\delta > 0$和充分大的 n，有

$$p\left(\left|\sum_i^n -\frac{logp(X_i)}{n} - E(-logp(X))\right| \le \varepsilon\right) \ge 1-\delta \tag{8.5.5}$$

但$E(logp(X)) = -H(X)$且$\sum logp(X_i) = log(p(X_1, \ldots, X_n))$，因此

$$p\left(\left|\frac{1}{nlog\left(p(X_1,\ldots,X_n)\right)^{-1}} - H(X)\right| \le \varepsilon\right) \ge 1-\delta \tag{8.5.6}$$

即，一个序列是 ε-典型序列的概率至少为 1- δ。

（2）ε-典型序列的概率之和必然小于 1，即

$$1 \geq \sum_{x\in T(n,\varepsilon)} p(x) \geq \sum_{x\in T(n,\varepsilon)} p(x) \geq 2^{-n(H(X)+\varepsilon)} = |T(n,\varepsilon)| \times 2^{-n(H(X)+\varepsilon)} \quad (8.5.7)$$

所以

$$|T(n,\varepsilon)| \leq 2^{-n(H(X)+\varepsilon)} \quad (8.5.8)$$

又由（1）的证明，ε-典型序列的概率之和必然大于 1- δ，即

$$1-\delta \leq \sum_{x\in T(n,\varepsilon)} p(x) \leq \sum_{x\in T(n,\varepsilon)} 2^{-n(H(X)+\varepsilon)} = |T(n,\varepsilon)| \times 2^{-n(H(X)+\varepsilon)} \quad (8.5.9)$$

所以

$$(1-\delta)2^{n(H(X)-\varepsilon)} \leq |T(n,\varepsilon)| \quad (8.5.10)$$

综上，得证。

(3) 取$\varepsilon < H(X) - R$，$0 < \varepsilon < \delta/2$，将 S(n)中的序列分为 ε-典型序列和 ε-非典型序列，总可找到充分大的 n，使得 ε-非典型序列的总概率小于$\delta/2$。

在 S(n)中的 ε-典型序列最多有2^{nR}个，每个出现的概率最多为$2^{-n(H(X)-\varepsilon)}$，因此

$$\sum_{x\in S(n)} p(x) \leq \sum_{x\in S(n),T(n,\varepsilon)} p(x) + \delta/2 \leq 2^{nR} \times 2^{-n(H(X)-\varepsilon)} + \delta/2 \quad (8.5.11)$$

因为$R - H(X) + \varepsilon < 0$，所以总能找到 n，$2^{n(R-H(X)+\varepsilon)} < \delta/2$，于是$\sum_{x\in S(n)} p(x) \leq \delta$.

定理 8.5.3（Shannon 无噪声信道编码定理）

设$\{X_i\}$是一个熵为 H(X)的 i.i.d 信源。假设 R>H(X)，则该信源存在比率为 R 的可靠压缩方案；反之，若 R<H(X)，则任何压缩比率为 R 的压缩方案都是不可靠的。

证明：设 R>H(X)，取 ε 满足$H(X) + \varepsilon < R$.考虑 ε-典型序列的集合$T(n,\varepsilon)$，对任意的$\delta > 0$和充分大的 n，最多有$2^{n(H(X)+\varepsilon)} < 2^{nR}$个这样的序列，且信源产生这样序列的概率至少为$1 - \delta$，从而设置这样的压缩方案，检查信源输出是否为 ε-典型，如果是，则通过 nR 比特的编码存储，如果不是，则压缩到某个固定的指示失败的 nR 比特串，这样可以以趋近于 1 的概率完成压缩。

当$R < H(X)$，因为压缩解压缩方案最多有2^{nR}个输出，故信源最多能有2^{nR}个序列可以无差错的压缩解压缩。由典型序列定理，对充分大的 n，从信源输出的序列落到一个2^{nR}大小的子集中的概率趋于 0，因此任何这样的压缩方案都是不可靠的。

于是定理得证。

定义 8.5.4（ε-典型状态）设一个量子信源相关联的密度算子 ρ 具有标准正交分解：$\rho = \sum_x p(x)|x\rangle\langle x|$.这里的 p(x)满足非负且和为 1，则有$H(p(x)) = S(\rho)$。设$x_1, x_2, \ldots, x_n$是 ε-典型序列，满足

$$\left|\frac{1}{n}\log\frac{1}{p(x_1,\ldots,x_n)} - H(X)\right| \leq \varepsilon, \quad (8.5.12)$$

则状态$|x_1\rangle|x_2\rangle \ldots |x_n\rangle$称为 ε-典型状态。

所有的 ε-典型状态张成的子空间称为 ε-典型子空间，记为$T(n,\varepsilon)$，并把到 ε-典型子空间上的投影记做$P(n,\varepsilon)$，有：

$$P(n,\varepsilon)=\sum_{x\text{为 }\varepsilon-\text{典型的}}|x_1\rangle\langle x_1|\otimes|x_2\rangle\langle x_2|\otimes\ldots|x_n\rangle\langle x_n|. \tag{8.5.13}$$

定理 8.5.5（典型子空间定理）

(1) 固定 ε>0，则对任意的 δ>0 和充分大的 n，有

$$tr(P(n,\varepsilon)\rho^{\otimes n})\geq 1-\delta \tag{8.5.14}$$

(2) 对任意固定的 ε>0，δ>0，对充分大的 n，ε-典型子空间的维数$|T(n,\varepsilon)|=tr(P(n,\varepsilon))$满足

$$(1-\delta)2^{n(S(\rho)-\varepsilon)}\leq|T(n,\varepsilon)|\leq 2^{n(S(\rho)+\varepsilon)}. \tag{8.5.15}$$

(3) 令 S(n)为到$H^{\otimes n}$的任意至多2^{nR}维子空间的一个投影，其中$R<S(\rho)$固定，则对任意的 δ>0 和充分大的 n，有

$$tr\big(S(n)\rho^{\otimes n}\big)\leq\delta. \tag{8.5.16}$$

证明

（1）$P(n,\varepsilon)\rho^{\otimes n}=\sum_{x\text{为 }\varepsilon-\text{典型的}}p(x_1)p(x_2)\ldots p(x_n)|x_1\rangle\langle x_1|\otimes|x_2\rangle\langle x_2|\otimes\ldots|x_n\rangle\langle x_n|$,所以$tr\big(P(n,\varepsilon)\rho^{\otimes n}\big)=\sum_{x\text{为 }\varepsilon-\text{典型的}}p(x_1)p(x_2)\ldots p(x_n)$.

由典型序列定理的第一个结论，一个序列为 ε-典型序列的概率至少是 1- δ，所以

$$tr(P(n,\varepsilon)\rho^{\otimes n})\geq 1-\delta \tag{8.5.17}$$

（2）因$H(p(x))=S(\rho)$，由典型序列定理第二个结论直接得出。

这里利用了$\rho^{\otimes n}=\sum_x p(x)|x\rangle\langle x|$是标准正交分解。

（3）取$0<\varepsilon<S(\rho)-R$，因为

$$tr\big(P(n,\varepsilon)\rho^{\otimes n}\big)=tr\Big(S(n)\rho^{\otimes n}P(n,\varepsilon)\Big)+tr\big(S(n)\rho^{\otimes n}(I-P(n,\varepsilon))\big), \tag{8.5.18}$$

分别作估计，有$\rho^{\otimes n}P(n,\varepsilon)=P(n,\varepsilon)\rho^{\otimes n}P(n,\varepsilon)$，所以

$$tr\Big(S(n)\rho^{\otimes n}P(n,\varepsilon)\Big)=tr\Big(S(n)P(n,\varepsilon)\rho^{\otimes n}P(n,\varepsilon)\Big) \tag{8.5.19}$$

注意到$P(n,\varepsilon)\rho^{\otimes n}P(n,\varepsilon)$的特征值有上界$2^{-n(S(\rho)-\varepsilon)}$，所以

$$tr\Big(S(n)\rho^{\otimes n}P(n,\varepsilon)\Big)\leq 2^{nR}2^{-n(S(\rho)-\varepsilon)} \tag{8.5.20}$$

且当 n 趋于无穷时，此项趋于 0。

又因为$\rho^{\otimes n}(I-P(n,\varepsilon))$是半正定算子，所以

$$tr\big(S(n)\rho^{\otimes n}(I-P(n,\varepsilon))\big)\leq tr\Big(I\rho^{\otimes n}\big(I-P(n,\varepsilon)\big)\Big)=tr\big(\rho^{\otimes n}\big)-tr(\rho^{\otimes n}P(n,\varepsilon))\big).$$

由$tr(P(n,\varepsilon)\rho^{\otimes n}) \geq 1-\delta$，所以当 n 趋于无穷时，此项也趋于 0。

综上，结论成立.

一个 i.i.d 量子信源由一个 Hilbert 空间 H 和一个密度矩阵 ρ来描述。同时假定ρ是一个更大系统上的纯态的一部分， ρ中的混合性质是由 H 和剩余部分系统的纠缠造成。

一个量子系统 Q 制备于状态ρ，引入一个量子系统 S，使得 SQ 联合状态为一个纯态，有一个保迹量子操作ε作用于ρ，定义量子操作ε能够保持 Q 和 S 的纠缠的程度为纠缠保真度 $F(\rho,\varepsilon)$：$F(\rho,\ \varepsilon) = F(SQ, S'Q')^2$

若E_i为ε的一组操作元，则纠缠保真度具有性质：$F(\rho,\ \varepsilon) = \sum_i |tr(E_i\rho)|^2$

一个比率为 R 的压缩方案，包括保迹操作C^n和D^n，C^n把$H^{\otimes n}$中的状态映射到2^{nR}维状态空间，D^n把2^{nR}维状态空间中的状态映射回原来的空间。压缩方案可靠，意味着对于充分大的 n，$F\left(\rho^{\otimes n}, D^n \circ C^n\right)$应该趋于 1

定理 8.5.6（Schumacher 无噪声信道的编码定理）令$\{\boldsymbol{H},\boldsymbol{\rho}\}$是独立同分布的量子信源。若$\boldsymbol{R} > \boldsymbol{S}(\boldsymbol{\rho})$，则对该源存在比率为$\boldsymbol{R}$的可靠压缩方案；若$\boldsymbol{R} < \boldsymbol{S}(\boldsymbol{\rho})$则比率为$\boldsymbol{R}$的任何压缩方案都不可靠。

Schumacher 定理是 Shannon 第一定理的量子推广，证明如下。

证明 1）当$\boldsymbol{R} > \boldsymbol{S}(\boldsymbol{\rho})$，取$\boldsymbol{0} < \boldsymbol{\varepsilon} < \boldsymbol{R} - \boldsymbol{S}(\boldsymbol{\rho})$，根据典型子空间定理，对任意的$\boldsymbol{\delta} > \boldsymbol{0}$和充分大的 n，$\boldsymbol{tr}\left(\boldsymbol{P}(\boldsymbol{n},\boldsymbol{\varepsilon})\boldsymbol{\rho}^{\otimes \boldsymbol{n}}\right) \geq \boldsymbol{1}-\boldsymbol{\delta}$，且$\boldsymbol{\dim}\left(\boldsymbol{T}(\boldsymbol{n},\boldsymbol{\varepsilon})\right) \leq \boldsymbol{2}^{\boldsymbol{nR}}$.

令$\boldsymbol{H}_{\boldsymbol{c}}^{\boldsymbol{n}}$为包含$\boldsymbol{T}(\boldsymbol{n},\boldsymbol{\varepsilon})$的任意$\boldsymbol{2}^{\boldsymbol{nR}}$维子空间，编码方式如下:

首先进行正交投影的完备集$\boldsymbol{P}(\boldsymbol{n},\boldsymbol{\varepsilon})$、$\boldsymbol{I}-\boldsymbol{P}(\boldsymbol{n},\boldsymbol{\varepsilon})$的测量，相应的输出结果记为 0 和 1，若结果为 0 则什么也不做，若结果为 1，则将状态替换为从典型子空间选出的某个标准状态$|\boldsymbol{0}\rangle$，则编码可表示为$\boldsymbol{C}^{\boldsymbol{n}}: \boldsymbol{H}^{\otimes \boldsymbol{n}} \to \boldsymbol{H}_{\boldsymbol{c}}^{\boldsymbol{n}}, \boldsymbol{C}_{\boldsymbol{n}}(\boldsymbol{\sigma}) = \boldsymbol{P}(\boldsymbol{n},\boldsymbol{\varepsilon})\boldsymbol{\sigma}\boldsymbol{P}(\boldsymbol{n},\boldsymbol{\varepsilon}) + \sum_{\boldsymbol{i}} \boldsymbol{A}_{\boldsymbol{i}}\boldsymbol{\sigma}\boldsymbol{A}_{\boldsymbol{i}}^{\dagger}$，其中$\boldsymbol{A}_{\boldsymbol{i}} \equiv |\boldsymbol{0}\rangle\langle\boldsymbol{i}|$，$\{|\boldsymbol{i}\rangle\}$是典型子空间正交补的标准正交基底。

解码运算$\boldsymbol{D}_{\boldsymbol{n}}$：$\boldsymbol{H}_{\boldsymbol{c}}^{\boldsymbol{n}} \to \boldsymbol{H}^{\otimes \boldsymbol{n}}$，定义$\boldsymbol{D}_{\boldsymbol{n}}(\boldsymbol{\sigma}) = \boldsymbol{\sigma}$为恒等变换。由以上定义，有

$$\begin{aligned}\boldsymbol{F}\left(\boldsymbol{\rho}^{\otimes \boldsymbol{n}}, \boldsymbol{D}^{\boldsymbol{n}} \circ \boldsymbol{C}^{\boldsymbol{n}}\right) &= \left|\boldsymbol{tr}\left(\boldsymbol{\rho}^{\otimes \boldsymbol{n}}\boldsymbol{P}(\boldsymbol{n},\boldsymbol{\varepsilon})\right)\right|^2 + \sum|\boldsymbol{tr}\left(\boldsymbol{\rho}^{\otimes \boldsymbol{n}}\boldsymbol{A}_{\boldsymbol{i}}\right)|^2 \\ &\geq \left|\boldsymbol{tr}\left(\boldsymbol{\rho}^{\otimes \boldsymbol{n}}\boldsymbol{P}(\boldsymbol{n},\boldsymbol{\varepsilon})\right)\right|^2 \\ &\geq \left|\boldsymbol{1}^{\boldsymbol{i}} - \boldsymbol{\delta}\right|^2 \\ &\geq \boldsymbol{1} - \boldsymbol{2\delta}\end{aligned}$$

当 n 足够大的时候，$\boldsymbol{\delta}$可以任意小，所以这个压缩方案是可靠的。

2）当$\boldsymbol{R} < \boldsymbol{S}(\boldsymbol{\rho})$时，不失一般性，设压缩变换把$\boldsymbol{H}^{\otimes \boldsymbol{n}}$映射到一个$\boldsymbol{2}^{\boldsymbol{nR}}$维子空间上，对应的投影算子为$\boldsymbol{S}(\boldsymbol{n})$，令$\boldsymbol{C}_{\boldsymbol{j}}$为压缩操作$\boldsymbol{C}^{\boldsymbol{n}}$的操作元，而$\boldsymbol{D}_{\boldsymbol{k}}$为解压缩操作$\boldsymbol{D}^{\boldsymbol{n}}$的操作元，令$\boldsymbol{S}^{\boldsymbol{k}}(\boldsymbol{n})$为到$\boldsymbol{D}_{\boldsymbol{k}}$映射到的子空间的投影，则有

$$F\left(\rho^{\otimes n}, D^n \circ C^n\right) = \sum_{jk} \left|tr\left(D_k C_j \rho^{\otimes n}\right)\right|^2 \quad (8.5.21)$$

易得,

$$C_j = S(n) C_j, \ S^k(n) D_k S(n) = D_k S(n), \quad (8.5.22)$$

$$D_k C_j = D_k S(n) C_j = S^k(n) D_k \, S(n) C_j = \ S^k(n) D_k C_j \quad (8.5.23)$$

所以,

$$F\left(\rho^{\otimes n}, D^n \circ C^n\right) = \sum_{jk} \left|tr\left(S^k(n) D_k C_j \rho^{\otimes n}\right)\right|^2 = \sum_{jk} \left|tr\left(D_k C_j \rho^{\otimes n} S^k(n)\right)\right|^2 \quad (8.5.24)$$

应用 Cauchy-Schwarz 不等式和 Hilbert-Schmidt 内积，令

$$A_{kj} = \left(D_k C_j \left(\rho^{\otimes n}\right)^{\frac{1}{2}}\right)^{\dagger}, B_k = \left(\rho^{\otimes n}\right)^{\frac{1}{2}} S^k(n) \quad (8.5.25)$$

则，

$$F\left(\rho^{\otimes n}, D^n \circ C^n\right) = \sum_{jk} \left|\left(A_{kj}, B_k\right)\right|^2 \leq \sum_{kj} \left(A_{kj}, A_{kj}\right) \left(B_k, B_k\right) \quad (8.5.26)$$

即，

$$F\left(\rho^{\otimes n}, D^n \circ C^n\right) \leq \sum_{jk} tr\left(D_k C_j \rho^{\otimes n} C_j^{\dagger} D_k^{\dagger}\right) tr\left(S^k(n) \rho^{\otimes n}\right). \quad (8.5.27)$$

根据典型子空间定理，$tr\left(S^k(n) \rho^{\otimes n}\right) \leq \delta$，不等式成立与 k 无关。注意到

$$\sum_{jk} tr\left(D_k C_j \rho^{\otimes n} C_j^{\dagger} D_k^{\dagger}\right) = D^n \circ C^n\left(\rho^{\otimes n}\right), \quad (8.5.28)$$

而D^n, C^n都是保迹操作，所以有

$$\sum_{jk} tr\left(D_k C_j \rho^{\otimes n} C_j^{\dagger} D_k^{\dagger}\right) = tr\left(\sum_{jk} D_k C_j \rho^{\otimes n} C_j^{\dagger} D_k^{\dagger}\right) = tr\left(D^n \circ C^n\left(\rho^{\otimes n}\right)\right) = tr\left(\rho^{\otimes n}\right) = 1$$

因此，$F\left(\rho^{\otimes n}, D^n \circ C^n\right) \leq \delta \sum_{jk} tr\left(D_k C_j \rho^{\otimes n} C_j^{\dagger} D_k^{\dagger}\right) = \delta$。

由于δ是任意的，所以当 n 趋于无穷时，$F\left(\rho^{\otimes n}, D^n \circ C^n\right)$趋于 0，从而任意的压缩方案都是不可靠的。定理得证。

信道ε传递直积态$\rho_1 \otimes \rho_2 \ldots \otimes \rho_n$编码经典消息，则信道容量$C^{(1)}(\varepsilon)$由下述定理给出：

定理 8.5.7（HSW 定理）设ε是一个保迹量子操作，定义:

$$\chi(\varepsilon) \equiv \max_{\{p_i, \rho_i\}} \left[S\left(\varepsilon\left(\sum_j p_j \rho_j\right)\right)\right] - \sum_j p_j S\left(\varepsilon\left(\rho_j\right)\right), \quad (8.5.29)$$

其中最大值是在信道的所有可能状态ρ_j的系综$\{p_j, \rho_j\}$上取的，则有$C^{(1)}(\varepsilon) = \chi(\varepsilon)$。

参考书目

1. M A Nielsen and I L Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000

2. J Gruska, Quantum Gomputating, McGraw-Hill, 1999

3. J J Sakurai, Modern Quantum Mechanics, 世界图书出版公司，1994

4. J D 比约肯，S D 德雷尔，相对论量子力学，科学出版社，1984

5. E G 哈里斯，现代理论物理导论（第二卷），上海科学技术出版社，1985

6. 曾谨言，裴寿镛，量子力学新进展（第一辑），北京大学出版社，2000

7. J D Barrow, et al., Science and Ultimate Reality, Cambridge University Press, 2004

8. 张礼，葛墨林，量子力学的前沿问题，清华大学出版社，2000

9. A Peres, Quantum Theory: Concepts and Methods, Kluwer Academic Publishers, 1995

10. 卢开澄，组合数学，清华大学出版社，1991

11. F Kuhnert，广义逆矩阵与正则化方法，高等教育出版社，1985

12. 倪国熙，常用的矩阵理论和方法，上海科学技术出版社，1984

13. 徐洁磐，离散数学导论，高等教育出版社，1982

14. 冯登国，裴定一，密码学导引，科学出版社，1999

15. D R Stinson，密码学原理与实践，电子工业出版社，2009

16. 李承祖等，量子通信与量子计算，国防科技大学出版社，2000

习题

习题 1.$\{\vec{n}_\alpha \,|\, |\vec{n}_\alpha|^2 = 1, \alpha = 1,2,\cdots,N\}$满足$\sum_\alpha \lambda_\alpha \vec{n}_\alpha = 0$，其中$0 < \lambda_\alpha < 1$，$\sum_\alpha \lambda_\alpha = 1$。构造$\hat{F}_\alpha = \lambda_\alpha(\hat{I} + \vec{n}_\alpha \cdot \hat{\sigma})$，证明$\hat{F}_\alpha$是半正定的，且$\sum_\alpha \hat{F}_\alpha = \hat{I}$，从而$\{\hat{F}_\alpha \,|\alpha = 1,\cdots,N\}$在一个量子位的二维态空间中定义了一个 POVM 测量。

习题 2.电子自旋$\vec{s} = \frac{\hbar}{2}\vec{\sigma}$，沿空间方向$\vec{n} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$的分量为$\vec{\sigma}\cdot\vec{n}$。矩阵表示为$\vec{\sigma}\cdot\vec{n} = \begin{pmatrix} \cos\theta & \sin\theta e^{-i\varphi} \\ \sin\theta e^{i\varphi} & -\cos\theta \end{pmatrix}$，求密度矩阵$\rho(\sigma_n = 1)$和$\rho(\sigma_n = -1)$，并在$|\sigma_n = 1\rangle$态下证明：

$$\begin{cases} \langle\sigma_x\rangle = tr(\rho\sigma_x) = \sin\theta\cos\varphi \\ \langle\sigma_y\rangle = tr(\rho\sigma_y) = \sin\theta\sin\varphi \\ \langle\sigma_z\rangle = tr(\rho\sigma_z) = \cos\theta, \end{cases}$$

即$\langle\vec{\sigma}\rangle = \vec{n}$。

习题 3.证明$(\vec{\sigma}\cdot\vec{n}_1)(\vec{\sigma}\cdot\vec{n}_2) = (\vec{n}_1\cdot\vec{n}_2)\,I + i\,\vec{\sigma}\cdot(\vec{n}_1\times\vec{n}_2)$。

习题 4.利用 Schmidt 分解证明复合系统 AB 的一个态$|\psi\rangle$是直积态当且仅当 Scmidt 数为 1。并证明$|\psi\rangle$是直积态当且仅当ρ^A是纯态。

习题 5.$\{|0\rangle, |1\rangle\}$是希尔伯特空间R^2的一组正交基，令$A := |0\rangle\langle 0| + |1\rangle\langle 1|$。考虑以下三种情况时：

(1) $\quad |0\rangle = \begin{pmatrix}1\\0\end{pmatrix}; |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$

(2) $\quad |0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}; |1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$

(3) $\quad |0\rangle = \begin{pmatrix}\cos\theta\\\sin\theta\end{pmatrix}; |1\rangle = \begin{pmatrix}\sin\theta\\-\cos\theta\end{pmatrix}$

请写出 A 的矩阵表达式。

习题 6.令$|\psi\rangle = \begin{pmatrix} e^{i\phi}\cos\theta \\ \sin\theta \end{pmatrix}$，其中$\phi, \theta \in \mathbf{R}$。

(1) 计算$\rho = |\psi\rangle\langle\psi|$；

(2) 计算$tr\rho$；

(3) 计算ρ^2。

习题 7.受控非门的作用由$|c\rangle|t\rangle \to |c\rangle|t \oplus c\rangle$给出，即如果控制量子比特置为$|1\rangle$，则目标量子比特翻转，否则目标量子比特保持不变。请写出受控非门的矩阵表示，并说明原因。

习题 8.X,Y,Z 分别为三个泡利矩阵，H 为 Hadamard 变换，证明：

$$HXH = Z; \quad HYH = -Y; \quad HZH = X。$$

习题 9.证明若算子 A、B 是厄米的，则$i[A,B]$是厄米的。

习题 10.证明任意单量子比特混合态的密度矩阵可以表示为

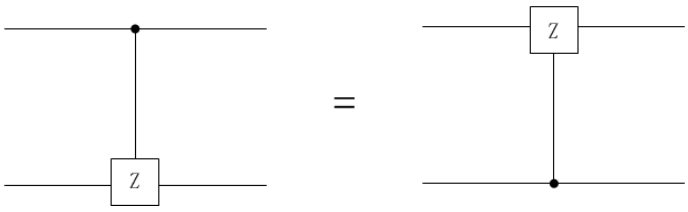
$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2},$$

其中$\vec{r}$是满足$\| \vec{r} \| \leq 1$的实三维向量，$\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$是泡利算子构成的向量。

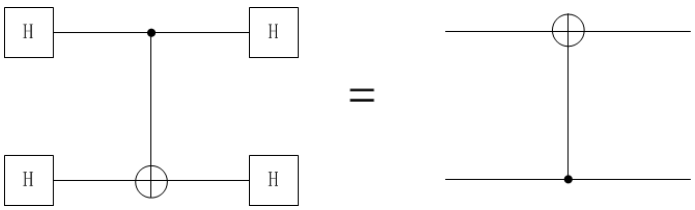
习题 11.设 C 为第一个量子比特作为控制比特，第二个量子比特作为靶比特的 CNOT 门，下标 1 表示算子作用于第一个量子比特，下标 2 表示算子作用于第二个量子比特。证明下面等式:

$$\begin{aligned} CX_1C &= X_1X_2; \\ CY_1C &= Y_1X_2; \\ CZ_1C &= Z_1; \\ CX_2C &= X_2; \\ CY_2C &= Z_1Y_2; \\ CZ_2C &= Z_1Z_2。 \end{aligned}$$

习题 12.证明：



习题 13. 证明：



习题 14.

(1)证明对任意满足$A^2 = I$的算子A，有$exp(iAx) = \cos xI + i\sin xA$。

(2)利用(1)中证明的公式，写出旋转算子$R_x(\theta) \equiv e^{-i\theta X/2}$,$R_y(\theta) \equiv e^{-i\theta Y/2}$，$R_z(\theta) \equiv e^{-i\theta Z/2}$的矩阵表示。

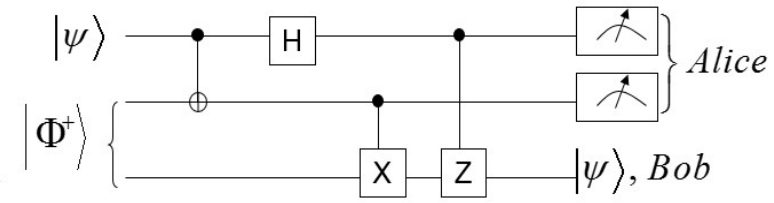
习题 15. 证明正规矩阵是厄米的，当且仅当它的特征值为实数。

习题 16. 证明厄米算子的具有不同本征值的两个本征向量必须正交。

习题 17. 设ρ是一个密度算子，证明$tr(\rho^2) \leq 1$，且$tr(\rho^2) = 1$当且仅当ρ是纯态。

习题 18. 对 Bell 态$|\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$，求第一个量子比特的约化密度矩阵。

习题 19. 图为量子隐形传态的量子线路，上面两个量子比特属于 Alice，下面的一个属于 Bob。试证明，当 Alice 的输入端为任意量子态$\Psi\rangle$时，Bob 的输出端为$|\Psi\rangle$。



习题 20.

已知双量子比特系统的一个量子态$\rho_{AB} = \frac{1}{8}I + \frac{1}{2}|\Psi^-\rangle\langle\Psi^-|$，其中$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$。求$\rho_{AB}$的普表示。

习题 21. 对下列给出的校验阵，分别求相应的生成阵，并说明可以纠正几位错误。

（1）

$$H_3 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

（2）

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

习题 22. $\{p_x\}$和$\{q_x\}$为两个概率分布，证明经典的迹距离满足：

$$D(p_x, q_x) = \max_S(p(S) - q(S)) = \max_S(\sum_{x\in S} p_x - \sum_{x\in S} q_x),$$

其中最大是对指标集$\{x\}$的所有子集S取的。

习题 23. $|\Psi\rangle$为纯态，σ为密度算子，证明：

$$1 - F(|\Psi\rangle, \sigma)^2 \le D(|\Psi\rangle, \sigma)。$$

习题 24. 证明迹距离在酉变换下不变，即对任意的密度算子ρ和σ，任意的酉算子U有：

$$D(U\rho U^\dagger, U\sigma U^\dagger) = D(\rho, \sigma)。$$

习题 25. 求两个密度算子$\frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$，$\frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|$的迹距离。

习题 26. (保真度的凹性).证明：

$$F(\sum_i p_i\,\rho_i, \sigma) \ge \sum_i p_i\,F(\rho_i, \sigma)。$$

习题 27(Hilbert-Schmidt 内积与纠缠). 假设 R 和 Q 是有着相同 Hilbert 空间的两个量子系统，$|i_R\rangle$和$|i_Q\rangle$分别是 R 和 Q 的标准正交基。A 是作用在 R 上的算子，B 是作用在 Q 上的算子，令$|m\rangle \equiv \sum_i |i_R\rangle|i_Q\rangle$，证明：

$$tr(A^\dagger B) = \langle m|(A^* \otimes B)|m\rangle,$$

等式左边的乘法是矩阵乘法，矩阵 A 和 B 是算子 A，B 分别对应于基$|i_R\rangle$和$|i_Q\rangle$的矩阵。

习题 28. 证明保真度在酉变换下不变，即对任意的密度算子ρ和σ，任意的酉算子U有：

$$F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho,\sigma)。$$

习题 29. 对任意矩阵 A，范数$\|\cdot\|$定义为：

$$\| A \| \equiv \max_{\langle u|u\rangle=1} |\langle u|A|u\rangle|。$$

设 A 有本征值λ_i，定义λ是$|\lambda_i|$中的最大值，证明：

（1）$\| A \| \geq \lambda$;

（2）当 A 为厄米阵时，$\| A \| = \lambda$

习题 30. $|AB\rangle$是复合系统 AB 的一个纯态，证明$|AB\rangle$是纠缠态当且仅当条件熵$S(B|A) < 0$。

习题 31. 函数$\eta(x) \equiv -x\log x$，利用导数证明当$|r-s| < \frac{1}{2}$时：

$$|\eta(r) - \eta(s)| \leq \eta(|r-s|)。$$

习题 32. 设 Alice 交给 Bob 处于$|\phi_1\rangle = |0\rangle$或$|\phi_2\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$两状态之一的量子比特，构造一个 POVM$\{E_1, E_2, E_3\}$，使得如果结果是$E_i, 1 \leq i \leq 3$时，Bob 可以确定他收到的是状态$|\phi_1\rangle$还是$|\phi_2\rangle$。

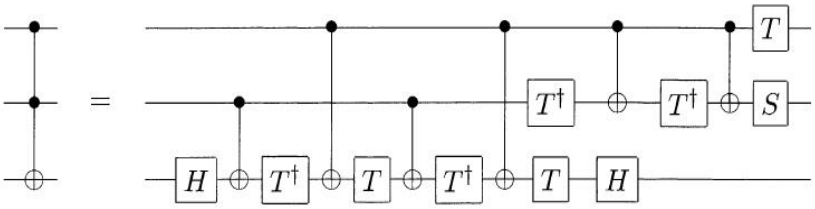
习题 33. 设$f(\cdot)$是任意将复数映成复数的函数，$\vec{n}$是三维单位向量，θ是实数，证明：

$$f(\theta\,\vec{n}\cdot\vec{\sigma}) = \frac{f(\theta)+f(-\theta)}{2} I + \frac{f(\theta)-f(-\theta)}{2}\vec{n}\cdot\vec{\sigma}.$$

习题 34. 证明：

$$F(\rho,\sigma) = \max_{|\varphi\rangle} |\langle\psi|\varphi\rangle|$$

其中$|\psi\rangle$是任意固定的ρ的纯化态，极大是对σ的所有纯化态取的。



习题 35. 证明下图中的两个电路相等，即 Toffoli 门可以表示为等号右边的电路。

习题 36(Tsirelson 不等式). 假设$Q=\vec{q}\cdot\vec{\sigma}$，$R=\vec{r}\cdot\vec{\sigma}$，$S=\vec{s}\cdot\vec{\sigma}$，$T=\vec{t}\cdot\vec{\sigma}$，其中$\vec{q}$，$\vec{r}$，$\vec{s}$，$\vec{t}$是三维空间的实单位向量。证明

$$(Q\otimes S+R\otimes S+r\otimes T-Q\otimes T)^2=4I+[Q,R]\otimes[S,T]$$

其中两个算子A,B的对易子$[A,B]$定义为$[A,B]=AB-BA$仍是Hilbert 空间上的算子。并用这个结果证明：

$$<Q\otimes S>+<R\otimes S>+<R\otimes T>-<Q\otimes T>\leq 2\sqrt{2}.$$

习题 37. 假设 A 是半正定矩阵。定义超算子$\mathcal{A}(X)\equiv AX$，其中 X 是 Hilbert 空间上的任意线性算子。证明$\mathcal{A}$相对于 Hilbert-Schmidt 内积是半正定的，即对所有的 X，有$tr(X^{\dagger}\mathcal{A}(X))\geq 0$。类似地，证明超算子$\mathcal{A}\equiv XA$相对于 Hilbert-Schmidt 内积是半正定的（Hilbert 空间上两个算子 A，B 的 Hilbert-Schmidt 内积定义为$\langle A,B\rangle=tr(A^{\dagger}B)$）。

习题 38. 设 AB 是复合量子系统，处于状态ρ^{AB}。对系统 B 单独地作用酉算子U_B后，系统的密度算子为$\rho^{A'B'}$，证明系统 A 的约化密度算子不变，即

$$\rho^{A}=\rho^{A'}.$$

习题 39. 求密度矩阵$\rho=\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}$的熵$S(\rho)$。

习题 40. 证明 vonNeumann 熵的上限。如果ρ有 D 个不为零的本征值，于是将有:

$$S(\rho)\leq \log D.$$

等号是当所有非零本征值均相等时成立。

习题 41. 按均匀分布制备以下三个态

$$|\psi_1\rangle=\begin{pmatrix}1\\0\end{pmatrix},\quad |\psi_2\rangle=\begin{pmatrix}-\frac{1}{2}\\\frac{\sqrt{3}}{2}\end{pmatrix},\quad |\psi_3\rangle=\begin{pmatrix}-\frac{1}{2}\\-\frac{\sqrt{3}}{2}\end{pmatrix},$$

求相应的混合态的密度矩阵。

习题 42. 如果量子态$|\alpha\rangle$和$|\beta\rangle$是非正交的，请证明没有测量可以严格区分以上两个量子态，并写出具体证明过程。

习题 43. 求两个密度算子$\frac{3}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|$和$\frac{2}{3}|+\rangle\langle +|+\frac{1}{3}|-\rangle\langle -|$的迹距离。

习题 44. 已知量子态$\rho = p|0\rangle\langle 0| + (1-p)|+\rangle\langle +|$，计算$S(\rho)$的值。

习题 45. 量子态$\rho = p|0\rangle\langle 0| + (1-p)|+\rangle\langle +|$通过量子相位翻转信道传输，请写出纠缠保真度$F(\rho, \epsilon)$（量子相位翻转信道的运算元为：$E_0 = \sqrt{p}I$，$E_1 = \sqrt{1-p}Z$）。

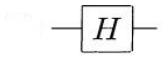
习题 46. 假如$\rho_A = \frac{1}{2}(I + \vec{n}_A \cdot \vec{\sigma})$和$\rho_B = \frac{1}{2}(I + \vec{n}_B \cdot \vec{\sigma})$，证明$tr(\rho_A \rho_B) = \frac{1}{2}(I + \vec{n}_A \cdot \vec{n}_B)$，其中$\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$为泡利矩阵构成的向量。

习题 47. 任意两个矩阵A和B，称$A \leq B$若$B - A$是一个半正定阵。证明若$A \leq B$，则对任意矩阵X有$XAX^\dagger \leq XBX^\dagger$。

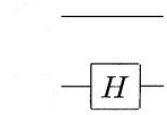
习题 48. 证明：$[X, Y] = 2iZ$;　　$[Y, Z] = 2iX$;　　$[Z, X] = 2iY$。

习题 49. 写出下面线路在计算基下的4×4矩阵表示。

(1)



(2)



习题 50. 证明保真度是联合凹的，即

$$F\left(\sum_i p_i \rho_i, \sum_i p_i \sigma_i\right) \geq \sum_i p_i F(\rho_i, \sigma_i)。$$