Liangzixinxiyuliangzijisuan

量子信息与量子计算

简明教程

jianmingjiaocheng

陈汉武 编

東南大學出版社

jiangzixinxiyuliangzijisuan

jianmingjiaocheng

责任编辑／ 张　烨
封面设计／ 余晓莉

ISBN 7-5641-0349-3
9 787564 103491 >

ISBN 7-5641-0349-3
TP·57　定价：20.00 元

量子信息与量子计算简明教程

陈汉武　编

东南大学出版社

内 容 简 介

本书以量子信息为起点，以经典信息理论为参照，通过经典比特(bit)与量子比特(qubit)的属性对比，引入量子计算概念，解读信息量子化的基本变换规则，介绍基本量子逻辑门。在量子经典信息的基础上着重讲解量子信息计算的基本规则与原理，讲解量子信息传输中信息演算的基本方法。本书的内容涉及量子纠错编码原理及其编码构成原则，量子纠缠状态及其在量子通信方面的应用，量子纠缠状态的纯粹化协议及其应用，以及量子通信信道及量子信道容量简介。

本书可以作为信息与计算学科、应用数学、通信工程、信息工程等专业本科生的教材，或大学高年级学生和研究生的自学读本，也可作为一般有兴趣的读者了解该领域的入门读物。

图书在版编目(CIP)数据

量子信息与量子计算简明教程/陈汉武编. —南京：
东南大学出版社，2006.6
ISBN 7-5641-0349-3

Ⅰ.量... Ⅱ.陈... Ⅲ.①第五代计算机—教材
②量子力学—信息技术—教材 Ⅳ.①TP387②0413.1

中国版本图书馆 CIP 数据核字(2006)第 039578 号

东南大学出版社出版发行
（南京四牌楼 2 号 邮编 210096）
出版人：宋增民
江苏省新华书店经销 溧阳市晨明印刷有限公司
开本：700mm×1000mm 1/16 印张：12.25 字数：240 千
2006 年 6 月第 1 版 2006 年 6 月第 1 次印刷
印数：1—2000 册 定价：20.00 元
（凡因印装质量问题，可直接向读者服务部调换。电话 025-83792328）

前　言

量子信息与量子计算的研究可以追溯到几十年前，但真正引起广泛关注是在20世纪90年代中期，这期间发现了Shor量子因子分解算法和Grover量子搜索算法，这两个算法展示了量子计算机从根本上超越经典计算机计算能力和在信息处理方面的巨大潜力。与此同时，量子计算机和量子信息处理装置在物理实现方面的研究，成为继并行计算机、生物计算机等之后的非串行计算体系的又一热点。

量子信息与量子计算对人类社会最具影响也最为惊人的发现之一，是量子计算机能够迅速破解广泛使用的RSA密码系统，掌握量子计算能力的制高点已成为关系信息安全的重要课题。

编者在日本留学期间，在指导教师的影响与帮助下，于1999年申请到由日本地方政府资助的题为“实现信息量子通信基础技术的理论研究”的预研项目，从此在学习与研究中开始涉及量子信息与量子计算的相关内容。首先参加了每周一次的研讨班，于是有了对量子信息理论的初步认识，也有了最初的一些收获与积累。2000年春节假期后由于工作需要编者离开了研讨班，直到2003年回国任教。回国后，学校鼓励教师为学生开设新课，编者便自然而然地想到了量子信息与量子计算这门为近代科技日渐关注的新的研究领域，于是决定为信息类的学生开设信息理论基础的课程，其中量子信息与量子计算内容作为课程的后半部，编者重新整理材料，编写了“量子信息与量子计算基础”讲义，经过一轮试讲与两轮修改，于是有了现在的这本教材。本教材可作为信息与计算学科、应用数学、通信工程、信息工程等专业本科生的教材，或大学高年级学生和研究生的自学读物，也可作为有兴趣的读者了解该领域的入门读物。

量子信息与量子计算领域发展非常迅速，既有理论层面的研究又有应用层面的研究，限于水平，书中难免存在一些错误和不足，希望广大读者批评指正。

编者

2006.3

目　录

绪　论

人类社会的生存与发展无时无刻都离不开信息，人们越来越注重各类信息的获取、处理、控制、传递和利用。随着人类迈入 21 世纪高度信息化的时代，信息的重要性更是不言而喻。

哲学家和科学家普遍认为：物质、能量和信息是组成物质世界的三大支柱，是科学历史上三个重要的基本概念。的确，宇宙万物无时不在运动，只要有运动的事物，就需要有能量，就会产生各种各样事物运动的状态和方式，也就会产生信息。可见，信息是普遍存在的，是物质的一种普遍属性。

信息是物质的属性，但不是物质自身。事物运动的状态和方式一旦体现出来，就可以脱离原来的事物而相对独立地载负于别的事物上而被提取、表示、处理、存储和传输。因此，信息不等于它的原事物，也不等于它的载体。信息虽不等于物质本身，但它也不能脱离物质而独立存在，必须以物质为载体，以能量为动力。物质、能量和信息三者相辅相成，缺一不可，这也正是信息的绝对性和普遍性。

研究信息的产生、存储、加工、传播等行为的科学理论称为信息学理论。根据研究的范畴和侧重点不同，信息学理论一般有三种理解：狭义信息论、一般信息论和广义信息论。

狭义信息论以传输信息的各种通信系统为对象，研究信息传输和处理的共同规律。我们从各种通信系统中抽象出具有共同特性的元素，即可将其概括成一个如图 1 所示的理论模型。

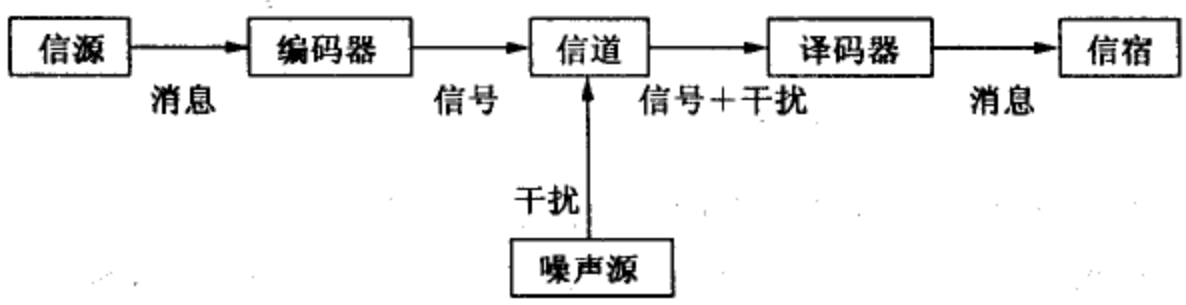


图 1　通信系统的理论模型

其中：

（1）信源——产生消息和消息序列的源；

(2) 编码器——把消息变换成信号的设备；

(3) 信道——指通信系统把载荷消息的信号从甲地传输到乙地的媒介；

(4) 译码器——对信道输出的编码信号进行逆变换的设备；

(5) 信宿——消息传送的对象。

图中所指编码器可分为两种：信源编码器和信道编码器。信源编码的目标是尽可能地缩短消息和消息序列的平均编码的长度，实现数据压缩，提高信息传输的效率。信道编码将根据信道的统计特性，在选择最佳译码规则的前提下，适当增加信息编码的冗余，使通过信道编码设施输出的信号在有噪信道的传输过程中，通过尽可能小的编码冗余使信号具有最强的自动纠错能力，以提高信息传输的可靠性。

近年来，以计算机为核心的大规模信息网络，尤其是互联网的建立和发展，对信息传输的质量要求更高了，不但要求既快速有效又能可靠地传递信息，而且还要求信息传输过程中保证信息的安全保密，不被伪造和窜改。于是，信息传输的高效性、可靠性、保密性和认证性四项指标构成了对现代通信系统的全面要求。高效性旨在系统用尽可能少的时间和尽可能少的设备来传输一定数量的信息；可靠性就是要使信源发出的信息经过信道传输后尽可能准确、不失真地再现在接收端；保密性是指要隐蔽和保护通信系统中传输的信息；认证性强调信息的接收者能正确判断所接收的消息的正确性，验证消息的完整性，确认其不是伪造和被串改的。带有信息安全保密的通信系统可以概括成如图 2 所示的理论模型。

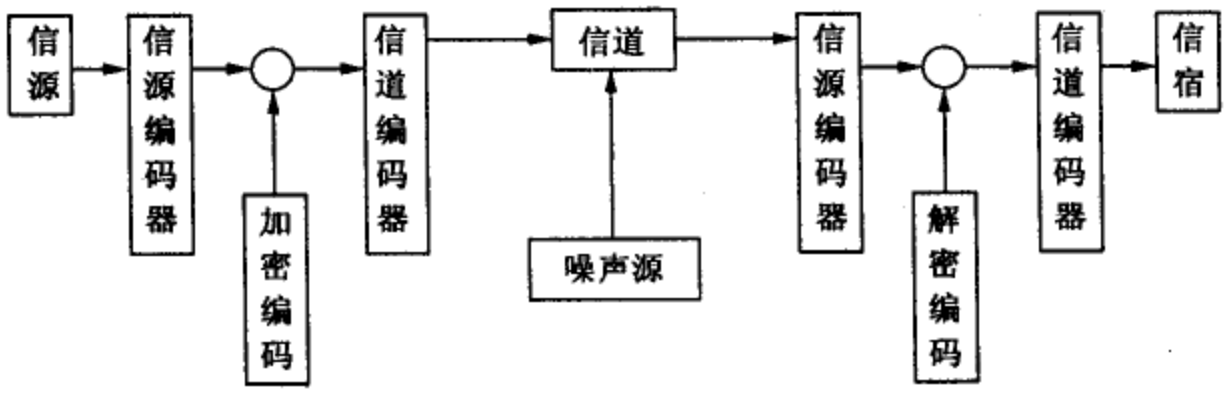


图 2　带有信息安全保密的通信系统的理论模型

每个人都会认为“信息”是个抽象的词汇。每个人都知道“通信”是人类活动中普遍的现象之一。每个人都希望在频繁的信息传递和交换中，能够高效、可靠地传递和接收到信息。那么，人们是否会自然地提出这样一些问题：信息是什么？衡量通信的有效程度和可靠程度的标准是什么？怎样判断通信方法的优和劣？显然，解决这些问题的关键就在于解决信息的定义与度量的问题。

最早对信息进行科学定义的是哈特来(R. V. L. Hartley)，1928 年他发表的

《信息传输》一文首先提出了“信息”这一概念。1948 年控制论创始人之一维纳(N. Wiener)出版了《控制论——动物和机器中通信与控制问题》一书,他指出“信息是信息,不是物质,也不是能量”。这就是说,信息就是信息自己,它不是其他什么东西的替代物,它是与“物质”、“能量”同等重要的基本概念。1948 年香农(C. E. Shannon)在 BSTJ(Bell System Technical Journal)上发表了著名的论文《通信的数学理论》(A Mathematical Theory of Communication)。论文中香农集人类在长期有关信息操作的实践中,应用概率统计、随机过程、代数等数学方法,研究信息的表示、存储、加工和传输等一般的规律之大成,从研究通信系统信息传输的实质出发,探讨了信息的测度问题,研究了信息的信源编码和信道编码的最佳性与极限性理论,以及编码后的信息传输率与信道的容量及其计算理论等内容。香农在论文中对信息作出了科学的定义,利用平均信息量(熵)对信息及其行为进行了定性和定量的描述,从而奠定了信息学理论的数学基础。因此,经典信息理论也称为香农理论。

香农在《通信的数学理论》中给出了信息学理论中两个著名的基本定理:信源编码定理与信道编码定理。信源编码定理也称为无噪信道编码定理或称香农第一编码定理;信道编码定理又称为含噪信道编码定理或称香农第二编码定理。从信息编码与高效可靠的通信角度来看,信源编码强调利用以哈夫曼码(Huffman codes)为代表的编码技术,考虑数据压缩,去除编码冗余,实现信息传输的高效性;信道编码采用汉明码(Hamming codes)思想,通过增加信息编码的冗余(校验码元),增强信息自身的抗干扰能力,达到编码自动纠正错误的目标,实现信息传输的可靠性。

信息理论在考虑信息的测度、信息编码的效率时,以消息事件及其发生的概率组成的概率空间为研究对象,用某消息发生时对观察者来说消除某种不确定性程度的大小来表示该消息含有的信息量。利用概率学中的熵(Entropy)表示(消息)概率空间的平均信息量,并以此为尺度基点,度量信息量的大小,衡量消息的编码效率,给出信源编码的压缩极限和信道编码的传输效率并推导出信道的容量。香农在其论文中针对人类通信活动的特点,以新颖的思想提出用数学方法定量描述信息,在信息的抽取和度量中精辟地概括出信息的“形式化”假说、“非决定”论和“不确定”性三个概念。

所谓信息的“形式化”假说是要我们大胆地去掉蕴含在消息中那些狭义信息理论并不关心的语义与语用等因素,保留那些能用数学形式描述的因素和符号,使得用数学工具定量测度信息成为可能。

所谓信息的“非决定”论观点是对信息通信活动的总的认识观。香农利用概率中弱大数定律的直接推论,得到的信息集合的渐近等分割性并从中划分出 ε

典型序列后，从原则上解决了必须应用概率论、随机过程及数理统计等数学工具，从大量不可预料的随机消息（包括噪音）的集合中，寻求信息的统计规律，揭示出信息的表示本质，从而选择并获取一个实际的正确的消息。

香农从消息发生的“不确定”性观点出发，给“信息”下了这样明确的定义：“信息就是用来消除不确定性的东西”，即通信后接收者获取的信息，在数量上等于通信前后不确定性的消除量。因为我们知道“不确定”性与“可能”性是相互联系的。“可能”性的大小表示事物出现或发生几率的大小，在数学上可以用概率的大小来表示。概率大即表示事物出现的“可能”性大；概率小即表示事物出现的“可能”性小。而“可能”性大就意味着“不确定”性小；“可能”性小就意味着“不确定”性大。这样，“不确定”性就可与消息发生的概率联系起来。因此，我们可以得出这样的结论：通信后获取的信息量应该是消息发生概率的某一函数。这就从理论上完全解决了信息的度量问题。

熵是一个抽象的起源于热力学解析的数学概念，自从 1865 年克劳修斯发现并提出了熵的概念以来，熵就作为一个数学工具，在探索那些属性表现模糊、知识点表示暧昧、时空不确定的物质世界的规律之中起着重要的作用。熵可以测度现实世界中存在的但却无法触摸的事物本体“体量”统计平均值的大小，平均值的大小来自于一切具体的事物本体信息集合除去信息本身语义后余下的纯粹数值性的量，利用这个量的概念我们可以形式化地表现和处理现实世界中很多知识表现模糊的问题。因此，熵的概念不但在信息理论中起到主导作用，在当今许多应用科学领域的研究中也起到了重要作用。

由以上叙述可知，信息论是一门高度抽象和概括的学科，它的研究对象不是具体的消息，而是各种不同形式的消息抽象后的“信息”。信息论的研究目标是提高信息系统的可靠性、有效性、保密性和认证性，确保信息系统的最优化。它是信息科学与技术发展的起点和基石，它的研究方法及理念在现代许多科学领域中有着广泛的应用。

相对于 20 世纪末期新生的现代量子信息理论，我们称香农理论为经典信息理论。量子信息学是一门新兴的、以量子力学与经典信息学理论为主干的交叉性学科。量子信息学的研究对象主要包括量子通信技术、量子密码技术、量子计算技术以及量子器件技术的研究与开发。量子信息理论为信息科学和技术的变革、持续高速发展提供了新的原理和方法。随着科学的发展和微电子器件技术的进步，我们跨越了经典信息论和计算理论的奠基者、科学家们的年代。随着量子物理实验成果的不断涌现，我们对信息及其表示与处理的认识有了质的变化，从承传香农、图灵、冯·诺伊曼等科学家视信息处理为宏观过程，到今天事实告诉我们：信息的处理能够以微观过程实现。

微观过程存在于微观世界，微观世界的客体是统称为量子的微观粒子，描述微观粒子运动规律的学科是量子力学。微观世界是一个充满新奇的混沌世界，微观客体的行为怪异多变，微观系统的能力无法估量。

在经典物理中物理量具有确定的量值，服从明确的规律。而量子力学中物理量要服从统计的规律，必须用“态矢空间”里的“算符”表示。一般说来，一个量子量有多个“本征值”，测量时我们无法获得它们所有确定的量值，而是以被测量值发生在一定概率区间的概率幅得到它们的某个本征值。概率幅是复数，它的模平方是概率。概率幅具有模量和相角，因此量子状态的叠加还会产生干涉现象。这个干涉现象，宏观世界的人类无法理解，也为微观世界蒙上了神秘的色彩。人类把微观粒子具有的那些神奇的属性统称为量子态特性。量子态的特性包括量子的“波粒二象性”、量子态叠加性、量子态纠缠、量子态不可克隆等所谓的量子相干的特性。量子计算和量子通信正是建立在这些量子态特性之上，充分利用量子相干性的独特性质，探索以全新的方式对信息进行计算、编码和传输的可能性，它们也是量子信息学研究的目标之一。摩尔定律预示着计算机芯片的集成度不久将会达到它的极限尺寸，所以突破芯片元件尺寸的极限是当前计算机科学和信息科学所面临的一个重大科学问题。量子信息的研究可为突破芯片的极限尺寸提供新概念、新思路和新途径。利用量子态相干性可实现超高速并行计算、以量子态方式实现信息通信，可以实现不可解密码通信及超高速的信息通信。

第1章 量子信息与量子计算的基本概念

当今社会正在步入高度信息化的时代，更高速的信息传输，更快速的信息处理与更大容量的信息存储是人类永远追求的目标。20世纪微电子技术的迅速发展，大大提高了电子计算机集成电路的集成度，为现代信息化社会打下了物质基础。按照著名的“摩尔定律”，随着集成电路集成度的日益提高，电路板蚀刻精度也将越来越高，中央处理器芯片上集成的晶体管器件就会越来越密，这将迫使电路线宽不断狭窄，直至狭窄到不得不考虑运动在电路中的电子的波动性将在电路中产生新的物理现象——即量子效应时（当电路线宽小于0.1微米），现有的芯片制造理念及技术将达到极限。随着社会的进步和科技的发展，进入21世纪，面对信息科学、计算机科学、社会高度信息化，我们将直面学科发展、社会需求所带来的值得关注的、需要研究的、亟待解决的若干重要课题：电子计算机是否存在极限运算速度？进而能否实现不可破译、不可窃听的保密通信？近年来，物理学者加入了解决这些问题的研究行列，他们设想用微观粒子作为信息的载体，制作利用量子效应工作的电子元件，在量子力学理论之上研究信息的行为，成功地将量子理论和信息科学结合起来，孕育出量子信息学理论，为信息科学的持续发展开创了新的空间。

利用微观粒子的状态表示的信息就称为量子信息。信息一旦量子化，描述“原子水平上的物质结构及其属性”的量子力学特性便成为描述信息行为的物理基础，在此基础上研究信息的存储、传输和处理的一般规律的学科称为“量子信息学”。量子信息学是量子力学与经典信息学结合的新兴学科，微观系统的量子特性为信息学带来许多令人耳目一新的现象，在信息的表示、加工、处理和传输上产生一些新的概念、原理和方法，量子信息与量子通信将在未来的信息与通信的研究领域具有独特的不可替代功能，发挥重要的作用。

以量子（微观粒子）状态载荷信息，实现信息存储，遵从量子力学规则实施信息的处理与传输。量子信息的研究不断爆出惊人的结果，揭示出超越经典信息学与量子力学两个理论体系本身所包含内容预想不到的全新概念，完成了现代信息科学中以下两个根本性的发现：

（1）将经典信息0和1（Shannon information）映射到量子状态上，依照量子

状态的特性对信息实施存储、传输和处理，此时出现(科学家发现)了若干基于经典信息理论认为是不可能的“信息机能”，例如信道容量的超加法性等。

(2) 将量子状态的构造定义为量子信息，量子信息的定量化用 qubit 表示。遵从量子力学规则存储、处理和传送量子信息，此时科学家观察到了量子力学预见的、但迄今为止宏观世界无法想像的有关量子计算机以及量子远程瞬间传送(teleport)实现信息通信等科学技术。

这两个根本性的发现在提高计算机信息的处理速度、增大信息的存储容量、确保信息的网络状态安全、实现不可破译、不可窃听的保密通信等方面都可以突破现有的经典信息通信系统的极限，并将为信息科学与通信技术带来根本性的重大突破，为计算机科学与技术的可持续发展开辟了崭新的空间。基于量子信息学理论的量子通信技术和量子计算机技术将会成为 21 世纪带给人类完美的礼物，对于改善人类的生活质量、保护地球环境、保卫国家安全、保证经济增长等都具有很大潜力。当前，量子计算机、量子通信与量子密码技术等已经成为量子信息学应用研究的热点，并已取得了重要进展。

1.1　量子信息

在介绍量子信息理论的有关内容之前，我们首先简单介绍量子信息理论与量子计算理论中的基本术语、符号及其相关概念。

1.1.1　量子

量子最早出现在光量子理论中，是微观系统中能量的一个力学单位。现代物理将微观世界中所有的微观粒子(如光子、电子、原子等)统称为量子。普朗克于 1900 年在有关黑体辐射问题研究中提出“物质辐射(或吸收)的能量只能是某一最小能量单位的整数倍数”的假说，称为量子假说。假说的含义是：对于一定频率 ν 的电磁辐射，物体只能以此最小单位吸收或发射它(由此可见微观世界物质的能量是不连续的)。换言之，吸收或发射电磁辐射只能以“量子”方式进行，每个“量子”的能量为

$$\varepsilon = h\nu$$

式中 h 为一个普适常量。这种吸收或发射电磁辐射能量的不连续性的概念，在经典力学中是无法理解的。

微观世界中量子具有宏观世界无法解释的微观客体的许多特性，这些特性集中表现在量子的状态属性上，如量子态的叠加性、量子态的纠缠、量子状态的

不可克隆、量子的“波粒二象性”以及量子客体的测量将导致量子状态“波包塌缩”等现象。这些奇异的现象来自于微观世界中微观客体间存在的相互干涉，即所谓的量子相干特性。

利用微观粒子的量子态叠加及相干特性能够实现未来计算机超高速并行计算；利用微观粒子的量子态纠缠、量子态不可克隆的力学特性能够实现超高速的信息传送，实现不可破译、不可窃听的保密通信。

1.1.2 量子信息

利用微观粒子状态表示的信息称为量子信息。量子信息学是指以量子力学基本原理为基础，通过量子系统的各种相干特性(如量子并行、量子纠缠和量子不可克隆等)，研究信息存储、编码、计算和传输等行为的理论体系。

量子信息的载体可以是任意两态的微观粒子系统。例如，光子具有两个不同的线偏振态或椭圆偏振态，恒定磁场中原子核的自旋，具有二能级的原子、分子或离子，围绕单一原子旋转的电子的两个状态(如图 1－1 所示)等。这些微观粒子构成的系统都是只有量子力学才能描述的微观系统，传递和处理载荷在它们之上的信息必定具备量子特征的物理过程。

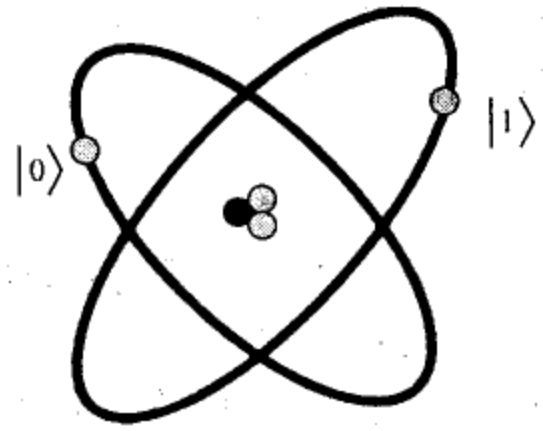


图 1－1 具有两个电子层面的原子可以表示量子信息

图 1－1 表示的原子模型中，具有两个层面的电子既能稳定在所谓的“基本”(ground)状态又能稳定在所谓的“激活”(excited)状态，我们分别把这两种状态称为一个电子的两个极化状态，并用状态$|0\rangle$和状态$|1\rangle$分别表示。在这个微观系统中，如果将一束具有适当能量的光以适当长的时间照射在这个原子上，我们就能够将状态$|0\rangle$改变成状态$|1\rangle$，反之亦然。有趣的现象是可以通过减少光的照射时间，使这个电子从最初状态$|0\rangle$向状态$|+\rangle$的改变过程中定位在状态$|0\rangle$和$|1\rangle$的任意中间状态。利用量子的某一状态表示信息时，我们就说是信息量子化了并称为量子信息。

信息一旦量子化，描述“原子水平上的物质结构及其属性”的量子力学特性便成为量子信息的物理基础。此时由于信息载体（量子）的微观特征，量子化的信息也变得多姿多彩。这些微观特征主要表现在：① 量子态相干性：微观系统中量子间相互干涉的现象成为量子信息诸多不可思议特性的重要物理基础；② 量子态纠缠性：N（大于 1）个量子在特定的（温度、磁场）环境下可以处于较稳定的量子纠缠状态，对其中某个子系统的局域操作会影响到其余子系统的状态；③ 量子态叠加性：量子状态可以叠加，因此量子信息也可以叠加，所以可以同时输入或操作 N 个量子比特的叠加态；④ 量子不可克隆定理：量子力学的线性特性确保对任意量子态无法实现精确的复制，量子不可克隆定理和测不准原理构成量子密码技术的物理基础。

利用量子信息实现通信的过程是使每一个微观粒子，通过自身的物理特性携带经典信息 0 和 1 的叠加信号后实现的数据传输的技术。事实上，经典计算机也是量子力学的产物，它的器件也利用了诸如量子隧道现象等量子效应。但仅仅应用量子器件的信息技术，并不等于现在所说的量子信息。目前的量子信息主要是基于量子力学的相干特征，重构信息密码、信息计算和信息通信的基本原理。

1.1.3　量子信息的基本存储单元及其特性

相对于经典信息的基本存储单元比特（bit），量子信息的基本存储单元称为量子比特（qubit）。在经典信息处理过程中，记述经典信息的二进制存储单元比特由经典状态 1 和 0（如电压的高低）表示。从物理角度讲，比特是个两态系统，它可以制备为两个可识别状态中的一个。

对于量子信息而言，记述量子信息的存储单元称为量子比特。一个量子比特的状态是一个二维复数空间的向量，它的两个极化状态 $|0\rangle$ 和 $|1\rangle$（参见图 1-1）对应于经典状态的 0 和 1。

在量子力学中使用迪拉克标记“$\langle|$”和“$|\rangle$”表示量子态。英文中括号叫 bracket，迪拉克把符号“$\langle\cdot|\cdot\rangle$”① 拆成两半：bra 和 ket，分别用来称呼括号的左半“$\langle x|$”和右半“$|y\rangle$”，bra 和 ket 在中文中分别译作左矢（左向量）和右矢（右向量）。“$\langle|$”和“$|\rangle$”是量子力学中表示量子状态的标记。

量子比特的重要特性在于一个量子比特可以连续地、随机地存在于状态 $|0\rangle$ 和 $|1\rangle$ 的任意叠加状态上。

由于量子效应在微观世界中会鲜明地凸现出来，因此量子比特与经典比特

注：①量子物理中表示一个光子的偏振态沿某方向分解的概率幅。

的不同在于：一个量子比特能够处在既不是$|0\rangle$又不是$|1\rangle$的状态上，而是处于状态$|0\rangle$和$|1\rangle$的一个线性组合的所谓中间状态之上，即处于状态$|0\rangle$和$|1\rangle$的叠加态上。

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.1}$$

这里的α和β为任意复数，且必须满足归一化要求$\alpha\alpha^* + \beta\beta^* = 1$。处于两种状态$|0\rangle$和$|1\rangle$叠加态的粒子系统就是量子信息的基本存储单元——量子比特(qubit)。图1-2表现的几何图形对于我们想像一个复杂量子比特会有帮助。因为$|\alpha|^2 + |\beta|^2 = 1$，我们可以将等式(1.1)改写成如下形式：

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{1.2}$$

式中$-\pi \leqslant \theta \leqslant \pi$，$0 \leqslant \varphi \leqslant 2\pi$，$x = \sin\theta \times \cos\varphi$，$y = \sin\theta\sin\varphi$，$z = \cos\theta$。显然$\theta$和$\varphi$在单位三维球体上定义了一个点，这个球体通常称为布洛赫球。布洛赫球提供了非常直观实用的单个量子比特纯状态可视化的几何表示，我们常常利用布洛赫球作为测评量子计算和量子信息有关新设想的绝好平台。

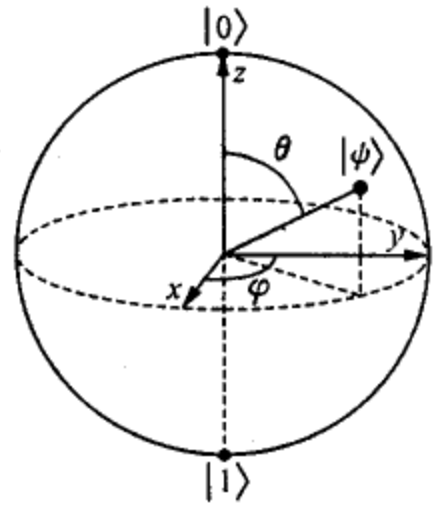


图1-2 一个量子比特的布洛赫球表示法

由等式(1.1)和图1-2可知，一个量子比特可以连续地、随机地存在于状态$|0\rangle$和$|1\rangle$的任意叠加态上，直到它被某次测量退化为止(量子物理指出测量粒子运动会导致“波包塌缩”，使被测量的量子比特状态以某一概率区间值退化到状态$|0\rangle$或$|1\rangle$上)。例如，一个量子比特能够处在以下状态：

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

当测量这个量子比特时，测量的瞬间其50%($|1/\sqrt{2}|^2$)的结果是0，还有50%($|1/\sqrt{2}|^2$)的结果是1。由此可见，一个量子比特在每种状态上出现的概率$p = |c|^2$是由复系数$c = \alpha$、β确定的。需要指出，这种的叠加态具有明显的量子相干特征，经典概率$p = |c|^2$不足以描写这个叠加态，α和β相对的位相在量子信息过程中起着至关重要的作用。

量子比特存储量子态表示信息是量子信息的出发点。量子力学理论描述量子信息的行为。薛定谔方程制约着量子态信息每一步演变，线性代数的幺正变换约束着可逆的量子态信息计算；量子信息的传输是由量子通道端点上量子纠缠集合状态的变化，结果信息的获取便是在得到输出态之后，量子计算机对输出

态进行一定的测量后给出的结果。

1.1.4　线性代数中的量子符号及其运算的简介

量子力学理论是线性的，因此在本书中我们使用线性代数中有关量子力学的标准符号与概念。我们已知在量子力学态矢空间中使用标准符号$|\Psi\rangle$描述向量，且用 0 表示该向量空间的零向量，因此对于任意的$|v\rangle$，下列等式成立：

$$|v\rangle + 0 = |v\rangle$$

一个向量空间的生成集合是一个向量集合$\{|v_1\rangle, \cdots, |v_n\rangle\}$，该向量空间中的任意向量$|v\rangle$都能够写成这个生成集合的线性组合 $|v\rangle = \sum_i a_i |v_i\rangle$。例如，向量空间 C^2 的生成集合是

$$|v_1\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}; \quad |v_2\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

因此 C^2 中的任意向量

$$|v\rangle \equiv \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$$

能够写成$|v_1\rangle$和$|v_2\rangle$的线性组合 $|v\rangle = a_1|v_1\rangle + a_2|v_2\rangle$。我们说$|v_1\rangle$和$|v_2\rangle$生成向量空间 C^2。

式(1.3)给出了一个 m 维向量与 n 维向量的张量乘积的矩阵表示。张量乘积是线性代数的基本运算。

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} \otimes \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1 b_1 \\ \vdots \\ a_1 b_n \\ a_2 b_1 \\ \vdots \\ a_2 b_n \\ \vdots \\ a_m b_n \end{bmatrix} \tag{1.3}$$

表 1－1 给出了线性代数中表述量子力学中量的标准符号及其简要说明。

表 1-1 线性代数中的一些量子力学标准符号

符 号	说 明
z^*	复数的复变换。$(1+\mathrm{i})^* = 1-\mathrm{i}$
$\|\Psi\rangle$	矢量，也称为 ket
$\langle\Psi\|$	$\|\Psi\rangle$的对偶矢量，也称为 bra
$\langle\varphi\|\Psi\rangle$	矢量$\|\varphi\rangle$和$\|\Psi\rangle$的内积
$\|\varphi\rangle\otimes\|\Psi\rangle$	矢量$\|\varphi\rangle$和$\|\Psi\rangle$的张量积
$\|\varphi\rangle\|\Psi\rangle$	矢量$\|\varphi\rangle$和$\|\Psi\rangle$的张量积的简写
A^*	矩阵 A 的复共轭
A^T	矩阵 A 的转置
A^H	矩阵 A 的埃尔米特变换或称为矩阵 A 的伴随 $A^H = (A^T)^*$，$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^H = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$
$\langle\varphi\|A\|\Psi\rangle$	矢量$\|\varphi\rangle$和 $A\|\Psi\rangle$的内积，等于矢量 $A^H\|\varphi\rangle$和$\|\Psi\rangle$的内积

1.1.5 量子态叠加与量子态纠缠(纠缠态)

量子态的叠加性源于微观粒子“波粒二象性”的波动“相干叠加性”(一个以上的信息状态累加在同一个微观粒子上的现象)；量子纠缠状态(entangled state)指的是两个或多个量子系统之间的非定域、非经典的关联，是量子系统内各子系统或各自由度之间关联的力学属性(一个以上的微观粒子因微观系统的特性相互交缠在一起的现象)。量子态可以叠加的物理特性是实现量子并行计算的基础；量子态能够纠缠是实现信息高速的不可破译通信的理论基础，它们都是量子信息理论中特有的概念。

(1) 量子态的矩阵表示

例：一对量子比特

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} 和 |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

能够组成 4 个不重复的量子比特对$|00\rangle$，$|01\rangle$，$|10\rangle$，$|11\rangle$，它们张量积的矩阵

表示如下：

$$|00\rangle \equiv |0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{bmatrix}1\times\begin{pmatrix}1\\0\end{pmatrix}\\0\times\begin{pmatrix}1\\0\end{pmatrix}\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$$

$$|01\rangle \equiv |0\rangle \otimes |1\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{bmatrix}1\times\begin{pmatrix}0\\1\end{pmatrix}\\0\times\begin{pmatrix}0\\1\end{pmatrix}\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

$$|10\rangle \equiv |1\rangle \otimes |0\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{bmatrix}0\times\begin{pmatrix}1\\0\end{pmatrix}\\1\times\begin{pmatrix}1\\0\end{pmatrix}\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}$$

$$|11\rangle \equiv |1\rangle \otimes |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{bmatrix}0\times\begin{pmatrix}0\\1\end{pmatrix}\\1\times\begin{pmatrix}0\\1\end{pmatrix}\end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

很显然，集合{|00⟩，|01⟩，|10⟩，|11⟩}是四维向量空间的生成集合。

(2) 量子态叠加与量子态纠缠

量子态的纠缠是量子系统内各子系统或各自由度之间关联的属性。经典系统内也有此关联，但它反映在概率不相乘上，而量子态的纠缠却反映在概率幅不相乘上。概率幅的叠加表现出量子力学特有的干涉现象，概率幅的纠缠将对量子干涉产生重要的影响。

当量子比特列的叠加状态无法用各量子比特的张量乘积表示时，这种叠加状态就称为量子纠缠状态。例如，有一量子叠加状态

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

由于其最后一位量子比特位都是|0⟩，因此能够将它写成量子比特 $(1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle)$ 与量子比特|0⟩的乘积：

$$\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)|0\rangle$$

但是，对于下列的量子叠加状态：

$$\frac{1}{\sqrt{2}}|01\rangle+\frac{1}{\sqrt{2}}|10\rangle$$

无论采用怎样的方法都无法写成两个量子比特的乘积。这个叠加状态就称为量子纠缠状态。

量子纠缠状态是量子信息理论中特有的概念，尽管处在纠缠的两个或多个量子系统之间不存在实际物质上的联系，但不同的量子位却会因为纠缠而彼此影响。正是由于“纠缠”的神秘性，使得一个量子的状态将同与之发生纠缠的另一个量子的状态相关，似乎在它们相互之间的关联性比紧密结合的两个原子还强。

说到量子状态叠加与并行处理的关系，现用以下两个简单的例子粗略地介绍一下：例如十进制数 10 和 5，若用量子比特来表示，则可分别写成

$$|10\rangle\rangle_{10}\equiv|1010\rangle=|1\rangle\otimes|0\rangle\otimes|1\rangle\otimes|0\rangle$$

$$|5\rangle\rangle_{10}\equiv|0101\rangle=|0\rangle\otimes|1\rangle\otimes|0\rangle\otimes|1\rangle$$

取它们的叠加态就得到如下的表示：

$$\begin{aligned}&|10\rangle\rangle_{10}+|5\rangle\rangle_{10}=|1010\rangle+|0101\rangle\\&=|1\rangle\otimes|0\rangle\otimes|1\rangle\otimes|0\rangle+|0\rangle\otimes|1\rangle\otimes|0\rangle\otimes|1\rangle\end{aligned}$$

针对它们的叠加态可以利用量子算法同时处理十进制整数的 10 和 5。显然，状态的各量子位是纠缠态，可以对这个叠加状态实施各种运算，其结果如同同时对 10 和 5 进行计算，最后通过测量即可分别获得 10 和 5 的计算结果，实现两个数物理上的并行计算。

更进一步，如果打算同时计算一个函数 $f(x)$在 $x=x_1, x_2, \cdots, x_n$ 一系列位置上的取值，也可以取更复杂的纠缠态。例如，设置 x 和 $y=f(x)$ 为两个存储器，他们的量子态分别为$|x\rangle\rangle$和$|f(x)\rangle\rangle$，则下列纠缠态就包含了该函数整体上的信息：

$$\begin{aligned}&\sum_{i=1}^{n}|x_1\rangle\rangle\otimes|f(x_1)\rangle\rangle\\&=|x_1\rangle\rangle\otimes|f(x_1)\rangle\rangle+|x_2\rangle\rangle\otimes|f(x_2)\rangle\rangle+\cdots+|x_n\rangle\rangle\\&\quad\otimes|f(x_n)\rangle\rangle\end{aligned}\tag{1.4}$$

对它实施各种运算，就如同并行计算一个函数 $f(x)$在 $x=x_1, x_2, \cdots, x_n$ 一系列位置上的函数值。由此可见，量子叠加状态是实现真正物理意义上并行

计算的物质基础。

1.2　量子通信与量子加密

量子通信系统由量子态产生器、量子通道和量子接收设备组成。可以说它是光纤通信技术的一种，只不过其量子信道利用光的量子特性，让一个个光子传输 0 和 1 的信息。量子通信技术按其所传输的信息是经典还是量子而分为两类，前者主要用于量子密钥的传输，开发无法破译的密码；后者则是量子瞬间传送(teleport)，一种令人难以置信但在量子世界里确实可行的瞬间远距离“实物”传输技术。

量子密码学是密码学与量子力学结合的产物。密码的关键在于密钥，早期是暗密钥，即传送者和接收者要事先知道密钥才能阅读对方的信息。其缺点是在传输过程中，密码可能被第三者不留痕迹地窃取且破解。而目前常用的加密设备，通常用一较大的质数作公用密钥，它没有被窃取的可能，破解的关键在于求一个很大整数的质因数。如前所述，以一个四百位数的整数来说，要求得其质因数，最快的计算机大概要花上数十亿年的时间。因此，这样的安全机制几乎被视为是无法破解的。然而，利用量子计算机能够在短时间内找出超大整数的质因数，这样，一旦研发出量子计算机，对现代的金融甚至国防安全体系就会带来很大的威胁。

如何使信息传输快速、方便而又安全，是信息科学的主要课题。早在 1970 年，美国科学家威斯纳(S. Wiesner)就提出如何将量子特性用于密码科学，利用单量子态制造不可伪造的“电子钞票”。这个构想因量子态的寿命极短而无法实现，但却让 IBM 的贝内特(C. Bennett)博士和加拿大学者布拉萨德(G. Brassard)想到可将单量子态用于传送信息。量子密码技术并不用于传输密文，而是用于建立、传送解码本。根据量子力学的测不准原理，任何观测都会立刻改变系统的状态，因此，任何窃听者都会被发现，从而保证解码本的绝对安全，也就保证了加密信息的绝对安全。

最初的量子密码通信利用的是光子的极化特性，目前主要的方法则用光子的相位(纠缠态)特性进行编码。简单地说，如果传送者 A 先传送一组随机比特序列给接收者 B，此随机比特序列是以偏极光子或纠缠态光子来表示，随后 A 再与 B 沟通，以便确立解码本。在后来的沟通过程中，即使被窃听者 C 听到，C 也无法知道光子的状态。如果 C 试图去拦截光子，由于不知道光子的状态，会得到错误消息。甚至，光子的状态会因为 C 的观测而改变，这时，A 与 B 便会察觉 C 的存在。解码本确立之后，便可按照解码本来加密资料并传送。

量子密码的优点是可检查解码本是否被盗用。当然，环境噪声也有可能破坏解码本中的比特而留下痕迹，因此量子密码必须以所有机器正常运作为前提，如何在有光源噪声的环境下也能正常运作，是量子密码实用化所面临的最大难题。

量子信息在通信领域最奇妙的应用应该是量子瞬时传输，即脱离实物的一种实物信息传送，其基本想法是：先提取原物所有的信息，类似扫描一样，在这过程中同时将原物体毁掉，然后将这些信息传送到接收地点，接收者依据这些信息制造出完全相同(具有相同微观结构)的三维空间原物体。但是，根据量子力学的测不准原理，越精确的测量或扫描，越容易在扫描过程中改变原物体微观粒子的量子状态，这样在提取原物体的全部信息前，原物体可能已面目全非了。因此，长期以来，量子瞬时传送不过是一种幻想而已。

直到上世纪 90 年代初，包括贝内特博士在内的六位科学家提出了利用经典与量子相结合的方法来实现量子瞬时传输：将原物体的信息分成经典信息和量子信息两部分，经典信息是发送者对原物体进行某种测量(扫描)而提取原物体的一部分信息，量子信息是发送者在扫描中留下未测量的信息；经典信息和量子信息分别经经典通道和量子通道传送，接收者获得这两种信息后，就可以备制出原物体量子态的完美复制品。该方案中最关键的地方是量子信息部分的传送，发送者甚至对这部分量子信息一无所知，因此量子信息部分的传送，是接收者利用一对纠缠光子态，通过将其中的一个光子备制到原物体的量子态上来提取原物体的信息，并非由发送者传送给接收者，从而保证信息的完整性。

利用一对纠缠态光子实现瞬时传输的物理基础在于量子力学(纠缠态)的非定域特性。量子力学的非定域性是指一旦两量子系统的状态(比如两光子的极化态)构成纠缠态(例如 $|00\rangle+|11\rangle$)，则不管后来这两个量子系统间的距离被分隔多远，且它们之间可能不再有力学上的交互作用，但只要仍保持在纠缠态，它们之间超强的量子关联性就不会改变。早在 20 世纪 30 年代，伟大的科学家爱因斯坦对量子态的这种远距离关联性提出了质疑，即著名的爱因斯坦-波渡斯基-罗逊(Einstein - Podolsky - Rosen，简称 EPR)谬论，他认为自然界不可能存在这种非定域的现象，一定是量子力学在某个地方出错了。直到 30 年后，贝尔(J. S. Bell)证明爱因斯坦的定域性观念与量子力学是不兼容的(贝尔定理)，20 世纪 70 年代许多实验进一步证实了量子态的非定域性。但即使量子态的这种非定域性确实存在，人们认为这种超距离的量子关联特性并不具真正的实用意义，因为这种非定域关联并不直接传送信息。直到量子瞬时传输实现后，人们对量子力学的非定域性所展现出来的神奇效应才有了更深入的认识。

量子瞬时传输不仅对人们认识量子力学的神秘规律具有重要意义，而且可以用量子态作为信息载体，通过量子态完成大容量信息的瞬时传输，并具有原则

上无法破解的量子保密通信功能。1997 年，奥地利学者塞林革(A. Zeilinger)和合作者在国际上首次完成了未知量子态的远距传输，成功地将一个量子态从甲地的极化光子传送到乙地的极化光子上。实验中传送的只是表达量子信息的“状态”，作为信息载体的光子本身并不被传送。随后，美国加州理工学院的肯保(H. J. Kimble)教授和合作者用光的压缩态，成功地将一束光从一个房间转移到另一个房间。为了进行远距离的量子态瞬时传输，必须让相距遥远的传送和接收两个系统一直保持在纠缠状态。但由于各种不可避免的环境噪声，使量子纠缠态的纠缠性随传输距离的增加而变得越来越差。因此，如何保持量子纠缠态的纯度是目前量子通信研究中的难题。

总而言之，量子信息技术在计算速度、通信安全、信息容量等方面，可远远突破传统信息系统的极限。量子计算机具有超强的平行计算能力，能够解决传统计算机难以解决的许多重要问题。虽然当前量子信息无论在理论上还是实验上都不断地获得重要的突破，但是想要有效地制备和操作实用的量子信息系统，还是相当困难的。

1.3　量子计算

物理学家费曼(R. P. Feynman)生前曾认真地研究过用量子力学理论，实现量子计算并构建量子计算机。费曼的构想虽然在当时引起了部分科学家很大的兴趣，但大家对量子计算的概念基本上停留在“原则上可行”的状态，原因之一是由于量子态的测不准性质和量子系统容易受噪声干扰，使量子运算很容易出错。1994 年，量子计算的基本问题取得突破性的进展。美国电话电报公司(AT&T)计算机专家苏尔(P. Shor)证明量子计算机能快速地进行大因数分解，他还发展出第一套量子算法编码。但是这靠传统计算机是无法有效实现的，从而使量子计算机的研究进入实验时代。

简单地说，量子计算就是利用量子态进行信息处理的方法，其实体设备称为量子计算机。量子计算机的基本原理就是通过量子力学的运用，将微晶体管压缩到原子般大小，然后在极小的面积上放入数十亿颗量子微晶体管，进而利用量子态的叠加性和相干性进行信息运算、保存及处理。

在传统计算机中，运算对象是各种比特序列，在量子计算机中，运算对象是量子比特序列，所不同的是，量子比特序列可以处在各种正交态的叠加态上。以一个由 3 比特组成的序列为例，可以用 8 个三位二进制数表示：000，001，010，…，111，分别代表 0 到 7 这 8 个数字。由这三位比特序列构成的经典存储器每次只能记录这 8 个数字中的一个，但量子存储器可以在同一时刻以量子叠加态

同时记录这 8 个不同的数字，这意味着用更多的量子比特组成的存储器，其存储信息的能力将呈指数增加。4 个量子比特可同时存储 16 个不同的数字，n 个量子比特可同时存储 2^n 个数字。换句话说，在相同比特位数下，量子计算机记录信息的容量是目前传统计算机的 2^n 倍。用 300 量子比特就能存储比已知宇宙中所有原子的总数还要多的数字。

另一方面，计算机运算是由逻辑门电路做基本组件的，而量子计算机则由量子逻辑门电路构成其运算组件。与传统计算机不同的是，量子计算机中的量子逻辑组件对应于数学上的一个幺正变换矩阵。例如，量子逻辑门不仅可以将$|0\rangle$态和$|1\rangle$态做交换，还可以将$|0\rangle$态和$|1\rangle$态变为它们的任意叠加态。

更为关键的是，量子计算会将存储器内的量子比特变换为纠缠态。量子纠缠指的是两个或多个量子系统之间具有的非经典的强关联。例如，两个量子比特可构成纠缠态（$|00\rangle+|11\rangle$），其特性是它不能被分解为两个单独量子比特状态的乘积。因此，纠缠态内量子比特间具有很强的相干性或关联性，其中一个量子比特状态被改变或测量时，也决定了纠缠态内所有其他比特状态的相应变化，这类特殊量子态提供了量子平行处理的可行性。量子平行处理就是对量子态每一叠加分量进行幺正变换，所有这些变换在同一时刻一次完成，并按一定的概率幅叠加起来得出结果。一台 32 个量子比特的计算机，其能力相当于 40 亿台传统计算机作平行运算。如果求一个 400 位的数字的所有质因数，目前最快的计算机大概要花上数十亿年的时间，而量子计算机只需要几分钟的时间。

除了进行平行计算外，量子计算机的另一重要用途是模拟量子系统。虽然现在的计算机已被广泛用来解各种复杂的量子力学问题，但正如费曼先生生前指出，用传统计算机模拟真实的量子演化过程是不切实际的，因为用一般计算机模拟量子系统所需的时间随系统的大小呈指数增长。另一方面，传统计算机中的随机变量都是虚假的，而量子态是一种真正的随机分布，量子计算机内的运算过程本身就是量子态的一个变换过程，因此只有量子计算机能瞬间模拟量子系统的演化。

不管是量子平行计算还是量子模拟计算，本质上都是利用量子纠缠态特有的相干性。但在实际系统中，量子纠缠态很难维持。在量子计算机中，由于量子比特是由原子或其他微粒子系统所构成，很容易受外部环境影响，导致量子相干性的消失，称为退相干，从而使运算容易产生错误结果。要使量子计算成为现实，最重要的问题就是克服这种退相干，其最有效的方法是在发生退相干前完成运算，或用误差修正的方法消去因退相干引起的错误。前者依赖于纠缠态的寿命，一般说来，一个量子信息由产生到消失的时间只有十亿分之一秒；而后者是同时做几种相同的运算，并不断对相应状态做比较，发生偏差时及时修正，但这

样的方法会降低运算效率。如何保持纠缠态不衰减，或当纠缠态发生偏差时及时修正，是目前量子信息研究中最基本且亟待解决的问题。

1.4　经典解读

在学习量子信息理论的有关内容之中，我们会遇到一些量子力学的经典术语，它们的背后涉及到一些有趣的概念，我们将用有限的篇幅做一个简单的通俗易懂的介绍。

1.4.1　薛定谔猫与 EPR 佯谬

20 世纪的前四分之一的时间中，人们逐渐发现微观客体（光子、电子、质子、中子等）既有波动性，又有粒子性，即所谓“波粒二象性（wave－particle dualism）”。“波动”和“粒子”都是经典物理从宏观世界里获得的概念，在人们的认知和常识的范畴之内，容易直观地理解它们。然而，微观客体的行为与人们的日常经验相差甚远，对每一个观察者来说显得十分的“怪诞”和“神秘”，很难顺理成章地接受。微观粒子的波粒二象性告诉我们：微观客体既是粒子也是波，它是粒子和波两象性矛盾的统一。此时波虽不再是经典概念下的波，但它却具有波动性中最本质的东西——波的“相干叠加性”；粒子也不再是经典概念下的粒子，因为它不满足“粒子有确切轨道”的属性，但它却具有粒子运动最本质的现象——粒子的直线运动与反射。由于微观粒子的波粒两象性使得人们不得不引入波函数 $\Psi(r)$（量子态）来描述它们的状态。

由于微观粒子的波动呈现出它运动的一种统计规律，因此称此波动为概率波（probability wave）。波函数 $\Psi(r)$ 的绝对值的平方等于粒子在点 r 附近出现的概率 p：

$$p(r) = \Psi^*(r)\Psi(r) = |\Psi(r)|^2$$

也就是说，$|\Psi(r)|^2\Delta x\Delta y\Delta z$ 代表在点 r 附近的小体积元 $\Delta x\Delta y\Delta z$ 中找到粒子的概率，因此也称 $\Psi(r)$ 为概率波幅（probability amplitude）。$\Psi(r)$ 是量子力学里最基本、最重要的概念。$\Psi(r)$ 是复数，它含有模 $|\Psi(r)|$ 和相位 $\varphi(r)$ 两部分

$$\Psi(r) = |\Psi(r)|\,e^{i\varphi(r)}$$

著名物理学家费曼曾指出：量子力学的精妙之处在于引入概率波幅（即量子态）的概念。事实上，微观世界千奇百态的特性正是起源于这个量子态，而关于量子力学理论是否完备的 EPR 佯谬长期激烈争论的焦点也在这个量子态上。在量子力学近百年的学术争论中，影响最大的就是薛定谔于 1935 年提出的所谓

“薛定谔猫”佯谬和爱因斯坦等人在 1935 年提出的 EPR 佯谬。

(1) 薛定谔猫

图 1 - 3 刻画了所谓的“薛定谔猫”的假想实验。薛定谔设想在一个封闭容器里有个放射源和一只猫，放射源以每秒 0.5 几率释放一个粒子。换句话说，按照量子力学的叠加性原理，一秒钟后体系处于无粒子态和一个粒子态的等几率幅叠加态。一旦粒子发射出来，它将启动一传动机构落下一铁锤打破装有氰化氢的瓶子，毒气释放后会导致容器里的那只猫立刻死亡。当然，如果无粒子的发射，这一切均不会发生，猫仍然活着。现在的问题是：一秒钟后容器里的猫是死还是活？既然放射性粒子是处于 0 和 1 的叠加态，那么这只猫理应处于死和活的叠加态。这只在特定状态下的半死半活的猫就是著名的“薛定谔猫”。“薛定谔猫”的意义在于薛定谔通过这个假想实验将看不见的微观世界与我们熟悉的宏观世界联系起来，诱导观察者本能地用已有的宏观思维去考虑微观客体的行为，从而得到不可思议的结论。

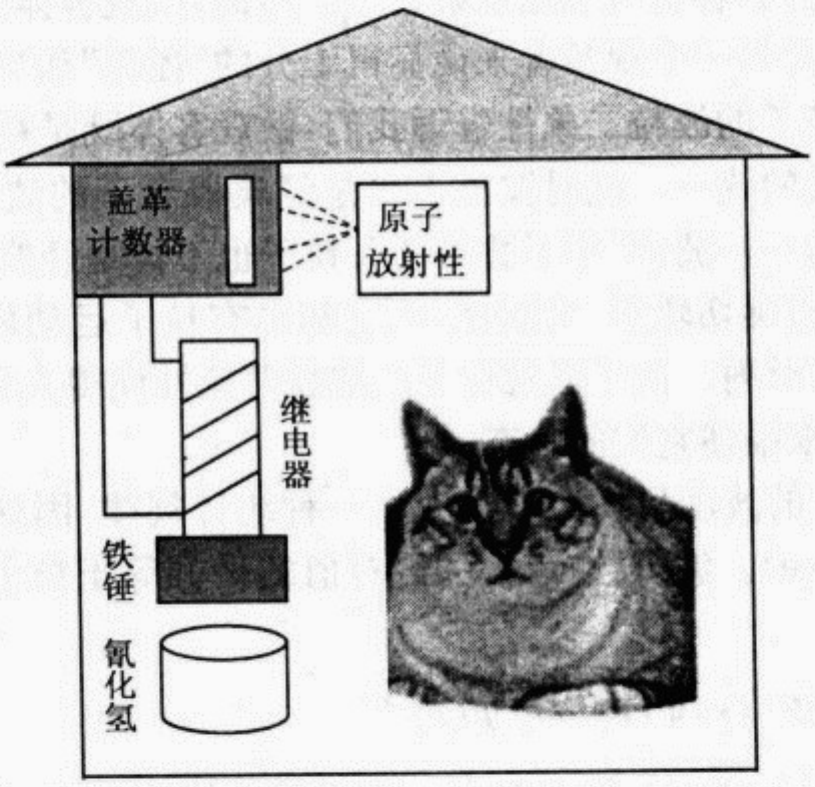


图 1 - 3 “薛定谔猫”的假想实验

在这个假想实验中，抛掉“猫”这个宏观形象表征之外，薛定谔想要阐述的物理问题是：微观世界遵从量子叠加原理，那么，如果自然界确实按照量子力学运行的话，宏观世界也应遵从量子叠加原理。薛定谔的实验装置巧妙地把微观放射源与宏观的猫联系起来，最终诞生出这只死活不定的薛定谔猫，结论似乎否定了宏观世界存在可以区分的量子态的叠加态。然而，随着量子光学的发展，人们研究各种制备宏观量子叠加态的方案，1997 年科学家终于在离子阱中观察到这种“薛定谔猫”态，即一个被观察的粒子在同一时间里处于两个不同的状态。薛

定谔的问题还可以进一步扩展为:宏观世界中是否存在量子效应? 事实上,大量实验事实都肯定地回答了这个问题。最近几年引起广泛兴趣的玻色—爱因斯坦凝聚的实验研究进展更有力地证实了宏观量子效应。

(2) EPR 佯谬

"EPR 佯谬"在近 60 多年的量子力学发展中起着重要的推动作用。这个实验是爱因斯坦等人与量子力学创始人之一的玻尔就有关量子力学是否自洽、是否完备的学术争论而引发的一系列假想实验中的一个著名的思想实验,这个思想实验所预示的结果完全遵从量子力学原理,但却令人难以接受。1935 年由爱因斯坦与波多尔斯基(B. Podolsky)、罗森(N. Rosen)联名发表一篇论文,以该思想实验结论的方式对量子力学的完备性提出了质疑。

爱因斯坦等人考虑两个粒子 A 和 B 组成的一对总自旋为零的粒子对(称为 EPR 对),两个粒子随后在空间上分开,并设想分开的距离如此之大,以至于对粒子 A 进行的任何物理操作都不会对粒子 B 产生干扰。假定将粒子 A 放在地球位置 x_1 上,而将粒子 B 放在月球位置 x_2 上,则两者之间的距离为 $a = x_1 - x_2$。如在地球上测得粒子 A 的位置为 x,就意味着测得粒子 B 的位置为 $x - a$;如在月球上测得粒子 B 的动量为 p,就意味着测得粒子 A 的动量为 $-p$;这就是说对粒子 A 的位置和动量都进行了测量,相当于对粒子 B 的同一物理量也进行了测量。量子力学(测不准原理)宣称,我们不能对粒子 A 的位置和动量同时进行精确的测量,这就是说,在测量粒子 A 位置的同时,连粒子 B 的动量也不能精确测量了。"EPR 对"理论认为若单独测量 A(或 B)的自旋,则自旋可能向上,也可能向下,各自概率为 0.5。但若地球上已测得粒子 A 的自旋向上,那么,月球上的粒子 B 不管测量与否,必然会处在自旋向下的本征态上。爱因斯坦认定真实世界绝非如此,月球上的粒子 B 决不会受到地球上对 A 测量的任何影响。因此,下列结论二者必居其一:① 存在着即时的超距离作用,在测量粒子 A 的位置的同时,立即干扰了粒子 B 的动量;② 一个粒子的位置和动量本来同时是有精确值的,只是量子力学的描述不完备。由此得出的结论是量子力学不足以正确地描述真实的世界。玻尔则持完全相反的看法,他认为粒子 A 和 B 之间存在着量子关联,不管它们在空间上分得多开,对其中一个粒子实行局域操作(如上述的测量),必然会立刻导致另一个粒子状态的改变,这是由量子力学的非局域性所决定的。

这场争论的本质在于:真实世界是遵从爱因斯坦的局域实在论,还是玻尔的非局域性理论。长期以来,这个争论一直停留在哲学上,难以判断"孰是孰非",直到贝尔基于爱因斯坦的隐参数理论而推导出著名的贝尔不等式,人们才有可能在实验上依据贝尔不等式寻找判定这场争论的依据。法国学者首先在实验上

证实了贝尔不等式可以违背，即爱因斯坦的局域实在论在微观世界不是真理，支持了玻尔的看法。之后，随着量子光学的发展，有更多的实验支持了这个结论，即宏观世界遵守贝尔不等式，而微观世界能够违背贝尔不等式。1997 年瑞士学者更直截了当地在 10 千米光纤中测量到作为 EPR 对的两个光子之间的量子关联。因此，现在可得出结论：① 量子力学是正确的(起码迄今完全与实验事实相自洽)；② 非局域性是量子力学的基本性质。现在由爱因斯坦等人在其佯谬中首先揭示的量子关联效应常被称为 EPR 效应，它是非局域性的体现。

事实上，按照量子力学理论，EPR 粒子对是处于所谓纠缠态的一对粒子，这个量子状态最大地违背贝尔不等式。它有着奇特的性质：无法单独地确定某个粒子处在什么量子态上，这个态给出的惟一信息是“两个粒子之间的相互关联”这类整体的特性。现在实验上已成功地制备出这类具有纠缠性的量子态。

1.4.2 贝尔态基与量子隐形传态

上一节说到了量子力学中有著名的贝尔不等式。爱因斯坦等人认为量子力学只给微观客体以统计性描述是不完备的，因为这样的描述不能解释微观粒子的某些行为。玻姆认为有必要引入一些附加变量对微观客体作进一步的描述，因此有了隐变量理论。贝尔源于隐变量理论推出了这个著名的不等式。由于贝尔不等式与量子力学的预言不相符，因此人们有可能通过在满足必须的条件下，实验结果是否满足不等式来判定以玻尔为代表的哥本哈根学派对量子力学的解释是否正确，即量子力学是否自洽、本身是否完备。

贝尔不等式大致给出这样的一个事实：假设两个观察者 A 和 B 分别对光子对的个别光子做偏振测量，两人可以任意选择各种不同的测量基底，假设 A 选了 a 和 a' 两种基底，而 B 选 b 和 b'。用 $E(a, b)$ 代表当 A 用基底 a 而 B 用基底 b 时，在他们重复多次同样的实验后，统计的结果“平行”与“垂直”的两种几率差(即期望值)，那么经典的理论预测总是有以下的不等式：

$$-2 \leqslant E(a, b) - E(a, b') + E(a', b) + E(a', b') \leqslant 2$$

这就是贝尔不等式。用某个算符 $\hat{B}$(称为贝尔算符)在一定量子态上的平均值将贝尔不等式表示成

$$-2 \leqslant \langle \Psi | \hat{B} | \Psi \rangle \leqslant 2$$

贝尔算符的全套本征态称为贝尔态基。贝尔态基由如下 4 个态矢组成：

$$|\beta_{00}\rangle=\frac{|00\rangle+|11\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}+\frac{1}{\sqrt{2}}\begin{bmatrix}0\\0\\0\\1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}$$

$$|\beta_{01}\rangle=\frac{|01\rangle+|10\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\0\\0\end{bmatrix}+\frac{1}{\sqrt{2}}\begin{bmatrix}0\\0\\1\\0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\1\\0\end{bmatrix}$$

$$|\beta_{10}\rangle=\frac{|00\rangle-|11\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}-\frac{1}{\sqrt{2}}\begin{bmatrix}0\\0\\0\\1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\-1\end{bmatrix}$$

$$|\beta_{11}\rangle=\frac{|01\rangle-|10\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\0\\0\end{bmatrix}-\frac{1}{\sqrt{2}}\begin{bmatrix}0\\0\\1\\0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\-1\\0\end{bmatrix}$$

贝尔态基也可以写成下列形式：

$$|\Psi^{(\pm)}\rangle=\frac{(|01\rangle\pm|10\rangle)}{\sqrt{2}}=\frac{1}{\sqrt{2}}(|0\rangle\otimes|1\rangle\pm|1\rangle\otimes|0\rangle)：\ (|\beta_{01}\rangle,|\beta_{11}\rangle)$$

$$|\Phi^{(\pm)}\rangle=\frac{(|00\rangle\pm|11\rangle)}{\sqrt{2}}=\frac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle\pm|1\rangle\otimes|1\rangle)：\ (|\beta_{00}\rangle,|\beta_{10}\rangle)$$

在科学幻想小说或电影中，有时会出现这样的场面：一个神秘人物突然在某个地方消失了，其后又在另一个地方莫名其妙地显现出来。这便是远距隐形传物(Teleportation)的概念，它仅仅是一种幻想。下面要讲的量子隐形传态(Quantum Teleportation)根据量子力学原理却是真实可行的。

所谓隐形传态指的是脱离实物的一种“完全”的信息传送。从物理学角度，可以这样来想像隐形传送的过程：先提取原物的所有信息，然后将这些信息传送到接收地点，接收者依据这些信息，选取与构成原物完全相同的基本单元，制造出原物完美的复制品。

1993 年 Bennet 等来自 4 个国家的六位科学家(如图 1－4 所示)联名发表的一篇文章中提出了量子隐形传态的设想，其原理就是利用量子态纠缠 EPR 粒子对的远程关联。六位科学家设想利用经典方法与量子理念相结合的方法实现量

子隐形传态的方案:将某个未知量子态的粒子 A 从甲地传送到乙地,将乙地的另一个粒子 B 制备到 A 的量子态上,而原来的 A 粒子仍然留在甲处。方案实现的基本思想是:由原物的信息生成经典信息和量子信息两部分,它们分别经由经典通道和量子通道传送给接收者。经典信息是由发送者对原物进行某种测量而获得的信息,量子信息是发送者在测量中未提取的其余信息;接收者在获得这两种信息后,就可以制备出原物量子态的完全复制品。该过程中传送的不是原物本身,而仅仅是原物的量子态的信息。发送者甚至可以对要传送的量子态一无所知,而接收者则是将另一个粒子备制到原物的量子态上。在这个方案中,纠缠态的非定域性起着至关重要的作用。量子力学是非定域的理论,这一点已被违背贝尔不等式的实验结果所证实,因此,量子力学展现出许多反直观的效应。在量子力学中能够以这样的方式制备这样的两个粒子——EPR 对,它们之间的关联不能被经典地解释。量子隐形传态不仅在物理学领域对人们认识与揭示自然界的神秘规律具有重要意义,而且可以用量子纠缠态作为信息传播的媒体,通过量子纠缠态的传送完成大容量信息的高速传输,和实现原则上不可破译的量子保密通信。

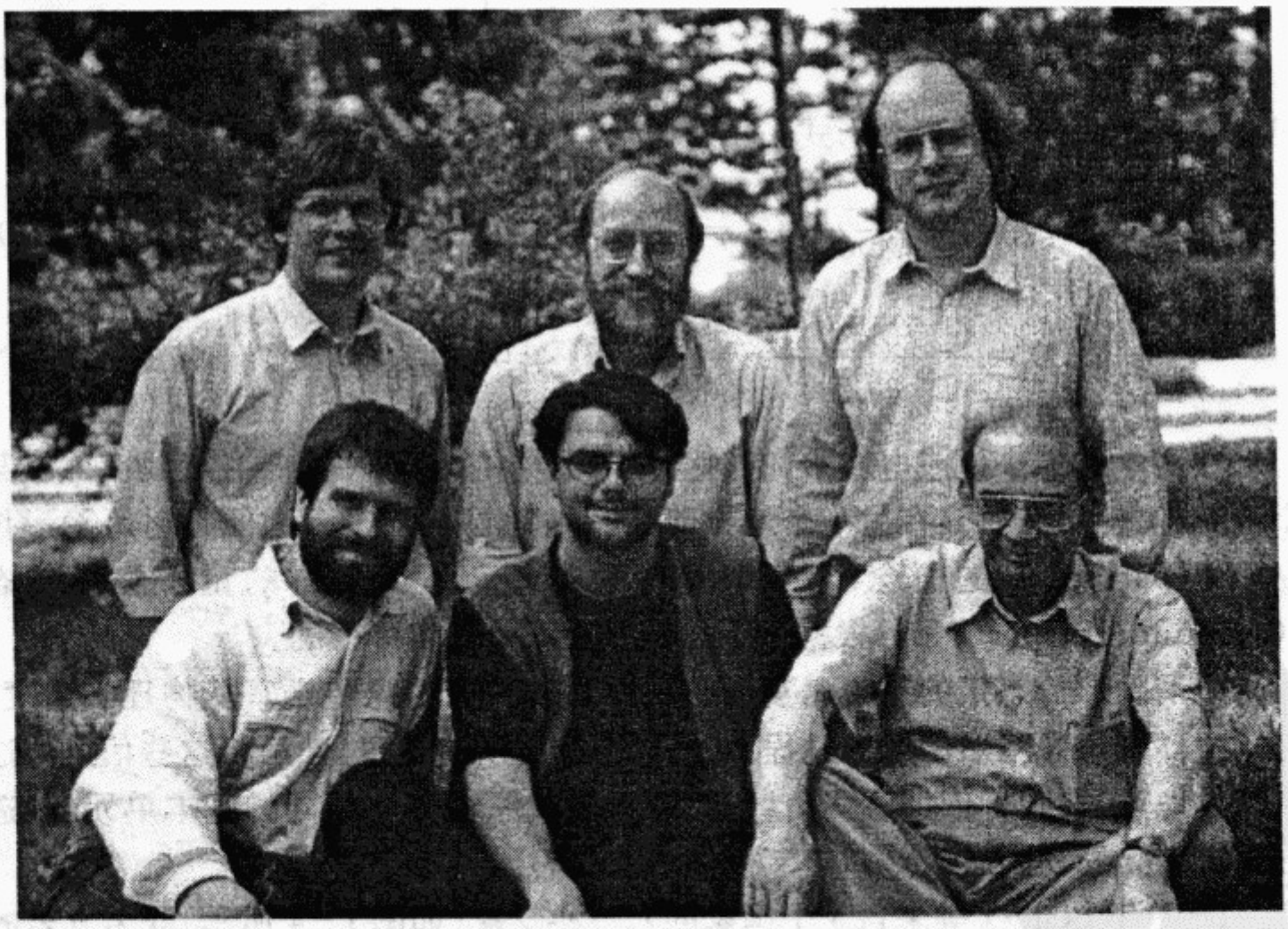


图 1-4 (top,left) Richard Jozsa, William K. Wootters, Charles H. Bennett. (Bottom left) Gilles Brassard, Claude Crépeau, Asher peres.

图 1-5 描述了量子隐形传态实验装置和量子隐形传态全过程的示意图：量子通信系统的基本部件包括量子态发生器、量子通道和量子测量装置。按其所传输的信息是经典还是量子而分为两类。前者主要用于量子密钥的传输，后者则可用于量子隐形传态和量子纠缠态的分发。

首先在 EPR 备制中心通过非线性晶体下转换器备制好 EPR 光子对（粒子 2、3 的纠缠态），并将光子 2 分发到 Alice，光子 3 分发到 Bob 处；将所要传递的信息通过起偏器体现在光子 1 的量子态中。然后将光子 1 和 2 通过光分束器产生纠缠，随即发生纠缠交换。然后Alice测量并判断粒子（1、2）处于哪个贝尔纠缠态，并向 Bob 通过经典信道传送测量结果。最后 Bob 通过偏振分析器和两个光子检测器来测量光子 3 的偏振态，即可获知光子 1 所加载的信息。其中信息是分经典信息和非经典信息两部分传递的：① 通过经典信道传送的经典信息是 Alice 所测得（1、2）粒子的贝尔态；② 通过 EPR 粒子对的纠缠态瞬间传递的非经典信息是 Bob 所得到的粒子 3 的量子态。所以全过程不可能在类空距离上传递，因果律并未遭到破坏。此外，在整个过程中第三者绝对不可能“偷听”，因此通信的保密性是绝对可靠的。

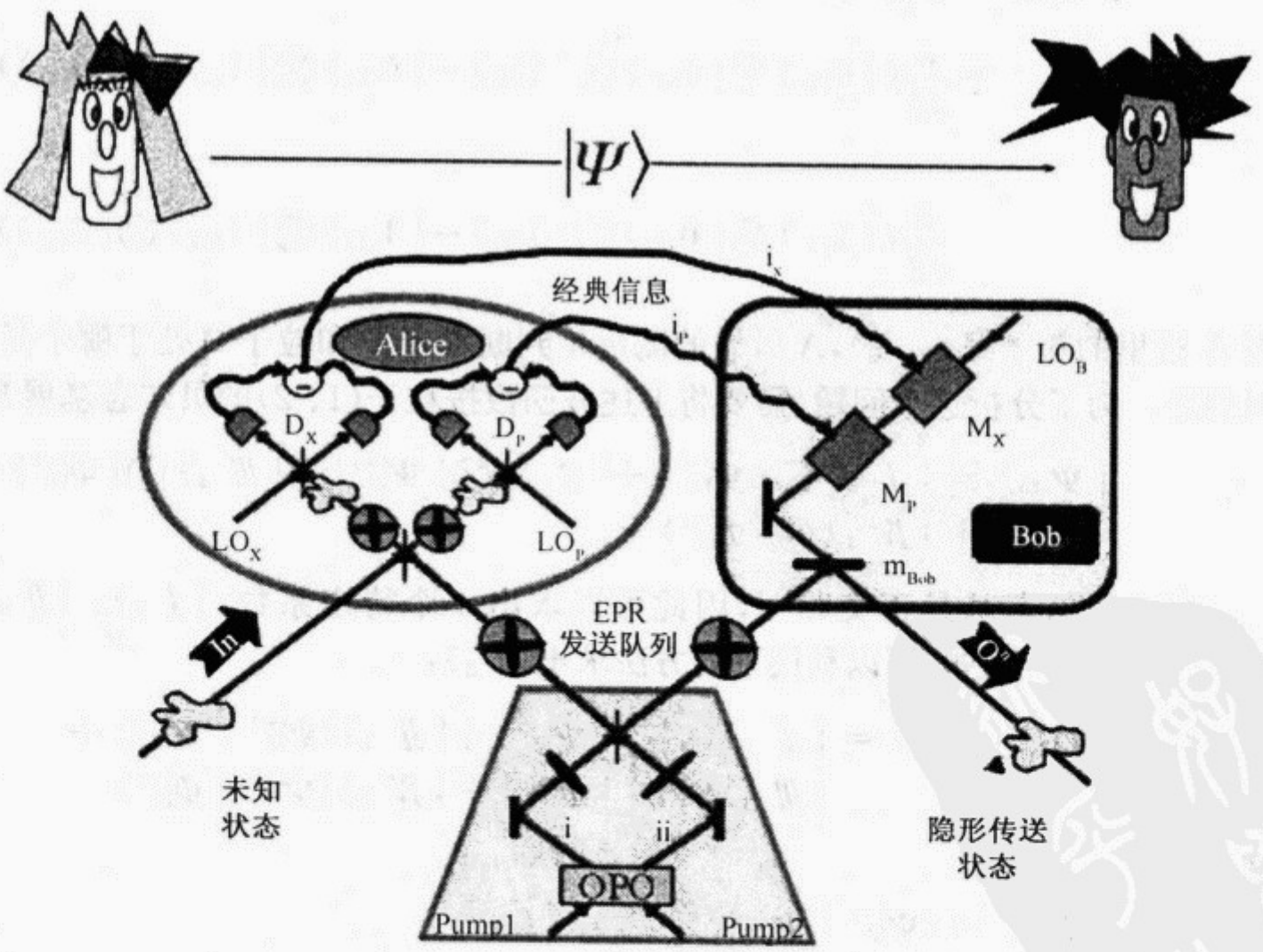


图 1-5　量子隐形传态的实验装置示意图

以下用数理解析的方式将整个信息的传递过程叙述如下。设想是这样的：一个自旋概率 0.5 的粒子(或光子)的量子态$|\varphi\rangle$中包含了所要传递的信息，Alice(以下简称 A)欲将此信息传给远方的 Bob(以下简称 B)。

事先准备好 EPR 粒子对(2、3)，使它们自旋方向相反，处在下列贝尔纠缠态：

$$|\Psi_{23}^{(-)}\rangle = \frac{(|01\rangle - |10\rangle)}{\sqrt{2}} = \frac{1}{\sqrt{2}}(|0_{(2)}\rangle \otimes |1_{(3)}\rangle - |1_{(2)}\rangle \otimes |0_{(3)}\rangle)$$

粒子 2 掌握在 A 手中，粒子 3 送到 B 处。所要传递的信息体现在粒子 1 的量子态中：

$$|\varphi_1\rangle = a|0_{(1)}\rangle + b|1_{(1)}\rangle \Rightarrow \begin{pmatrix} a \\ b \end{pmatrix}$$

下一步是 A 对粒子 1 和 EPR 粒子对(2、3)的联合系统进行测量。这时 A 所面临的粒子态为

$$\begin{aligned} |\Psi_{123}\rangle &= |\varphi_1\rangle \otimes |\Psi_{23}^{(-)}\rangle \\ &= \frac{a}{\sqrt{2}}(|0_{(1)}\rangle \otimes |0_{(2)}\rangle \otimes |1_{(3)}\rangle - |0_{(1)}\rangle \otimes |1_{(2)}\rangle \otimes |0_{(3)}\rangle) + \\ &\quad \frac{b}{\sqrt{2}}(|1_{(1)}\rangle \otimes |0_{(2)}\rangle \otimes |1_{(3)}\rangle - |1_{(1)}\rangle \otimes |1_{(2)}\rangle \otimes |0_{(3)}\rangle) \end{aligned}$$

在 A 这里的粒子是(1、2)，A 所做的测量是判断粒子 1 和粒子 2 处于哪个贝尔纠缠态。为了分析这个问题，需要将上述波函数按粒子(1、2)的贝尔态基展开：

$$\begin{aligned} |\Psi_{123}\rangle = {} & |I_3\rangle \otimes |\Psi_{12}^{(-)}\rangle + |II_3\rangle \otimes |\Psi_{12}^{(+)}\rangle + |III_3\rangle \otimes |\Phi_{12}^{(-)}\rangle + \\ & |IV_3\rangle \otimes |\Phi_{12}^{(+)}\rangle \end{aligned}$$

由于贝尔态基是正交归一，因此可以求出 4 个待定系数：$|I_3\rangle$，$|II_3\rangle$，$|III_3\rangle$，$|IV_3\rangle$。例如，可以利用下列方法求出$|I_3\rangle$：

$$\begin{aligned} \langle\Psi_{12}^{(-)}|\Psi_{123}\rangle = {} & |I_3\rangle\langle\Psi_{12}^{(-)}|\Psi_{12}^{(-)}\rangle + |II_3\rangle\langle\Psi_{12}^{(-)}|\Psi_{12}^{(+)}\rangle + \\ & |III_3\rangle\langle\Psi_{12}^{(-)}|\Phi_{12}^{(-)}\rangle + |IV_3\rangle\langle\Psi_{12}^{(-)}|\Phi_{12}^{(+)}\rangle \end{aligned}$$

则

$$\begin{aligned} |I_3\rangle &= \langle\Psi_{12}^{(-)}|\Psi_{123}\rangle \\ &= \frac{\langle 1_{(2)}0_{(1)}| - \langle 0_{(2)}1_{(1)}|}{\sqrt{2}}. \end{aligned}$$

$$\frac{a(|0_{(1)}0_{(2)}\rangle|1_{(3)}\rangle-|0_{(1)}1_{(2)}\rangle|0_{(3)}\rangle)+b(|1_{(1)}0_{(2)}\rangle|1_{(3)}\rangle-|1_{(1)}1_{(2)}\rangle|0_{(3)}\rangle)}{\sqrt{2}}$$

$$=\frac{a}{2}(\langle 1_{(2)}0_{(1)}|0_{(1)}0_{(2)}\rangle|1_{(3)}\rangle-\langle 1_{(2)}0_{(1)}|0_{(1)}1_{(2)}\rangle|0_{(3)}\rangle-\langle 0_{(2)}1_{(1)}|0_{(1)}0_{(2)}\rangle|1_{(3)}\rangle+\langle 0_{(2)}1_{(1)}|0_{(1)}1_{(2)}\rangle|0_{(3)}\rangle)+\frac{b}{2}(\langle 1_{(2)}0_{(1)}|1_{(1)}0_{(2)}\rangle|1_{(3)}\rangle-\langle 1_{(2)}0_{(1)}|1_{(1)}1_{(2)}\rangle|0_{(3)}\rangle-\langle 0_{(2)}1_{(1)}|1_{(1)}0_{(2)}\rangle|1_{(3)}\rangle+\langle 0_{(1)}1_{(2)}|1_{(1)}1_{(2)}\rangle|0_{(3)}\rangle)$$

$$=\frac{a}{2}(0|1_{(3)}\rangle-1|0_{(3)}\rangle-0|1_{(3)}\rangle+0|0_{(3)}\rangle)+\frac{b}{2}(0|1_{(3)}\rangle-0|0_{(3)}\rangle-1|1_{(3)}\rangle+0|0_{(3)}\rangle)$$

$$=\frac{1}{2}(a|0_{(3)}\rangle+b|1_{(3)}\rangle)$$

用同样的方法即可求出$|\Psi_{123}\rangle$式里的系数：

$$|I_3\rangle=\langle\Psi_{12}^{(-)}|\Psi_{123}\rangle=-\frac{1}{2}(a|0_{(3)}\rangle+b|1_{(3)}\rangle)$$

$$|II_3\rangle=\langle\Psi_{12}^{(+)}|\Psi_{123}\rangle=-\frac{1}{2}(a|0_{(3)}\rangle-b|1_{(3)}\rangle)$$

$$|III_3\rangle=\langle\Phi_{12}^{(-)}|\Psi_{123}\rangle=\frac{1}{2}(a|1_{(3)}\rangle+b|0_{(3)}\rangle)$$

$$|IV_3\rangle=\langle\Phi_{12}^{(+)}|\Psi_{123}\rangle=\frac{1}{2}(a|1_{(3)}\rangle-b|0_{(3)}\rangle)$$

写成矩阵形式，则有

$$|I_3\rangle\Rightarrow-\begin{pmatrix}a\\b\end{pmatrix}$$

$$|II_3\rangle\Rightarrow\begin{pmatrix}-a\\b\end{pmatrix}=\begin{pmatrix}-1&0\\0&1\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix}$$

$$|III_3\rangle\Rightarrow\begin{pmatrix}b\\a\end{pmatrix}=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix}$$

$$|IV_3\rangle\Rightarrow\begin{pmatrix}-b\\a\end{pmatrix}=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix}$$

也就是说，$|I_3\rangle$、$|II_3\rangle$、$|III_3\rangle$、$|IV_3\rangle$都是 $|\varphi_3\rangle \Rightarrow \begin{pmatrix} a \\ b \end{pmatrix}$ 经过某一幺正变换得到的量子态。

当 A 对于$|\Psi_{123}\rangle$进行(1、2)粒子贝尔态基的分析时，整个波函数以一定的概率随机地塌缩到某个贝尔态(譬如$|\Phi_{12}^{(+)}\rangle$)上，此时 B 手中的粒子 3 立即塌缩到与之对应的$|IV_3\rangle$上。这意味着粒子 1 和粒子 2 纠缠在一起，而粒子 3 与粒子 2 解除了纠缠。此过程称之为纠缠的交换(Entanglement Swapping)，它是不需要传递时间的。但 B 仍不知道 A 要传递给他的量子态$|\varphi_1\rangle$是什么，除非他知道 A 测得的是(1、2)粒子的哪个贝尔态。这时 A 通过经典的办法(譬如打电话或电报)告诉 B 测量的结果，于是 B 就知道用怎样的逆幺正变换把手中粒子 3 的量子态变回$|\varphi_1\rangle$，这便是 A 想要传递给他的量子态信息。

1.4.3 量子态不可克隆定理的说明

量子态不可克隆定理的道理很简单，因为量子力学的理论是线性的。

由于量子态具有叠加性，因此单次测量是不能完全得知一个量子态的。例如在一次测量自旋量子态

$$|\varphi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$$

的自旋 z 分量中，我们会得到它的本征值之一[+1/2]或[−1/2]，但不可能得到它的全部本征值，更不可能知道它们的概率幅 α 和 β。由于该次测量，这时此量子状态已塌缩了，不可能对它再进行重复测量。为了获取一个量子的完整信息，能不能将这个量子态复制出大量样本呢？有证明指出：任意量子态是不能复制的。这便是量子态不可克隆(Nonclonability of A Single Quantum)定理。定理的证明可以简述如下。

设 A 和 B 是两个量子系统，它们分别处于$|\varphi_A\rangle$和$|0_B\rangle$状态，后者是系统 B 在拷贝前所处的空白状态。假设有某种操作能够把系统 A 的任意量子态拷贝到系统 B 上，即

$$|\varphi_A\rangle \otimes |0_B\rangle \xrightarrow{\text{拷贝}} |\varphi_A\rangle \otimes |\varphi_B\rangle$$

那么，同样的操作当然也能够将另一量子态从系统 A 拷贝到系统 B 上：

$$|\Psi_A\rangle \otimes |0_B\rangle \xrightarrow{\text{拷贝}} |\Psi_A\rangle \otimes |\Psi_B\rangle$$

取它们的叠加态

$$|\Psi\rangle = |\varphi_A\rangle + |\Psi_A\rangle$$

按量子态的线性叠加原理，有

$$|\Psi\rangle \otimes |0_B\rangle = |\varphi_A\rangle \otimes |0_B\rangle + |\Psi_A\rangle \otimes |0_B\rangle$$

$$\xrightarrow{\text{拷贝}} |\varphi_A\rangle \otimes |\varphi_B\rangle + |\Psi_A\rangle \otimes |\Psi_B\rangle \neq |\Psi_A\rangle \otimes |\Psi_B\rangle$$

因为

$$|\Psi_A\rangle \otimes |\Psi_B\rangle = |\varphi_A\rangle \otimes |\varphi_B\rangle + |\Psi_A\rangle \otimes |\Psi_B\rangle + |\varphi_A\rangle \otimes |\Psi_B\rangle + |\Psi_A\rangle \otimes |\varphi_B\rangle$$

结论的矛盾表明，量子态的线性叠加原理排斥了克隆任意量子态的可能性。量子不可克隆定理是信息理论的重要基础，它为量子密码的安全性提供了理论保障。

1.4.4　NP 问题、量子并行计算与 Shor 算法的思想简介

量子并行计算的能力来自于量子态的可叠加性，是量子信息理论应用的一个重要分支。

量子计算机对每一个叠加分量实现的变换相当于一种经典计算，所有这些经典计算同时完成，并按一定的概率振幅叠加起来，最终给出量子计算机的输出结果，以这种方式实现的信息处理叫量子并行处理。量子并行处理大大提高了量子计算机的效率，使其可以完成经典计算机很难完成的工作，例如大自然数的因子分解。经典计算机中的 RSA 公钥体系就是利用两个大素数的乘积难以分解实现加密的。

经典信息处理的最基本单元是比特(Bit，即二进制数 0 或 1)。一个按照一定数学规则给出的随机二进制数据串就构成一个密钥，经典通信中最难解决的问题是密钥分配问题。由于密钥分配不是绝对保密的，经典密码也就不可能绝对保密。然而，基于量子力学线性叠加原理和不可克隆定理的量子密钥分配却可以解决密钥分配的保密性问题。

算法中的计算量，顾名思义，是指解决某问题所需要计算的时间。问题的计算时间若以计算项数幂次上升的计算量完成，我们称此问题为 P 问题(P 为英文多项式 Polynomial 的首字母)，包含所有此类问题的集合以 P 表示，因此 P 问题是一个能用 $O(n^k)$ 计算量解决的问题的集合。NP 是英文 Nondeterministic Polynomial 的缩写，意思就是非确定性的多项式时间。人们猜测可能在 P 之外还存在一类问题，其计算量是呈计算项数指数增加的，包含所有此类问题的集合以 NP 表示。NP 中有一批互依的问题又称之为 NP-complete 类。1971 年古克(Stephen A. Cook)发表了“The Complexity of Theorem Proving Procedures”

论文把 P 之外的问题归成了三大类，即 NP，NP-complete 以及 NP-hard。对经典计算机而言，一个呈幂次上升的计算量应该可以解决，但对一个呈指数上升的计算量在 n 相当大时则毫无希望。因此，我们面临的一个问题是如何将一个呈指数上升的计算量问题，简化成一个幂次上升的计算量问题。

经典计算中存在着一大类 NP 问题，这类问题在经典计算机上是不能计算的。例如 NP 问题的代表问题之一是售货员旅行问题。有一个售货员要开汽车到 n 个指定城市去推销货物，他必须经过全部的 n 个城市。现在他有一张有此 n 个城市的地图以及各城市之间的公路距离，试问他应如何取得最短的行程从家中出发再回到家中。

如图 1-6 所示，A，B，…，G 表示 7 个城市，而售货员要从 A 城市出发再回到 A 城市并访问 B，C，…，G 所有城市。一个可行的方法是

$$A\rightarrow B\rightarrow C\rightarrow D\rightarrow E\rightarrow F\rightarrow G\rightarrow A$$

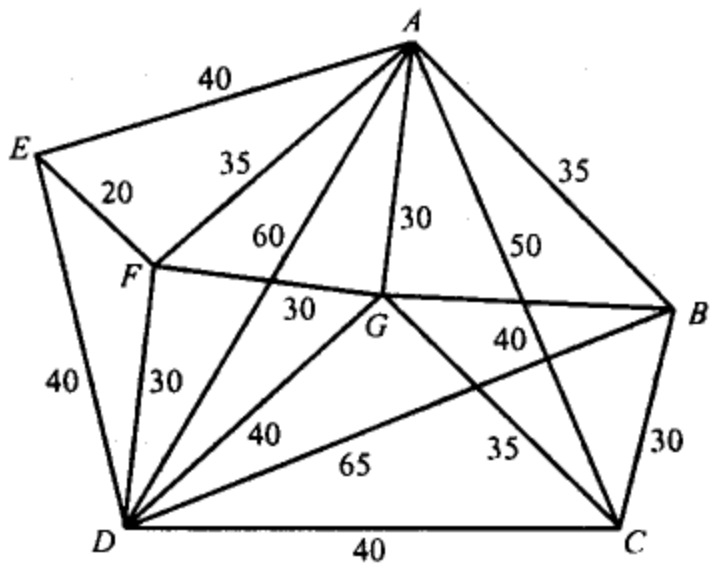


图 1-6　售货员的地图

上图中，A，B，C，…表示城市名，数字表示两城市之间的公里数距离。

问题是：这是否是最短路径？也许

$$A\rightarrow B\rightarrow C\rightarrow D\rightarrow E\rightarrow F\rightarrow G\rightarrow A$$

更近呢？加起来的结果第一条路径总长为 235 千米，而第二条路径总长为 230 千米，故第二条路径较短。但是，否存在一个更短的路径呢？目前有的方法是一个一个的排着试，但还没有找到更好可以寻得最短路径的方法。对 7 个城市而言，共有 $6!=720$ 个排法，尚不算难，但若有 20 个城市，则排法就有 19！种。因为

$$n!\cong\sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^{n}$$

故

$$19! \cong 1.21 \times 10^{17}$$

这一是一个非常大的数据，计算所需的时间随着城市个数 n 的增长而指数增长。

但是量子计算可以把其中的一部分 NP 问题变成 P 问题，即问题的复杂度随着比特位数的增长以多项式数量级上升。这类问题原则上是可以计算的。一个具体的例子就是大因数分解，按经典计算复杂性理论，这个问题不存在有效算法，所以被利用来进行经典密钥分配。但是如果用量子计算机结合 Shor 量子算法，这个问题就变成了 P 问题。

例如，为了对一个 400 位的阿拉伯数字进行因子分解，目前最快的超级计算机将耗时上百亿年，这几乎等于宇宙的整个寿命；而具有相同时钟脉冲速度的量子计算机只需要大约一分钟。因此，对于目前的密码系统，即使人们几乎无法利用经典算法对其进行破解，但如果人们拥有了一台量子计算机，那么目前的密码系统将毫无保密性可言。这一后果是对目前的密码系统的巨大挑战，因而对基于经典保密系统的行业（如军事、国家安全、金融等）的信息安全构成根本的威胁。

举例来说，我们进行 4 位数乘 4 位数的乘法计算，最多只需二三十步（即步数是 4 的多项式）即可完成，即使是小学生也能在很短的时间里算完。如果倒过来，4 位数乘 4 位数的乘积是 8 位数，即几亿的数量级，给你一个上亿的数字 N 让你做因子分解，就可能难住你。一般是除了逐个用小于 $\sqrt{N}$ 的素数试着去除它，别无其他什么妙法。而这样的素数有 10^4，即上万个，一个一个的去试除要花相当一段时间。这个问题用现代计算机去求解当然不成问题。那么给你一个 60 位的大数做因式分解会怎么样呢？现在世界上最快的计算机每秒作 10^{11} 次运算，每天 86400 秒，每年约 3×10^7 秒，不停的计算，可作 3×10^{18} 次运算。但求解 60 位大数的因式分解需要作 $\sqrt{10^{60}}=10^{30}$ 次运算，约需 3×10^{11} 年，这是宇宙年龄的 20 倍！然而量子计算机却有可望在以秒为单位的一段很短的时间内解决问题。

人们普遍相信，大数的因式分解不存在经典的多项式算法（或者说有效算法）。这一点在密码学中有着重要的应用。1977 年 Rivest、Shamir 和 Adelman 三人发明的 RSA 公钥体系，就是利用两个大素数的乘积难以分解来加密的。

1994 年 Shor 等人提出了一种大因素分解的量子多项式算法，引起了轰动。Shor 算法的核心是利用数论中的一些定理，将大数因子分解转化为求某个函数的周期。现将 Shor 算法的思想梗概作一介绍。

设待分解的大数为 N，它的平方用二进制来表示有 L 位，即 $N^2 < 2^L <$

$2N^2$。选用的周期性函数为余函数类：

$$f(x) = a^x \bmod N \tag{1.5}$$

这里 $a(a < N)$ 是任选的一个与 N 互为素数的整数，x 取从 0 到 2^L 的整数值，$\bmod N$ 表示取前面的数 N 被除的余数。显然 $f(x)$所取的值属于正整数集合 $\{1, 2, \cdots, N-1\}$，且是一个周期性的函数。举例来说，令 $N=14$，取 $a=3$，则

$$\begin{aligned}
&f(0)=1,\ f(6)=1,\\
&f(1)=3,\ f(7)=3,\qquad \vdots\\
&f(2)=9,\ f(8)=9,\qquad f(12)=1\\
&f(3)=13,\ f(9)=13,\qquad f(13)=3\\
&f(4)=11,\ f(10)=11,\qquad \vdots\\
&f(5)=5,\ f(11)=5,
\end{aligned}$$

它的周期 $T=6$，一般说来，对于大数 N，选定一个 a，若能求得式(1.5)中余函数的周期 T，设 T 为偶数(若求得的周期 T 为奇数，另选一个 a 重来)，则令 $A=a^{T/2}+1$，$B=a^{T/2}-1$，求(A, N)和(B, N)的最大公约数 C 和 D。由数论的结果可知 C 和 D 就是 N 的素因子 $N=C\times D$。例如当 $N=14$ 并选 $a=3$ 时，求得 $T=6$，于是 $A=28$，$B=26$，$C=7$，$D=2$，$N=7\times 2$。

虽然用量子计算机计算时，对于一个函数 $f(x)$可以取纠缠态，但在一次测量中只能得到非常有限的信息，此后该量子态就塌缩了。在 Shor 算法中我们只需要有关$f(x)$周期的信息，这可通过以下的傅里叶变换来提取。

取两组各有 L 个量子比特的存储器，通过幺正变换实现下式的纠缠状态：

$$\begin{aligned}
&\sum_{i=1}^{n} |\, x_i\rangle\rangle \otimes |\, f(x_i)\rangle\rangle\\
&=|\, x_1\rangle\rangle \otimes |\, f(x_1)\rangle\rangle + |\, x_2\rangle\rangle \otimes |\, f(x_2)\rangle\rangle + \cdots + |\, x_n\rangle\rangle \otimes |\, f(x_n)\rangle\rangle
\end{aligned}$$

式中 $f(x)$是由式(1.5)定义的余函数，$n=2^L$。对存储器 x 作离散傅里叶变换：

$$|\, x\rangle\rangle = \frac{1}{\sqrt{2^L}} \sum_{k=0}^{2^L-1} e^{2\pi i kx/2^L} \,|\, k\rangle\rangle \tag{1.6}$$

(注：函数系 $e^{2\pi ikx/2^L}$ 是区间$\left[-\frac{T}{2}, \frac{T}{2}\right]$上的标准正交函数系，$T$ 是 $f(x)$的周期)。于是两存储器里的纠缠态化为

$$|\Psi\rangle = \frac{1}{\sqrt{2^L}} \sum_{x=0}^{2^L-1} \sum_{k=0}^{2^L-1} e^{2\pi ikx/2^L} \; |k\rangle\rangle \otimes |f(x)\rangle\rangle \tag{1.7}$$

这时第一个存储器(x 存储器)变为 k 存储器。由于 $f(x)$的周期性,上式中许多项可以合并,而且大部分项相消或近似相消。只有 k 取下列各值时系数(概率幅)明显不为 0:

$$k = \left[m \frac{2^L}{T}\right], \; (m = 0, 1, \cdots, T-1) \tag{1.8}$$

式中 T 是 $f(x)$的周期,括号表示取大于它的最小整数。因此,除 $k = 0$ 外,

$$\frac{2^L}{k} \approx \frac{T}{m}, \; (m = 0, 1, \cdots, T-1) \tag{1.9}$$

以 $N = 14$, $T = 6$ 的例子来说, $N^2 = 196$, 需要取 $L = 8$, $2^L = 256$, $2^L/T = 42.667$, 系数(概率幅)明显不为 0 的 k 值有

$$k = 0, [42.667] = 43, [85.333] = 86, 128, [170.667] = 171, [213.333] = 214$$

这些是对 k 存储器进行测量时,实际上可能测到的 k 的本征值。要想求周期 T,就反过来计算 $2^L/k$(除 $k = 0$ 外):

$$\frac{2^L}{k} = \frac{256}{43} = 5.953 \approx 6$$

$$\frac{256}{86} = 2.977 \approx \frac{6}{2}$$

$$\frac{256}{128} = 2 \approx \frac{6}{3}$$

$$\frac{256}{171} = 1.497 \approx \frac{6}{4}$$

$$\frac{256}{214} = 1.196 \approx \frac{6}{5}$$

从若干个这样的数值不难推算出 $T = 6$ 来。

在量子计算机中 Shor 算法的每一步骤都是可以通过多项式算法来完成的。所以,在量子计算机中 Shor 算法是有效的算法。如果量子计算机能够实现,世界上许多保密系统将受到严重的威胁。因此,为了保证这些领域的信息安全,也为了拓宽人类对微观世界的认识,发展量子信息学刻不容缓:一方面,开发由量

子力学基本原理保证其保密性的量子密码系统；另一方面，研制按照量子力学基本原理运行的量子计算机。

1.5 量子逻辑门(量子逻辑电路)简介

量子逻辑电路又称为量子逻辑门，量子逻辑门按其输入比特的个数可分为单比特、二比特及三比特逻辑门等。

阅读表 1-2，让我们感到惊讶的是：描述单一量子比特逻辑门的矩阵 U 都是酉矩阵，也就是说 $U^{\dagger}U = I$，这里的 $U^{\dagger}$ 是 U 的伴随矩阵。幺正性约束是量子逻辑门上的惟一的约束。任何一个酉矩阵都可以指定为有效的量子逻辑门。有趣的是：与经典信息理论中的比特逻辑门的情况相对照，经典信息理论中非平凡单一比特逻辑门仅有一个，即非门(NOT gate)，而量子信息理论中有许多非平凡单一量子比特逻辑门。

表 1-2 单比特的量子逻辑门和电路的记号

名 称	记 号	说 明
Hadamard	—H—	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Pauli-X	—X—	$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
Pauli-Y	—Y—	$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$
Pauli-Z	—Z—	$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
Phase	—S—	$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$
$\pi/8$	—T—	$\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$

注：$e^{i\pi/4}$ 是 i 的平方根，所以 $\pi/8$-gate 是 Phase-gate 的平方根，而 Phase-gate 自身又是 Pauli-Z-gate 的平方根。

表 1-3　二比特的量子逻辑门和电路的记号

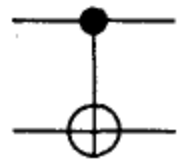
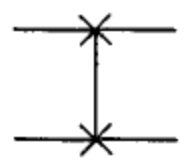
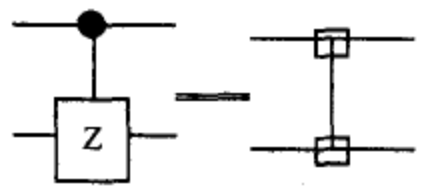
名　称	记　号	说　明
Controlled-NOT		$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$
Swap		$\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}$
Controlled-Z		$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix}$
Controlled-phase		$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&i\end{bmatrix}$

表 1-4　三比特的量子逻辑门和电路的记号

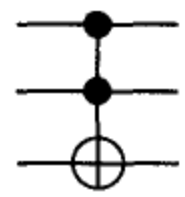
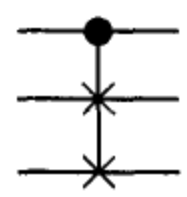
名　称	记　号	说　明
Toffoli		$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$
Fredkin(Controlled-swap)		$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\end{bmatrix}$

表 1-5 经常使用在量子信息图示描述中的记号

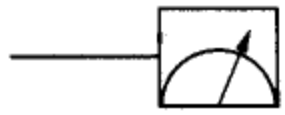
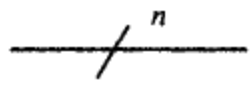
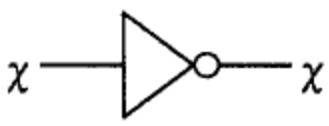
名 称	记 号	说 明
Measurement		投影到|0⟩和|1⟩上
Qubit		传送单一量子比特信号的信息
Classical bit		传送单一古典比特信号的信息
N qubit		传送 n 个量子比特信号的信息

图 1-7(a)给出了单比特逻辑门的输入与输出，图 1-7(b)给出了常用的单量子比特逻辑门及其输入和输出的对照。



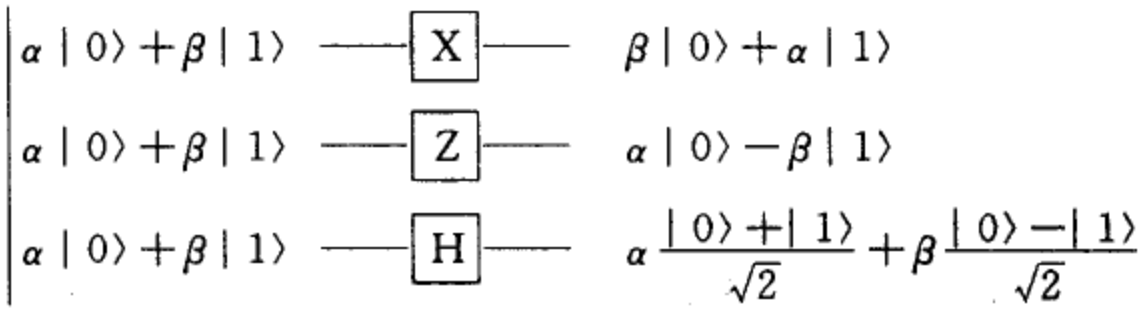


图 1-7(a) 单比特逻辑门　　图 1-7(b) 单量子比特逻辑门

图 1-8(a)给出了多比特逻辑门及其输入输出对照，图 1-8(b)给出了多量子比特控制非门及其输入和输出。

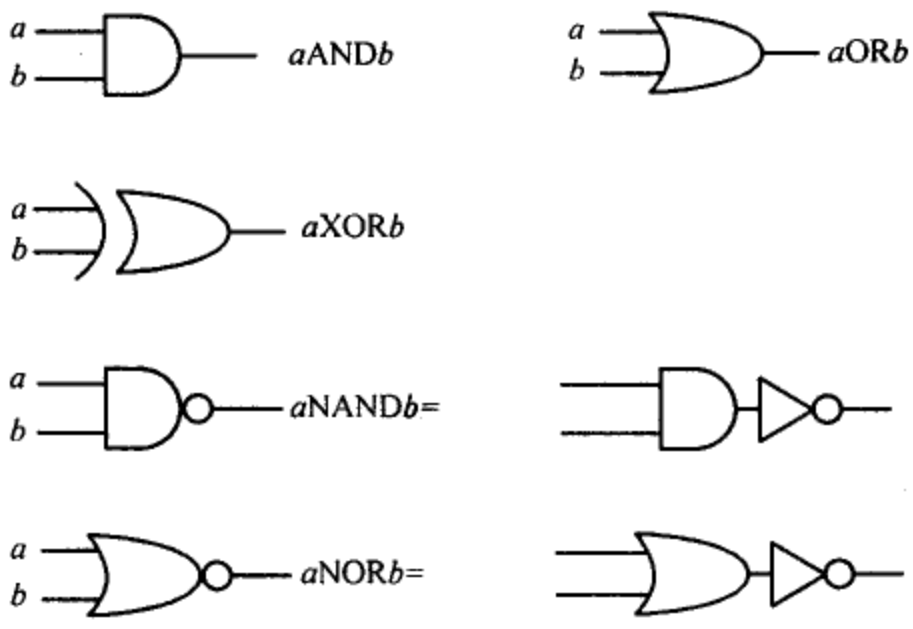


图 1-8(a) 二比特逻辑门

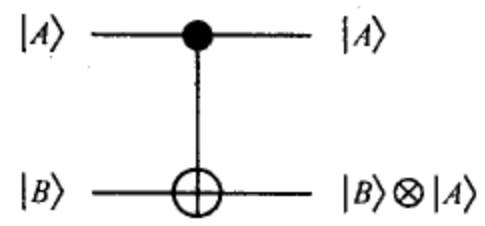


图 1-8(b) 二量子比特控制非门原型

这里对其中的两个重要且使用频繁的 Z-gate 和 Hadamard-gate 做一个简要说明：

① Z-gate

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

保持状态|0⟩不变，将状态|1⟩的符号翻转成−|1⟩。

② Hadamard-gate

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

这个逻辑门有时被描述成为非门的平方根（Square-Root of NOT）门，它将|0⟩变换到|0⟩和|1⟩的之间位置（|0⟩+|1⟩）/$\sqrt{2}$（由 Hadamard-gate 的第一列）上，同样它也将|1⟩变换到|0⟩和|1⟩的之间位置（|0⟩−|1⟩）/$\sqrt{2}$（由 Hadamard-gate 的第二列）上。Hadamard-gate 是量子逻辑门中最常用的门之一。我们利用布洛赫球可视化 Hadamard-gate 的操作（如图 1-9 所示）给出了输入状态为（|0⟩+|1⟩）/$\sqrt{2}$ 时，利用

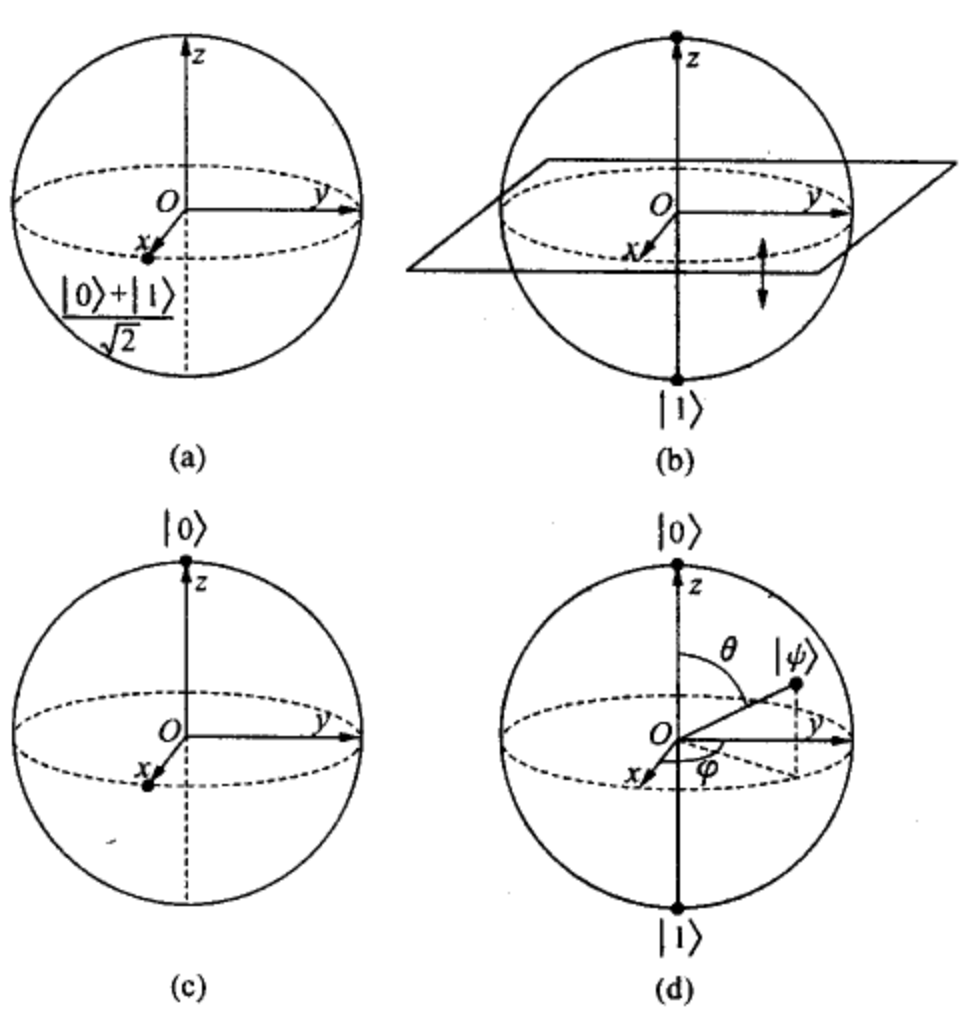


图 1-9　输入状态为（|0⟩+|1⟩）/$\sqrt{2}$ 时利用布洛赫球 Hadamard-gate 操作的可视化图示

布洛赫球 Hadamard-gate 操作的可视化图示。图中显示出单一量子逻辑门对应于布洛赫球的旋转和反射。Hadamard-gate 的操作恰好是布洛赫球关于 y 轴 90°的旋转、然后是关于 x 轴 180°的旋转。

1.6 图灵机、经典计算机与量子计算机基本概念浅议

计算机科学自开始以来就以研究问题的可计算性以及演算法的效率为己任。由于计算机的制造及运作方式各异，因此需要有一个理论模型来统一进行探讨。1930 年代初 Alonzo Church 及 Turing 提出了丘奇-图灵(Church-Turing)理论，其论点涉及判定什么是计算、什么问题是可计算的、什么问题是不可计算的这一切问题的最根本原则或标准。其中提出的图灵机是可以有效地描述任意计算机行为的数学模型，给出了所有可有效计算问题的模型。图灵机的模型虽然抽象，但是一般计算机上的算法均可有效地转化在图灵机上运算。电子计算机诞生后，丘奇-图灵理论成为刻画电子计算机计算能力的最基本的理论依据。70 年过去了，尽管新型的计算范例不断涌现，如神经网络计算、遗传计算、进化计算、DNA 计算等，但它们除了在计算复杂性方面(计算效率)较优，并没有从根本上动摇丘奇-图灵论点。

1990 年代以来，一种全新的更具挑战性的计算范例——量子计算机出现了。它是不是超越了丘奇-图灵论点的界限呢？是不是可以计算丘奇-图灵论点认为不可能计算的问题呢？对此人们产生了不同的看法，一种看法认为量子计算并没有超越丘奇-图灵论点的界限，只不过量子计算有着电子计算机不可比拟的计算效率；另一种看法认为量子计算超越了丘奇-图灵论点的界限，量子计算机能够计算电子计算机或图灵机所不能计算的一些问题。那么究竟如何，先让我们回顾一下图灵机与计算机、可逆计算、量子计算与量子计算机的相关概念。

1.6.1 图灵机、计算机与计算复杂度

经典计算机实际上就是一个通用图灵机(Turing-machine 以下简称 TM)。通用图灵机是计算机的抽象数学模型。它的主要构成与一般计算机的结构类似，具有处理单元以及记忆单元。利用一组设定好的控制程序，TM 可以进行运算工作。TM 的主要构成有：

(1) 记忆单元

TM 的记忆单元可以想像成是一条磁带，磁带上有一连串的存储单元，利用一组固定的字符(alphabet)记载着数据。磁带的长度不受限制，可以是无限长。这是 TM 和一般计算机最大的不同之处，因为一般计算机的记忆体无论其硬件

能力如何，总是有限的。磁带上记录着运算过程开始前输入的数据、运算过程中可能暂时产生的中间数据。以及运算终止时输出的数据。

(2) 处理单元

TM 的处理单元可以想像成是一个读写头，读写头指向磁带中某个存储单元，读写头可以读取该位置的数据，或是写入新的数据，并可在磁带上左右的移动，读写头中另有一个暂存器记录着 TM 当下所处状态。

(3) 控制程序

TM 的控制程序负责决定读写头在不同状态下遇到不同数据时所进行的操作，读写头可以对磁带写入数据，或是移动位置至左右两边的存储单元，也可更改 TM 的状态。整个图灵机的运算过程由控制程序完全决定。

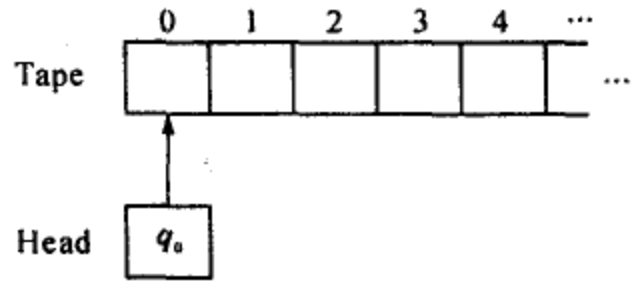


图 1-10　TM 的磁带及读写头

图 1-10 是一个简单的 TM 示意图，磁带上的存储单元自 0 开始向无限大延伸，读写头一开始指向磁带位置 0 的存储单元，并处于状态 q_0。

图 1-11 是 TM 的运算过程的范例，原本读写头指向存储单元 2 并处于状态 q_0，控制程序依照状态 q_0 及存储单元上的数据 a，决定将数据更改为 b，并将读写头左移至存储单元 1 同时将状态改为 q_1。

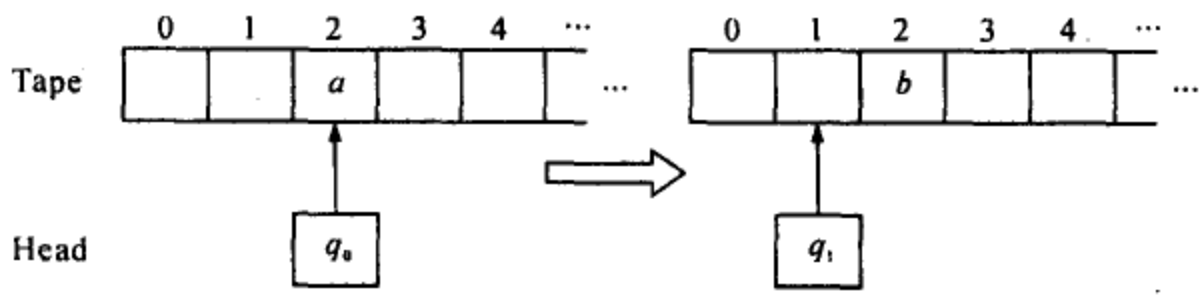


图 1-11　TM 运算过程

可以综合前述内容，将 TM 正式定义如下：

一台图灵机(TM)是一个三元组 $M=(Q,\Sigma,\delta)$，其中

Q 是一个有限非空集合，表示 TM 的状态；

Σ 是一个有限非空集合，表示运算开始前输入数据的字符，其中有一特别的符号 # 代表空白；

δ 是表示 TM 的控制程序的状态转换函数，该函数自 $Q\times\Sigma$ 映射至 $Q\times\Sigma$

$\times D, D=\{L,R,N\}$。L、R 和 N 分别代表读写头往左移动一格、往右移动一格或不移动。

可以如下方式定义 TM 的三元组态：

TMM 的三元组态为 c，代表在某一时间点上，所有可用以描述 M 的信息，包括 M 磁带中的所有内容、读写头所在位置、TM 所处状态 $q\in Q$；

TMM 假设出于组态 c 的状态，定义其后续组态 c' 为依照状态转换函数，考虑目前所处状态 q 及读写头所在的磁带内容 σ 后所得的结果。以 $c \xrightarrow[M]{} c'$ 表示这一状态转换动作。

规定 TMM 初始时的组态为：读写头在位置 0；TM 所处状态为 q_0；磁带上输入的数据为有限个，假设输入数据的数量为 s，则它们在磁带上的位置为 1～s。

TMM 的终止条件为当其进入一个特别定义的状态 q_t，此时 M 的组态称为其终止时的组态。

当 TM 开始运算之前，磁带上会先储存着关于此运算的输入数据，输入数据的内容必须是有限多组，其余部分均为空白符号 #。读写头初始的位置处于 0，状态为 q_0。接着 TM 便开始依照 δ 进行运算，直到进入状态 q_t。图 1-12 是一状态转换函数范例，它会在输入字符为 $\{a,b\}$ 的情况下，将输入数据拷贝一份，接着在输入数据的后面，举例来说，如果输入数据是 #ab#，则 TM 运算终止后，磁带上的数据为 #ab#ab#。图中的圆圈代表 TM 的状态，箭头表示状态转换的流程，箭头上的文字 $(a/b,X)$ 代表在输入为 a 的情况下将该存储单元写入 b，并在 X 方向移动一格（X 可能为 L，代表向左，或是 R，代表向右，或是 N，代表不移动）

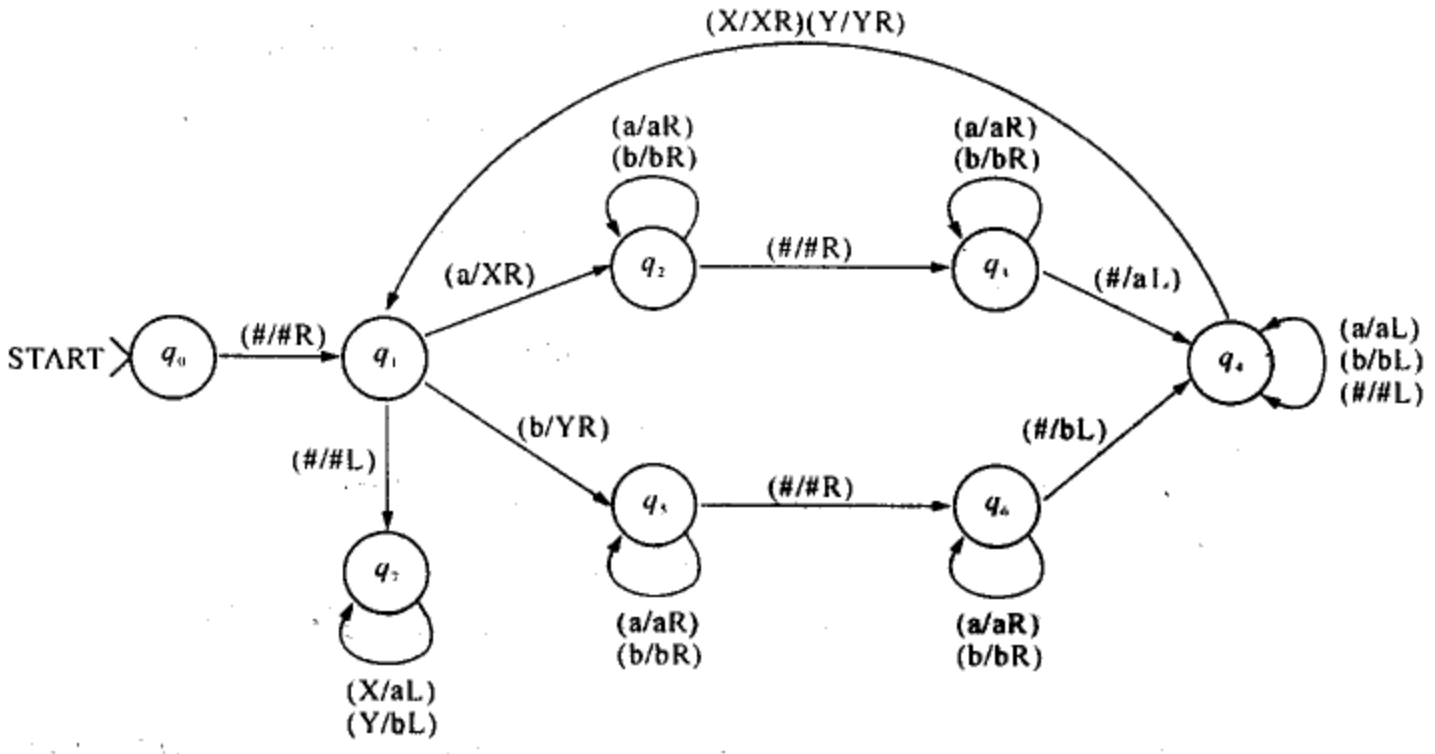


图 1-12 TM 运算过程

利用前述的 TM 定义，可以将各式演算方法以 TM 的状态转换函数 δ 表示，一个演算方法的优劣，通常可以利用其所耗用的执行步骤及所需使用到的磁带长度进行评估。TM 的执行步骤数即所耗用的时间，使用到的磁带长度代表其所耗用的空间。在计算理论中，可以针对演算方法对于时间及空间耗用程度进行归类，亦即探讨其计算复杂度。在探讨时间 t、空间 s 的复杂度时，均是试图求出 s,t 相对于输入数据长度 n 的函数关系。在考虑时间复杂度时，若执行时间 t 与输入数据长度 n 可以多项式函数表示，则一般认为这是有效率的演算方法，若 t 必须以 n 的指数函数表示，则认为这是没有效率的演算方法。由前述的 TM 定义可知，面对不同的计算问题，需要借助调整状态转换函数 δ 来定义不同的 TM。若将状态转换函数 δ 想像成为一组程序、其所处的 TMM 想像为一台计算机，则为每一组程序都必须建造一台特别的计算机！这显然相当没有效率，其实可以将所有的状态转换函数经过统一的编码之后，由一台通用图灵机(UTM)进行模拟任何 TM 的动作，概念上就如同在一台计算机上可以执行多个使用同样指令集撰写的程序。虽然目前仍然没有办法证明或给出反例，一般都认为 TM 的模型可以完全描述一般的计算过程，丘奇-图灵理论就是由此点出发，断言在 TM 上可被有效率的演算方法计算的问题即为所有可被任何其他计算模型有效率计算出的问题。这个断言相当严厉，代表若有一计算问题在 TM 的模型中找不到有效率的演算方法，则这个问题必定不可能在任何计算模型中找到有效率的演算方法。量子计算被视为一可能打破丘奇-图灵理论的计算模型，因为 P. W. Shor 在 1994 年提出了一个在量子计算的模型下的有效率的质因子分解算法，而一般均认为在一般经典计算机模型内，无法找到有效率的质因子分解算法。

1.6.2　可逆计算、量子图灵机与量子计算机

正如经典计算机建立在通用图灵机基础之上，量子计算机亦可建立在量子图灵机基础上。量子图灵机可类比于经典计算机的概率运算。

注意前一节提到的通用图灵机的操作是完全确定性的，用 q 代表当前读写头的状态，δ 代表当前存储单元内容，d 取值为 L、R、N 分别代表读写头左移、右移或不动，则在确定性算法中，当 q、δ 给定时，下一步的状态 q'、δ' 及读写头 d 的运动完全确定。我们也可以考虑概率算法，即当 q,δ 给定时，图灵机以一定的概率 $\delta(q,\sigma,d)$ 变换到状态 q'、σ' 及实行运动 d。概率函数 $\delta(q,\sigma,d)$ 为取值[0,1]的实数，它完全决定了概率图灵机的性质。经典计算机理论证明，对解决某些问题，概率算法比确定性算法更为有效。

量子图灵机非常类似于上面描述的经典概率图灵机，现在 q、σ、q'、σ' 相应地

变成了量子态，而概率函数 $\delta(q,\sigma,d)$ 则变成了取值为复数的概率振幅函数 $x(q,\sigma,d)$，量子图灵机的性质由概率振幅函数确定。正因为现在的运算结果不再按概率叠加，而是按概率振幅叠加，所以量子相干性在量子图灵机中起本质性的作用，这是实现量子并行计算的关键。

还注意到通用图灵机模型是不可逆的，例如，对如下图灵机的操作“写存储单元→左移一格”，其逆就变成了“左移一格→写存储单元”，该逆操作不再是一个有效的图灵机操作。但 Bennett 证明了一个基本结果：对所有不可逆的通用图灵机，都可以找到一个对应的可逆图灵机，使得两者具有完全相同的计算能力和计算效率。

因为计算机中的每步操作都可以改造为可逆操作，而在量子力学中，任何可逆操作都可以用一个幺正变换来代表。Benioff 最早用量子力学来描述可逆计算机。早期的量子可逆计算机，实际上是用量子力学语言表述出来的经典计算机，虽然其比特的载体为二能级的量子体系，但该体系只能处于$|0\rangle$和$|1\rangle$上，不能处于它们的叠加态，它没有利用量子力学中量子叠加和相干的本质特性，而 Feynman 指出这些量子特性可能在未来的量子计算机中起本质作用。

量子计算机可以等效为一个量子图灵机。但量子图灵机是一个抽象的数学模型，如何在物理上构造出量子计算机呢？理论上已证明，量子图灵机可以等价为一个量子逻辑电路，因此可以通过一些量子逻辑门的组合来构成量子计算机。因为量子逻辑门是可逆的，所以其输入和输出比特数相等。量子逻辑门对输入比特进行一个确定的幺正变换，得到输出比特。Deutsch 最早考虑了用量子逻辑门来构造计算机的问题，他发现，几乎所有的三比特量子逻辑门都是通用逻辑门。通用逻辑门的含义是指，通过该逻辑门的级联，可以任意精度逼近任何一个幺正操作。后来不少人发展了 Deutsch 的结果，最后 Deutsch 和 Lloyd 各自独立地证明了几乎所有的二比特量子逻辑门都是通用的，这里“几乎”是指，二比特通用量子逻辑门的集合是所有二比特逻辑门的集合的一个稠密子集。

实验上通常用一些具体的量子逻辑门来构造计算机。Barenco 等人证明，一个二比特的异或门和对一比特进行任意操作的门可构成一个通用量子门集。相对来说，单比特逻辑门在实验上比较容易实现，现在的不少实验方案都集中于制造量子异或门。量子异或门和经典异或门非常类似，它有 2 个输入比特：控制比特和受控比特。当控制比特处于$|1\rangle$态，即在上能级（激活态）时，受控比特态发生反转。用记号 C_{12} 代表量子异或操作，其中 1、2 分别代表控制和受控比特，则有

$$|n_1\rangle_1 |n_2\rangle_2 \xrightarrow{C_{12}} |n_1\rangle_1 |n_1 \oplus n_2\rangle_2$$

其中 n_1、n_2 取值 0 或 1，⊕表示模 2 加。已有的用来实现量子异或门的方案包括：利用原子和光腔的相互作用；利用冷阱束缚离子；利用电子或核自旋共振。在已实现的方案中，以冷阱束缚离子方案最为成功。

1.6.3　量子计算机浅议

量子计算机科学与技术的理论基础是量子信息理论。量子信息理论的研究起始于 20 世纪 70 年代的光量子通信研究。光量子通信理论着眼于光的量子特性，通过量子力学理论获取光量子通信的原理，考察光量子通信的真谛。70 年代是光量子通信实用化的阶段，这是研究的必然结果。这一阶段的主要研究成果有：利用量子信道实施数据通信时信道容量上界的理论结果（Holevo 界限），通过对编码整体一次性测定，比较一个记号单位测定所获取的信息获得信道容量增加的结论，即量子信道容量的超加法性，还有一些有关量子测量理论的研究成果。这个时代的研究成果被收录在 Helstrom 以及 Holevo 撰写的两本专著中，并一直影响着量子信息理论的研究。

20 世纪 80 年代初，计算机科学的研究领域里就出现了量子计算机的概念。R. P. Feynman 在他晚年有关计算理论的演讲中提出了量子计算机的概念，他认为基于量子力学理论的量子计算机其计算速度一定比现在的经典计算机要快。在这之后的 1985 年，D. Duetsch 在他的论文“Quantum theory, the Church-Turing principle and the universal quantum computer”中，根据量子态的叠加原理，给出了能够完成并列计算的量子计算机的量子图灵机的原理表述。但是对量子计算机在数学上给予严格的形式化描述，却是在进入 90 年代之后由 E. Bernstein和 U. Vazirani 在他们共同发表的“Quantum complexity theory”论文中给出。从 80 年代到 90 年代的初期，量子计算机理论的探讨还无法摆脱仅限于简单的计算模型的事实，因为有关量子计算的计算量理论里出现许多有待解决的新问题。

1996 年，美国《科学》周刊科技新闻报道了量子计算机的理念及其研究现状，从而引起了计算机理论领域的高度重视。同年，量子计算机的先驱之一，Bennett 在英国《自然》杂志新闻与评论栏声称，量子计算机将进入工程时代。那么，什么是量子计算机呢？

量子计算机，顾名思义，是一类遵循量子力学规律存储量子信息、实现量子计算的物理装置。当某个装置处理和计算的是量子信息，运行的是量子算法时，它就是量子计算机。要说清楚量子计算，首先看经典计算。经典计算机从物理上可以被描述为对输入信号序列按一定算法进行变换的机器，其算法由计算机的内部逻辑电路来实现。经典计算机具有如下特点：

(1) 其输入态和输出态都是经典信号,若用量子力学的语言来描述,就是:其输入态和输出态都是某一力学量的本征态。如输入二进制序列 0110110,用量子记号表示即为|0110110〉。所有的输入态均相互正交。对经典计算机不可能输入如下叠加态:

$$C_1 \mid 0110110\rangle + C_2 \mid 1001001\rangle$$

(2) 经典计算机内部的每一步变换都将正交态演化为正交态,而一般的量子变换没有这个约束,因此,经典计算机中的变换(或计算)只对应布尔矩阵理论中的一类特殊子集。

相应于经典计算机的以上两个限制,量子计算机本身具备性质对这两个限制分别作了如下的推广。因此量子计算机的特点为:

(1) 量子计算机的输入态和输出态为一般的叠加态,其相互之间通常不正交;

(2) 量子计算机中的变换为所有可能的幺正变换。得出输出态之后,量子计算机对输出态进行一定的测量,给出计算结果。

由此可见,量子计算对经典计算作了极大的扩充,经典计算是一类特殊的量子计算。量子计算最本质的特征为量子叠加性和相干性。量子计算机对每一个叠加分量实现的变换相当于一种经典计算,所有这些经典计算同时完成,并按一定的概率振幅叠加起来以后给出量子计算机的输出结果,实现量子并行计算。

量子计算机的概念源于对可逆计算机的研究,而研究可逆计算机是为了克服计算机中的能耗问题。早在 20 世纪 60 年代至 70 年代,人们就发现,能耗会导致计算机芯片的发热,影响芯片的集成度,从而限制了计算机的运行速度。Landauer 最早考虑了这个问题,他考察了能耗的来源,指出:能耗产生于计算过程中的不可逆操作。例如,对两比特的异或操作,因为只有一比特的输出,这一过程损失了一个自由度,因此是不可逆的,按照热力学,必然会产生一定的热量。但这种不可逆性是不是不可避免的呢? 事实上,只要对异或门的操作进行如图 1-13所示的简单改进,即保留一个无用的比特,该操作就变为可逆的。因此物理原理并没有限制能耗的下限,消除能耗的关键是将不可逆操作改造为可逆操作。

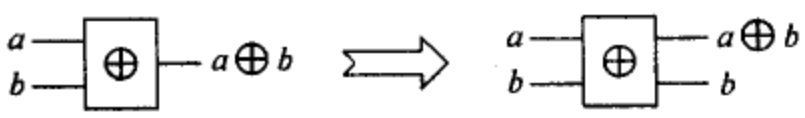


图 1-13 不可逆异或门改进为可逆异或门

Bennett 后来更严格地考虑了此问题,并证明了,所有经典不可逆的计算机都可以改造为逆计算机,而不影响其计算能力。

如上所述:在经典计算机中,基本信息单位为比特,运算对象是各种比特序列。与此类似,在量子计算机中,基本信息单位是量子比特,运算对象是量子比特序列。所不同的是,量子比特序列不但可以处于各种正交态的叠加态上,而且还可以处于纠缠态上。这些特殊的量子态,不仅提供了量子并行计算的可能,而且还将带来许多奇妙的性质。与经典计算机不同,量子计算机可以做任意的幺正变换,在得到输出态后,进行测量得出计算结果。因此,量子计算对经典计算作了极大的扩充,在数学形式上,经典计算可看作是一类特殊的量子计算。量子计算机对每一个叠加分量进行变换,所有这些变换同时完成,并按一定的概率幅叠加起来,给出结果,这种计算称作量子并行计算。除了进行并行计算外,量子计算机的另一重要用途是模拟量子系统,这项工作是经典计算机无法胜任的。

迄今为止虽然世界上还没有真正意义上的量子计算机。但是,世界各地的许多实验室正在以巨大的热情追寻着这个梦想。如何实现量子计算,方案并不少,问题是在实验上实现对微观量子态的操纵确实太困难了。目前已经提出的方案主要利用了原子和光腔相互作用、冷阱束缚离子、电子或核自旋共振、量子点操纵、超导量子干涉等。现在还很难说哪一种方案更有前景,只是量子点方案和超导约瑟夫森结方案更适合集成化和小型化。将来也许现有的方案都派不上用场,最后脱颖而出的是一种全新的设计,而这种新设计又是以某种新材料为基础,就像半导体材料对于电子计算机一样。研究量子计算机的目的不是要用它来取代现有的计算机。量子计算机使计算的概念焕然一新,这是量子计算机与其他计算机如光计算机和生物计算机等的不同之处。量子计算机的作用远不止是解决一些经典计算机无法解决的问题,量子计算机实现量子并行计算或量子模拟计算,其本质上都是利用了量子相干性。遗憾的是,在实际系统中量子相干性很难保持。在量子计算机中,量子比特不是一个孤立的系统,它会与外部环境发生相互作用,导致量子相干性的衰减,即消相干。因此,要使量子计算成为现实,一个核心问题就是克服消相干。而量子编码是迄今发现的克服消相干最有效的方法。主要的几种量子编码方案是:量子纠错码、量子避错码和量子防错码。量子纠错码是经典纠错码的类比,是目前研究的最多的一类编码,其优点为适用范围广,缺点是效率不高。

1.7　有关量子信息编码的基本概念

在经典信息论中,为了确保信息能够被快速无误地处理和传输,在以香农熵为度量准则的基础上,针对信息源引入了信源与信道的编码体系,其目的是去除冗余压缩代码提高传输效率,并在传输中能自动防错纠错。代码在信道中传输,

噪声干扰不可避免，为了克服由噪声引发的代码出错，引入了信息的信道编码体系，通过重复代码自身或重构代码、增加冗余的方法达到系统自动纠正信道传输中出错代码的目的，确保信息传输无误。量子信息理论中能否借鉴经典信息理论中的这些理念和方法一直备受计算机科学理论界的关注。

1983 年至 1986 年，美籍犹太裔的著名物理学家费因曼(Richard P. Feynman)于加州理工学院的一个系列讲座课程中，在重新考虑计算机的潜能与极限时，发现量子状态叠加与纠缠的现象赋予了量子计算指数增加的高度并行计算能力，可以实现经典计算机所无法达到的复杂计算，从此正式开启量子计算的研究领域。然而伴随着量子纠缠所可能发生的比特反转与位相翻转等现象极易导致错误的量子计算结果，此问题持续困扰着量子研究人员，令学术界全体同仁认识到在量子信息的传输与计算中，量子错误更正与容错同样是实现量子计算的重要课题之一。

自从贝尔实验室研究人员 P. W. Shor 利用量子计算中的量子信息的状态叠加与并行运算的原理，成功地实现大数因子分解的多项式算法以来，量子信息理论的研究对象从最初比特转移到量子比特，并开始构筑以量子比特为对象的量子信息理论。这个研究方向上早期的最大成果是 1995 年 B. Schumacher 在他的题为“Quantum coding”论文中给出了量子信息源编码定理，走出了历史性的一步。B. Schu-macher 在论文中，针对输出为量子比特的信息源，考虑以任意小的错误率能够恢复元代码序列的编码压缩方案时，明显地感觉到利用冯·诺伊曼熵(Von-Neumann entropy)概念能够给出量子信息源编码压缩的界限，他开始着手赋予冯·诺伊曼熵操作的意义，并将冯·诺伊曼熵引入量子信息理论。冯·诺伊曼熵与奠定经典信息理论的香农熵(shannon entropy)的类似性，促使量子计算机科学理论的研究者们进一步将经典信息理论的研究手法引入到量子信息理论的研究中。利用这些证明手法，在 1997 年和 1998 年，B. Schumacher 和 M. D. Westmoreland 两人组以及 Holevo 分别独立地证明了 70 年代获得的 Holevo 界限与无记忆量子信道的信道容量(信道中信息无失真地最大传输速率)相一致的结论，由此解决了长期未能明确的量子信道性能界限的上界问题。由于 Holevo 界限是由冯·诺伊曼熵与冯·诺伊曼条件熵的差决定的，而量子信道容量也具有冯·诺伊曼熵的特征，因此通过量子信息理论的研究，我们能够把冯·诺伊曼熵与香农熵的概念对应起来。

与经典信息的信源编码和信道编码的理念一样，量子信息理论的研究也包含信源编码和信道编码的研究。量子信源编码依然是考虑去除量子比特列中包含的冗余信息，压缩信息量；量子信道编码也依然是考虑增加量子比特列的冗余，实现量子信息的高可靠性的传输。量子信息自动纠错是量子信道编码体系

的主要研究对象，其目的是克服量子信道的噪音对量子信息的干扰，提高量子计算机的容错能力，实现量子信息的高可靠性的处理。然而量子错误更正编码的研究直到 20 世纪 90 年代中期以前一直处于混沌未开时期，由于信息的量子状态与环境的相互影响、量子状态的连续性、纠缠性以及量子信息无法科隆定理的存在，部分学者认为量子错误更正比数字通信纠错更为困难。美英学者深入研究多量子状态的纠缠现象，发现量子纠缠对于量子计算亦敌亦友，未经控制的量子纠缠足以破坏量子计算的结果，然而经过适当控制的量子纠缠却可以保护量子信息。量子错误更正的研究于 1995 年露出第一道希望的曙光，P. W. Shor 以及英国牛津大学学者 A. M. Steane 在物理层上，把复杂的纠缠态量子错误归结和简化为只需考虑每个量子位上独立发生的错误，并且错误类型只有三种：比特反转错误、位相翻转错误和比特反转加位相翻转错误，抽象成三个 Pauli 矩阵 σ_x、σ_y 和 σ_z。基于这种物理模型的简化，将量子状态代码化，通过增加冗余赋予代码对错误纠正的能力，构造出世界上第一个量子纠错码[[9,1,3]]，随后不久人们把它又改进为[[7,1,3]]和[[5,1,3]]，后者是最佳量子码，通常将该方案称为是针对经典比特纠错编码的量子版本。

1996 年，由 A. R. Calderbank 与 P. W. Shor 二人小组以及 A. M. Steane 几乎同时运用纠缠现象的量子纠错编码方案，以经典线形纠错编码的原理为基础，设计出理论上简单可行的量子纠错编码。以后为了纪念他们原创性的工作，采用三人的姓名字首，将所发现的量子纠错码简称为 CSS 码。至此运用量子纠缠来更正错误的概念广泛地被学术界所接受，世界各地的研究人员相继提出各种类型的量子错误更正码，迎来了 20 世纪 90 年代的量子信息错误更正编码研究的黄金时代，出现了量子纠错、量子避错、量子防错的量子错误更正的编码体系，其中最广为人知的是稳定码(stabilizer code)。稳定码是自 CSS 编码提出后数月，A. R. Calderbank，E. M. Rains，P. W. Shor，N. J. A. Sloane 等人总结了量子纠错编码理论的数学形式，并且给出一种构作量子码的系统的有效的数学方法，如同一般科学上的发现常常是构建于已知的基础再发扬光大，稳定码系 CSS 码的广义形式，是由若干稳定算子(矩阵)构成的群所定义，稳定码的码字为稳定算子对应于本征值 1 的本征向量，因此稳定码具备完整的数学架构。稳定码的编码方案给出经典纠错编码和量子纠错编码之间的密切联系，从而用经典纠错码的结果构作出一批好的量子码。他们的工作极大地推动了量子纠错编码数学理论的研究，1999 年以来，人们不仅利用各种经典纠错码得到一批纠错性能不断改善的量子码，而且开展了关于量子码性能的其他课题的研究，明确了经典纠错编码与量子纠错编码在代数性构造上的不同，指出了量子纠错编码的研究方向。

量子错误更正码与量子容错计算是实际操作量子计算机所不可或缺的技术。具备高度并行计算能力的量子计算机，执行计算的结果正确与否，极端依赖于准确控制神奇的量子纠缠现象。量子信息错误更正的各种编码巧妙地利用量子纠缠来纠正可能发生的错误，然而量子编码的电路本身，也需要采用适当的容错设计，以保证量子计算机能够实现精确的高速运算。量子错误更正编码的发展历史，至今不到十年的时间，量子容错计算的理论，仍有许多有待探索的部分，本节所简单介绍的量子错误更正与容错原理，仅仅提供一个优雅深邃理论内含的粗浅描述。

1.7.1 量子信息编码

现在利用计算机进行复杂运算时，我们不再为结果的可靠性担心。但是在计算机概念刚提出时，曾经有人提出如下反驳：在计算机这样一个复杂系统中，噪声是不可避免的，只要噪声使得计算机中任一部件发生一次错误，最后的运算结果都会变得面目全非，因此，利用计算机进行复杂运算是不可能的。这一困难后来是怎样克服的呢？信息的信道编码在克服这个困难的过程中起了关键性的作用。信道编码是通过引入冗余信息，使得在一部分比特发生错误的情况下，系统仍有可能按照一定的规则自动纠正这些错误，以实现无失真地传送和处理信息。举一个最简单的重复码为例，将信号 0 编码为 000 信号 1 编码为 111，这样如果最多只有一个比特发生错误，譬如，000 变成了 001，不过可以按照少数服从多数（择多译码）的原则，找出错误的比特（第三比特），并纠正该错误。

以上是经典编码的基本概念，为什么要引进量子编码呢？这与量子信息论特别是量子计算机的发展有关。量子信息论中，信息的载体不再是经典比特，而是一个一般的二态量子体系。这个二态量子体系，可以是一个二能级的原子或离子，也可以是一自旋为 1/2 的粒子或具有两个偏振方向的光子，所有这些体系，均称为量子比特。区别于经典比特，量子比特可以处于 0，1 两个本征态的任意叠加态，而且在对量子比特的操作过程中，两态的叠加振幅可以相互干涉，这就是所谓的量子相干性。已经发现，在量子信息论的各个领域，包括量子计算机、量子密码术和量子通信等，量子相干性都起着本质性的作用。可以说，量子信息论的所有优越性均来自于量子相干性。但不幸的是，因为环境的影响，量子相干性将不可避免地随时间指数衰减，这就是困扰整个量子信息论的消相干问题。消相干引起量子错误，量子编码的目的就是为了纠正或防止这些量子错误。虽然量子编码和经典编码的基本想法类似，即要以合适的方式引进信息冗余，以提高信息的抗干扰能力，但量子码可不是经典码的简单推广。在量子情况下，编码存在着一些基本困难，表现在如下 3 方面：

(1) 经典编码中，为引入信息冗余，需要将单比特态复制到多比特上去。但在量子力学中，有个著名的量子态不可克隆定理(见续讲《量子克隆与量子复制》，禁止态的复制。)

(2) 经典编码在纠错时，需要进行测量，以确定错误图样。在量子情况下，测量会引起态坍缩，从而破坏量子相干性。

(3) 经典码中的错误只有一种，即 0，1 之间的跃迁。而量子错误的自由度要大得多。对于一种确定的输入态，其输出态可以是二维空间中的任意态。因此，量子错误的种类为连续统。

因为这些原因，量子纠错比经典纠错困难得多。事实上，直到 1995 年底至 1996 年，Shor 和 Steane 才独立地提出了最初的两个量子纠错编码方案。量子纠错码通过一些巧妙的措施，克服了上面的 3 个困难，具体为：

(1) 为了不违背量子态不可克隆定理，量子编码时，单比特态不是被复制为多比特的直积态，而是编码为一较复杂的纠缠态。对于纯态而言，纠缠态即指不能表示为直积形式的态。通过编码为纠缠态，既引进了信息冗余，又没有违背量子力学的原理。

(2) 量子纠错在确定错误图样时，只进行部分测量。通过编码，可以使不同的分量错误对应于不同的正交空间，通过部分的量子测量(即只对一些附加量子比特，而不是对全部比特进行测量)使状态投影到某一正交空间。在此正交空间，信息位之间的量子相干性仍被保持，同时测量的结果又给出了量子错误图样。

(3) 量子错误的种类虽然为连续统，但人们发现，它可以表示为 3 种基本量子错误(对应于 3 个 Pauli 矩阵)的线性组合。只要纠正了这 3 种基本量子错，所有的量子错误都将得到纠正。

自从发现了最初的两个量子编码方案，各种更高效的量子码已被相继提出。下面介绍两类最重要的量子编码，即纠随机错的量子码和防合作错的量子码。

1.7.2　量子编码定理

量子编码定理研究的目标是要寻找 Shannon 定理的量子对应。Shannon 信源编码定理确定了任一信源给出的信息的最大压缩率，信道编码定理确定了信息在有噪信道中无失真地传输的最大速率，亦即信道容量。Shannon 定理奠定了整个经典信息论的基础，对于量子信息论，是否存在类似的定理？能否能够引进信道容量的概念？如何发展有效的算法去计算量子信道容量？这些问题显然都是量子信息论中的基本问题。

量子信源以概率 p_i 发送密度算符为 ρ_i 的量子态，$p=\sum_i p_i\rho_i$ 表示信源的总

密度算符。量子信源编码定理要回答的是，对于这样的量子系统，其信息最少可以用多少个量子比特表征出来？Schumacher 的定理表明，如果所有 p_i 均限制为纯态，以 2 为底的冯·诺伊曼熵 $S(\rho) = -tr(\rho\log_2\rho)$ 确定了所需的最小量子比特数。Schumacher 的定理后来经 Holevo 推广到 ρ_i 为混合态的情况，此时相对冯·诺伊曼熵 $S(p)=\sum_i p_i S(\rho_i)$ 确定了所需的最小量子比特数。

相比信源编码定理，信道编码定理的证明要复杂和困难得多。首先要弄清楚的一点是，量子信道可以同时传送经典信息和量子信息。因此，对于一个给定的量子信息，既存在经典信息容量，又存在量子信息容量，这两者有时相差悬殊。为了说明这种区别，我们举一个简单的例子。考虑一个具有如下性质的信道，如果输入态在基底$|0\rangle$，$|1\rangle$下具有对角形式，该信道不影响传送的态；反之，如果输入态为一般的量子态，信道将完全破坏$|0\rangle$，$|1\rangle$之间的相干性，亦即使基底$|0\rangle$，$|1\rangle$下的非对角项消失，但保持对角项不变，此信道称为完全解相干信道。可以证明，该信道的经典信息容量为 1，而量子信息容量为 0，因为量子相干性在该信道中不能维持。

量子信道编码定理的研究已经取得了很大进展。量子信道的经典信息容量已完全确定，它可以用前面引入的相对冯·诺伊曼熵表示出来，其证明有点类似于量子信源编码定理的证明。量子信道的量子信息容量尚未完全解决，但也已经取得重要突破。Schumacher，Lloyd 和 Nielsen 等引入了相干信息的概念，并证明，此概念可以作为经典交互信息的量子类比。利用相干信息，他们给出了量子信息容量的一个上限，此上限能否达到，目前还缺乏证明，但人们相信，通过合适的改进，该上限将给出量子信息容量。另外，当前还有一个迫切的问题是如何发展有效的算法去计算一般信道的量子信息容量。这些构成了进一步研究的课题。

1.7.3 量子编码方案

(1) 纠随机错的量子码

通常所谓的量子纠错码即指纠随机错的量子码。各种量子纠错方案，实际上都假定发生量子错误的比特数是给定的，例如常见的有纠一位错的量子码。然而在实际情况下，所有的量子比特均经历消相干，因此每个比特都有可能出错，发生错误的比特数是不定的。于是一个自然的问题为，那种设计用来纠一位错或更多位错的量子码在实际中是否有效？此问题的答案是肯定的。分析表明只要量子比特独立地发生消相干(亦即各个比特随机地出错)，所有的量子纠错方案都会行之有效。这里可以给一个简单的说明，设在 T 时间内进行 N 次纠错操作，在两次纠错间隔中，比特的出错率正比于 T/N(即 N 越大，间隔越小，比

特的出错率也就越小)。纠一位错后,其剩余错误率将正比于 T^2/N^2,因此 N 次纠错后,系统的累计剩余错误率正比于 $N(T^2/N^2)$。只要 N 足够大,亦即两次纠错的时间间隔足够小,就可以使得系统的累计剩余错误率任意地小。

Shor 的第一个纠错方案为量子重复码,它利用 9 比特来编码 1 比特信息,可以纠正 1 位错。Shor 的方案简单,而且与经典重复码有较直接的类比,但它的效率不高。事实上,Steane 的编码方案倒是对后来的量子纠错码影响更大。在该方案中,Steane 提出了互补基的概念,给出了量子纠错一些一般性的描述,并具体构造了一个利用 7 比特来编码 1 比特纠 1 位错的量子码。紧接着,Calderbank 和 Shor 以及 Steane 提出了一个从经典纠错码构造量子纠错码的方法,该方法建立在群论语言之上。纠 1 位错的最佳(效率最高)量子码也由两个小组独立地发现,该方案利用 5 比特来编码 1 比特。纠多位错的量子编码情况更复杂,迄今为止,只发现一些简单的纠多位错的量子码。现有的各种量子纠错码,都可以被统一在群论框架之下,该描述已由 Gottesman 和 Calderbank 等给出。但利用现有的理论去构造新的量子纠错码,仍然是一件非常艰巨的工作,为了寻求更高效的量子码,人们往往需要逐步地摸索。

(2) 防合作错的量子码

前面已表明,量子纠错方案适合于纠随机量子错。但在实际中,量子比特有可能发生合作消相干,结果导致各个比特出错的概率相互关联,此即合作量子错。设计用来纠随机错的量子编码是否适合于纠合作量子错? 这个问题还有待于解决。已有的研究可以肯定的一点是,对于克服合作消相干,利用纠随机错的量子码不是一种高效率的方案。事实上,已经发现更好的方案用来克服合作量子错。有别于量子纠错编码,这些方案防错而不纠错,它们本质性地利用了量子比特消相干过程中的合作效应。

Palma 等和中科大郭光灿领导的研究小组曾先后考察了 2 个比特或多个比特消相干和一般耗散过程中的合作效应,其中一种理想情况,即集体消相干(完全合作消相干)最值得注意。集体消相干和独立消相干具有明显不同的特征,其中最重要的一点区别为,对于集体消相干,存在相干保持态。相干保持态是一类特殊的能完全保持量子相平性的输入态,它可以表示为某个力学量的 1 组本征态,该力学量的形式依赖于具体的消相干模型。在合作消相干克服方案中,相干保持态得到了本质性的利用。这些方案一般都先建立相干保持态,然后将量子比特的输入态编码为相干保持态。最近的研究结果表明,这一想法具有广泛的应用价值。此方案基于量子比特的配对,配对的 2 个比特要求发生集体消相干,但不同对之间的量子比特既可以独立消相干,也可以合作消相干。对于量子比特对,存在相干保持态,从而可以将比特的一般输入态编码为比特对的相干保持

态，以达到克服消相干的目的。相比于量子纠错编码，此方案具有适用范围广、效率高等特点。它只需要用 2 比特来编码 1 比特，而且该编码可以很简单地用量子控制非门来实现。该方案还可以进一步推广用来克服量子门操作中的消相干，这只需要用作用于比特对的量子逻辑门来取代作用于比特的量子逻辑门，我们证明，作用于比特对的量子逻辑门仍然可以构成一个通用量子门集。

量子纠错编码假定了各个量子比将独立地发生消相干，另一方面，现有的几种合作消相干克服方案又利用了相干保持态，而相干保持态建立在某些量子比特发生集体消相干的假设之上。独立消相干和集体消相干显然都是一种理想情况，一个重要的问题是，对于具体的量子计算机，哪种假定更为合理？现在实验上已经提出几种量子计算机模型，对每种模型，都有多种噪声对消相干过程有贡献。最近的工作表明，不同噪声引起的消相干具有十分不同的特性：某些噪声引起独立消相干，另外一些噪声引起集体消相干或一般的合作消相干；有的噪声随时间增长速度快，另一些噪声随时间增长速度慢。为了使量子编码在实际中行之有效，有必要先根据具体的量子计算机和噪声模型，来分析其消相干特性。根据此特性，选择合适的量子纠错或防错编码，或者这两种方案的结合。

1.8 量子信息相关定理及其理论诞生年表

1948 年　信息理论的诞生(C. E. Shannon 1948)

1973 年　Holevo 界限定理(A. S. Holevo 1973)

1973 年　可达到信息量的理论(A. S. Holevo 1973；E. B. Davies 1978)

1984 年　BB84 协议(C. H. Bennett G. Brassard 1984)

1985 年　量子图灵机的提出(D. Deutsch 1985)

1992 年　量子高密度代码理论(C. H. Bennett S. J. Wiesner 1992)

1993 年　Holevo 界限定理向无限维的扩展(H. P. Yuen，M. Ozawa 1993)

1993 年　量子离物传态理论(C. H. Bennett G. Brassard C. Crepéau R. Jozsa A. Peres W. K. Wootters 1993)

1994 年　基于量子计算机的质数因数分解的快速算法(P. W. Shor 1994)

1995 年　量子信息源编码理论(Schumacher 1995)

1995 年　量子纠错编码理论(P. W. Shor A. M. Steane 1995)

1996 年　量子纯粹状态信道编码定理(P. Hausladen，R. Jozsa，B. Schumacher，M. Westmoreland，W. K. Wootters 1996)

1996 年　CSS 代码理论(A. R. Calderbank P. W. Shor 1996；N. J. ASteane 1997)

1996 年　量子纠缠态纯化协议(C. H. Bennett G. Brassard S. Popescu B. Schumacher J. A. Smolin W. K. Wootters 1996)

1996 年　基于量子计算机的数据库检索问题的快速算法(L. K. Grover 1996)

1996 年　面向混合状态一般化量子信道编码定理(A. S. Holevo 1996; B. Schumacher and M. Westmoreland 1997)

1997 年　Stabilizer 代码理论(D. Gottesman 1996; A. R. Calderbank E. M. Rains P. W. Shor N. J. ASloane 1997)

1997 年　量子信道容量理论(B. Schumacher M. D. Westmoreland 1997; A. S. Holevo 1998)

1998 年　面向连续系一般化量子信道编码定理(A. S. Holevo, 1998)

1998 年　量子信赖函数的理论(纯粹状态)(M. V. Burnashev, A. S. Holevo 1998)

1998 年　量子切断率理论(纯粹状态)(M. Ban, K. Kurokawa, O. Hirota 1998)

1998 年　超加法性的存在性证明(M. Sasaki, K. Kato, M. Izutsu, O. Hirota 1998)

1998 年　信道容量的数值解法(H. Nagaoka 1998)

1998 年　信道编码的逆定理的证明、量子有本界限的证明(T. Ogawa, H. Nagaoka 1998)

1999 年　戴维斯定理的扩展(M. Sasaki, S. M. Barnett, R. Jozsa, M. Osaki, O. Hirota 1999)

1999 年　简单状态最大相信息量:C1 的严密证明(纯粹 2 维)(M. Ban, K. Kurokawa, O. Hirota 1999; Osaki 1999)

1999 年　信道容量的解析解　离散系:对称信号(K. Kato, M. Osaki, O. Hirota 1999)

1999 年　信道容量的解析解　连续系:高斯信道(A. S. Holevo, M. Sohma, O. Hirota 1999)

第 2 章 经典比特与量子比特

通过第一章的学习我们知道:构成经典计算机内信息的最小单位—比特—是用二进制中的 0 和 1 表示,所有的信息都是由 0 与 1 组成、保存、运算及传递的。物理上,比特是由一个实际物理系统来实现。以开关为例,"关"代表 0,"开"代表 1;也可以用光纤中的光脉冲,磁带中的磁化性质等来实现。在传统的计算机里,0 与 1 是由电位的高低来表示,这种用传统比特存储和处理信息的手法称为经典信息。如果我们用量子力学中光子的两个极化状态,或电子的两个自旋状态,或原子的基态和激发态来实现信息中 0 与 1 的两个状态(记为$|0\rangle$和$|1\rangle$),这样的比特称为量子比特,用量子比特来存储和处理信息,则称为量子信息。

量子信息与经典信息最大的不同在于:经典信息中,比特只能处在一个状态,非 0 即 1;而在量子信息中,量子比特可以同时处在状态$|0\rangle$和状态$|1\rangle$中。量子比特的这一特性来自量子力学的状态叠加原理,即如果状态$|0\rangle$和$|1\rangle$是两个互相独立的量子态,它们的任意线性叠加$|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$也是某一时刻的一个量子态,而系数$\alpha$与$\beta$的绝对值的平方则描述系统分别处在$|0\rangle$和$|1\rangle$的概率。这使得每个量子比特可表示的信息比经典比特多得多,量子比特能利用不同的量子叠加态记录不同的信息,在同一位置上可拥有不同的信息。然而量子态是非常不稳定的,并且根据量子力学的测不准原理,任何观测都会立刻改变系统的状态,因此量子信息的实际可行性一直受到怀疑。但这恰恰保证了量子信息的绝对安全性,因为任何窃听(测量)者都会被发现。

在这一章节,我们首先介绍量子通信系统、量子计算机系统等量子信息处理系统的基本存储单元—量子比特(qubit:quantum bit),然后说明经典比特(bit)与量子比特的对应关系,即经典比特在量子比特的表示和演算中的作用,最后介绍在量子比特上实施的几种基本演算。

2.1 经典比特、量子比特及其叠加状态

在经典信息处理过程中,记述经典信息的二进制存储单元称为经典比特

(bit),经典比特由经典状态(如电压的高低) 的 1 和 0 表示。从物理角度讲,bit 是个两态系统,它可以制备为两个可识别状态中的一个。对于量子信息而言,记述量子信息的存储单元称为量子比特(qubit)。一个 qubit 的状态是一个二维复数空间的矢量,它的两个极化状态|0⟩和|1⟩对应于经典状态的 0 和 1。由于量子状态具有可叠加的物理特性,因此描述量子信息的 qubit 使用二维复数向量的形式表示量子信息的模拟状态。一个 qubit 与只能取 0 和 1 值的 bit 不同,理论上告诉我们 qubit 可以取无限多个值。以下的讨论是假设 qubit 与量子状态为同一事物。

qubit 的两个极化状态|0⟩和|1⟩也是二维复数列向量,它们构成二维复数空间的一对正规直交基底。也就是说复数向量|0⟩和|1⟩的长度均为 1,且|0⟩和|1⟩的内积为 0,因此可以用以下的方法选择|0⟩和|1⟩。例如:可以选择

$$|0\rangle=\begin{bmatrix}1\\0\end{bmatrix},|1\rangle=\begin{bmatrix}0\\1\end{bmatrix} \tag{2.1}$$

也可以选择

$$|0\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix},|1\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} \tag{2.2}$$

无论选择哪一对,它们的向量长度均为 1,计算其内积:无论是式(2.1)

$$\begin{bmatrix}1 & 0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}=1\times0+0\times1=0$$

还是式(2.2)

$$\frac{1}{2}\begin{bmatrix}1 & 1\end{bmatrix}\begin{bmatrix}1\\-1\end{bmatrix}=\frac{1}{2}(1\times1+1\times(-1))=0$$

结果都为 0。因此无论选择哪一组 qubit 对,我们都可以确认它们是直交的基底。

决定状态|0⟩和|1⟩对应于(选择)怎样的复向量,这依赖于实际的信息的载体采用哪一类微观粒子。假定采用光量子的偏光状态,那么可以认为 qubit 的状态|0⟩和|1⟩分别对应于两个相互直交的偏光状态;若采用电子的自旋方向,那么可以把 qubit 的状态|0⟩和|1⟩看成是电子的不同自旋方向。若采用二能级原子模型,那么可以把 qubit 的状态|0⟩和|1⟩看成是电子能级处在基态或激活状态上等。

qubit 与 bit 本质上的不同点在于,除了|0⟩和|1⟩状态以外,qubit 是以式

(2.3)给出的|0⟩和|1⟩两个状态的任意重叠组合状态。假定 α 与 β 是一对任意的满足归一化的复数，则量子比特$|\varphi\rangle$是式(2.3)描述的所有可能的叠加状态。

$$|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle \tag{2.3}$$

特别是如若状态|0⟩和|1⟩采用式(2.1)表示，$|\varphi\rangle$作为二维复向量可以写成

$$|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle=\alpha\begin{bmatrix}1\\0\end{bmatrix}+\beta\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}\alpha\\\beta\end{bmatrix}$$

由此可知，任意的二维复向量都可以看成是 qubit 的瞬间值。以这样一种叠加状态为例，能够表示光的偏光状态。如果以状态|0⟩和|1⟩分别表示水平偏光(↔)和垂直偏光(↕)，则可以用以下的方式表示两种斜偏光和右圆偏光：

对应于偏光↗的状态：$\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$

对应于偏光↘的状态：$\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle$

对应于右圆偏光○的状态：$\frac{1}{\sqrt{2}}|0\rangle+\frac{\mathrm{i}}{\sqrt{2}}|1\rangle$

此处 i 表示虚数单位。

服从量子理论的公理体系，以下假设 ket(右矢 0 和右矢 1)与其常数倍一视同仁，也就是说对于常数 $a\neq0$，$a|\varphi\rangle$与$|\varphi\rangle$被视为是同一个 qubit。在没有特别说明的情况下，假定 ket 的长度规范为 1。因此式(2.3)中的 α 与 β 必须满足下列关系式

$$|\alpha|^2+|\beta|^2=1$$

注：二维复向量$\begin{bmatrix}a_1\\a_2\end{bmatrix}$和$\begin{bmatrix}b_1\\b_2\end{bmatrix}$的内积，可以表示为$\begin{bmatrix}a_1^* & a_2^*\end{bmatrix}\begin{bmatrix}b_1\\b_2\end{bmatrix}=a_1^*b_1+a_2^*b_2$，其中“*”表示共轭复数。

2.2 量子比特的测定

对于经典 bit，我们能够准确地判断某一个 bit 在某一时刻取值是 0 还是 1。但对于量子比特 qubit 来说，要想正确地判定某一个 qubit 在某一时刻的状态，也就是说给定一个 qubit

$$|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$$

我们通常不可能正确地知道 α 和 β 的值。

以下来讲述如何从一个 qubit 获得所要的(经典)信息。

通过一个被称为是测定或观测的过程,可以把一个 qubit 的状态以概率幅(概率区域)的方式变换成 bit 信息。也就是说通过特殊的测定,量子比特 $|\varphi\rangle$ 将以下列方式被转换,即 $|\varphi\rangle$ 以

概率 $|\langle 0|\varphi\rangle|^2$ 变换成 bit 0

概率 $|\langle 1|\varphi\rangle|^2$ 变换成 bit 1

此处记号 $\langle x|y\rangle$ 表示 ket$|x\rangle$ 与 ket$|y\rangle$ 的内积。

由于内积是线性演算,且 $|0\rangle$ 和 $|1\rangle$ 是正规直角基底,因此我们能够求出量子比特 $|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$ 的两个内积 $|0|\varphi\rangle$ 和 $|1|\varphi\rangle$ 的计算结果为

$$\langle 0|\varphi\rangle=\alpha\langle 0|0\rangle+\beta\langle 0|1\rangle=\alpha$$

$$\langle 1|\varphi\rangle=\alpha\langle 1|0\rangle+\beta\langle 1|1\rangle=\beta$$

即 $|\varphi\rangle$ 以概率 $|\alpha|^2$ 取值 bit 0、以概率 $|\beta|^2$ 取值 bit 1。特别当 $\alpha=1$ 时 $|\varphi\rangle$ 取值 0 的概率为 1,当 $\beta=1$ 时 $|\varphi\rangle$ 取值 1 的概率为 1。在这样的情况下,qubit 的行为与 bit 完全一致。从这个意义上来说,qubit 包含了经典 bit,是信息状态的更一般性表示。

读者在有关测定的过程中应该注意的是:基于某个特定的(状态 $|0\rangle$ 和 $|1\rangle$ 的选择)方法其测定的结果是确定的;如果改变状态 $|0\rangle$ 和 $|1\rangle$ 的选择方法,则由测定获取的经典比特值,即 bit 0 和 bit 1 的发生概率将发生变化。例如,由向量表示的 qubit 为

$$|\varphi\rangle=\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$

如果选择式(2.2)给出的状态 $|0\rangle$ 和 $|1\rangle$ 为态矢空间的态基,则状态 $|\varphi\rangle$ 将被表示成

$$\begin{aligned}|\varphi\rangle&=\frac{\alpha+\beta}{2}\begin{bmatrix}1\\ 1\end{bmatrix}+\frac{\alpha-\beta}{2}\begin{bmatrix}1\\ -1\end{bmatrix}\\&=\frac{\alpha+\beta}{\sqrt{2}}|0\rangle+\frac{\alpha-\beta}{\sqrt{2}}|1\rangle\end{aligned}\tag{2.4}$$

那么该状态 $|\varphi\rangle$ 取 bit 值的概率就分别为

取 bit 0 的概率为 $\frac{|\alpha+\beta|^2}{2}$

取 bit 1 的概率为 $\frac{|\alpha-\beta|^2}{2}$

因此，根据状态$|0\rangle$和$|1\rangle$的不同选择方法，即使是同一个量子比特$|\varphi\rangle$通过测定其变换过程也会发生变化(图 2-1)。

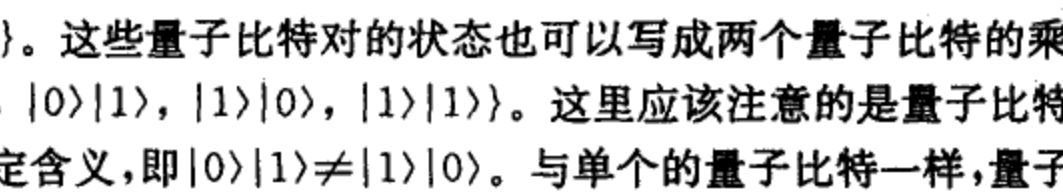


图 2-1 qubit 的测定

例题 2.1 给定量子比特$|\varphi\rangle$：

$$|\varphi\rangle=\begin{bmatrix}1\\0\end{bmatrix}$$

如果选择式(2.1)给出的状态$|0\rangle$和$|1\rangle$为态矢空间的态基，则

$$|\varphi\rangle=|0\rangle$$

通过测定量子比特$|\varphi\rangle$取值肯定为 bit 0 的概率是 1。如果选择由式(2.2)给出的状态$|0\rangle$和$|1\rangle$为态矢空间的态基的话，则

$$|\varphi\rangle=\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$$

此时通过测定量子比特$|\varphi\rangle$取值 bit 0 和 bit 1 的概率分别都是 0.5。

2.3 量子比特对与量子比特列阵

在这一节里将讨论一个以上(复数个)的量子比特以及它们的性质。如果用两个经典比特表述信息，可以获取 4 个状态{00,01,10,11}。但是如果拥有两个量子比特，或者说拥有一个量子比特对，那么将拥有 4 个正规直交基底{$|00\rangle$，$|01\rangle$，$|10\rangle$，$|11\rangle$}。这些量子比特对的状态也可以写成两个量子比特的乘积的形式，即{$|0\rangle|0\rangle$，$|0\rangle|1\rangle$，$|1\rangle|0\rangle$，$|1\rangle|1\rangle$}。这里应该注意的是量子比特列的排列顺序有其特定含义，即$|0\rangle|1\rangle\neq|1\rangle|0\rangle$。与单个的量子比特一样，量子比特对也可以取这些基底状态的叠加状态。一般来说使用复数 α_{00}，α_{01}，α_{10}，α_{11}，量子比特对$|\varphi\rangle$可以写成

$$|\varphi\rangle=\alpha_{00}|00\rangle+\alpha_{01}|01\rangle+\alpha_{10}|10\rangle+\alpha_{11}|11\rangle$$

当然量子比特对也必须规范化，因此 α_{00}，α_{01}，α_{10}，α_{11} 必须满足下列等式：

$$|\alpha_{00}|^2+|\alpha_{01}|^2+|\alpha_{10}|^2+|\alpha_{11}|^2=1$$

与单个的量子比特情况相同，通过测定量子比特对可获得其值，它们的值是经典比特列值 00，01，10，11 的其中之一。取经典比特各种列值的概率为

测定结果	出现概率
00	$\|\langle 00\|\varphi\rangle\|^2=\|\alpha_{00}\|^2$
01	$\|\langle 01\|\varphi\rangle\|^2=\|\alpha_{01}\|^2$
10	$\|\langle 10\|\varphi\rangle\|^2=\|\alpha_{10}\|^2$
11	$\|\langle 11\|\varphi\rangle\|^2=\|\alpha_{11}\|^2$

(2.5)

在第一章的讨论中我们知道基底状态$|00\rangle$，$|01\rangle$，$|10\rangle$，$|11\rangle$分别能够用 4 维复向量表示如下：

$$|00\rangle=\begin{bmatrix}1\\0\\0\\0\end{bmatrix},\ |01\rangle=\begin{bmatrix}0\\1\\0\\0\end{bmatrix},\ |10\rangle=\begin{bmatrix}0\\0\\1\\0\end{bmatrix},\ |11\rangle=\begin{bmatrix}0\\0\\0\\1\end{bmatrix} \tag{2.6}$$

在量子比特对的情况下，我们能够只测定其中某一个 qubit 的值。例如考虑只测定量子比特对的第一位 qubit 值的场合：其取值 bit 0 的概率等于同时测定第二位 qubit 时 00 出现的概率$|\langle 00|\varphi\rangle|^2$ 加上 01 出现的概率$|\langle 01|\varphi\rangle|^2$ 之和；取值 bit 1 的概率等于同时测定第二位 qubit 时 10 出现的概率$|\langle 10|\varphi\rangle|^2$ 加上 11 出现的概率$|\langle 11|\varphi\rangle|^2$ 之和，也就是量子比特对第一位测定结果为

取 bit 0 的概率是：$|\langle 00|\varphi\rangle|^2+|\langle 01|\varphi\rangle|^2$

取 bit 1 的概率是：$|\langle 10|\varphi\rangle|^2+|\langle 11|\varphi\rangle|^2$

这里要提醒读者注意的是，在做这样的测定时必须注意到测定后剩余的第二位 qubit 的状态将发生什么样的变化，由式(2.5)对应于测定结果，剩余的第二位 qubit 的状态将发生下列变化，即测定结果为

bit 0 的场合：$\dfrac{\alpha_{00}|0\rangle+\alpha_{01}|1\rangle}{\sqrt{|\alpha_{00}|^2+|\alpha_{01}|^2}}$

bit 1 的场合：$\frac{\alpha_{10}|0\rangle+\alpha_{11}|1\rangle}{\sqrt{|\alpha_{10}|^2+|\alpha_{11}|^2}}$

特别应该注意的是测定后剩余的第二位 qubit 其状态并非单纯的 $a|0\rangle+b|1\rangle$，例如 $\alpha_{00}|0\rangle+\alpha_{01}|1\rangle$，而是要除以 $\sqrt{|\alpha_{00}|^2+|\alpha_{01}|^2}$ 后再一次正规化。

例题 2.2 让我们来考察一下第一章中提到的称为贝尔状态基之一（或称为 EPR 对）的量子比特对 $|\beta_{00}\rangle$

$$\frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

首先由式(2.5)可知，当这个量子比特对被同时测定时，其状态值为 bit 00 或 bit 11 的概率都是 $|\frac{1}{\sqrt{2}}|^2=\frac{1}{2}$；为 bit 01 或 bit 10 的概率都是 0。

另外，测定该量子比特对的第一位 qubit 状态时，出现 bit 0 或 bit 1 的概率均为 $\frac{1}{2}$，而测定后剩余的第二位 qubit 的状态是：当第一位 qubit 测定的结果为 bit 0 的时候、剩余的 qubit 的状态是 $|0\rangle$；当第一位 qubit 测定的结果为 bit 1 的时候、剩余的 qubit 的状态是 $|1\rangle$。因此在该贝尔状态的场合，没有被测定的 qubit 的状态总是向被测定的 qubit 状态的结果一方迁移，即测定剩余的 qubit 获取的结果与最初的测定结果总是完全一致的。

考虑更一般的情况，我们能够考察由 n 个 qubit 组成的量子比特列阵。由 n 个 qubit 组成的列阵其正规直交基底是由 2^n 个形为 $|x_1x_2\cdots x_n\rangle$ 的 ket 组成的，其中 $x_i(i=1, 2,\cdots,n)$ 取 0 或 1 表示。当然，这些 qubit 列阵能够取这些正规直交基底的重合状态，且使用 2^n 维的复向量来表示。测定这样的 qubit 列阵 $|\varphi\rangle$，其取 bit 列为 $x_1x_2\cdots x_n$ 值的概率是由 $|\langle x_1x_2\cdots x_n\varphi\rangle|^2$ 决定的。有关部分性的测定可采取与 qubit 对的部分性测定同样的方法。

2.4 量子比特的基本操作

在第一章节的有关部分中，已经介绍了在量子通信及量子计算机等量子系统中对 qubit 能够实施的基本操作（演算）及其操作的性质。

众所周知，在经典数字计算机上可对单一的 bit 用逻辑非门（NOT Gate）实施否定演算，也就是将 bit 1 反转成 bit 0 或将 bit 0 反转成 bit 1 的演算。对于 qubit 来说，与否定演算对应的演算被称为 bit 反转演算，该演算对应量子逻辑非门（quantum NOT Gate）。Bit 反转演算将状态 $|0\rangle$ 反转成状态 $|1\rangle$，或将状态

$|1\rangle$反转成状态$|0\rangle$。更具一般性的是关于$|0\rangle$和$|1\rangle$的叠加状态，假定 bit 反转演算是线性算子，即对于叠加状态

$$\alpha|0\rangle+\beta|1\rangle$$

执行 bit 反转演算的结果是

$$\alpha|1\rangle+\beta|0\rangle$$

因此，一般地说有关 qubit 的量子演算对于量子叠加状态具有线性性质。

量子逻辑非门(bit 反转演算子)能够用下列 2×2 的泡利矩阵 σ_x 表示：

$$X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

称为 X-Gate。事实上，如果状态 $\alpha|0\rangle+\beta|1\rangle$用以下的列向量表示：

$$\alpha|0\rangle+\beta|1\rangle=\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$

对其实施 bit 反转演算将得到以下结果：

$$X\begin{bmatrix}\alpha\\ \beta\end{bmatrix}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}=\begin{bmatrix}\beta\\ \alpha\end{bmatrix} \tag{2.7}$$

显然，这就是状态 $\alpha|1\rangle+\beta|0\rangle$的向量表示。

以后对于 qubit 量子状态$|\varphi\rangle$作量子 bit 反转演算，所得结果将用 $X|\varphi\rangle$表示。我们将X－Gate称为 bit 反转演算子。

一般情况下，在量子系统中对单一 qubit 实施的量子演算都能够用与 X 同样的 2×2 矩阵表示。但是，并非所有的 2×2 矩阵都可以作为单一 qubit 的量子演算矩阵，下面来看一看 2×2 矩阵作为单一 qubit 的量子演算矩阵的条件。我们首先想到的是量子状态的模通常必须规范化，即长度为 1。意思是任意单一 qubit 的量子状态

$$|\varphi\rangle=\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$

必须满足等式$|\alpha|^2+|\beta|^2=1$。因此，对 qubit 的量子状态$|\varphi\rangle$作量子演算 U 获得的新状态

$$U|\varphi\rangle=\begin{bmatrix}\alpha'\\ \beta'\end{bmatrix}$$

也必须满足规范化要求，即必须满足$|\alpha'|^2+|\beta'|^2=1$。由线性代数学得知满足如此条件的2×2矩阵必须是酉矩阵。进而复矩阵U是酉矩阵的充分必要条件是其必须满足方程式

$$U^*U=I \tag{2.8}$$

此处U^*为U伴随或称为U的诶尔米特共轭矩阵，$U^*=(U^T)^*$。即U^*是U的转置且所有元素取共轭复数的矩阵。I表示2×2单位矩阵。前面介绍的bit反转演算子X，因其满足式(2.8)

$$X^*X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}=I$$

所以X－Gate是酉矩阵。

事实上，判断2×2矩阵能否成为单个qubit量子状态的演算算子的条件就是检验其是否满足式(2.8)。因此，从理论上说所有的酉矩阵都能成为量子演算算子。但是对于某一个酉矩阵来说，它是否能成为实际操作过程中的量子演算算子，要视其演算结果是否能够表达某一特定的物理现象，因此能够成为量子演算算子的酉矩阵是有限的。下面再看几个能够实现量子演算的酉矩阵。

下一个演算子Z被称为位相翻转演算子或称为Z－Gate。Z-Gate能够用泡利矩阵σ_z表示为

$$Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

很显然Z－Gate演算也是酉矩阵，通过Z－Gate演算看一下状态$|0\rangle$和$|1\rangle$将发生什么样的变化。这时有

$$Z|0\rangle=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix}=\begin{bmatrix}1\\ 0\end{bmatrix}=|0\rangle$$

$$Z|1\rangle=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}0\\ -1\end{bmatrix}=\begin{bmatrix}0\\ -1\end{bmatrix}=-|1\rangle$$

即对于Z－Gate演算，状态$|0\rangle$不变；状态$|1\rangle$发生位相翻转，变成$-|1\rangle$。与bit反转演算同样，以下对qubit量子状态$|\varphi\rangle$实施位相翻转演算所得结果用$Z|\varphi\rangle$表示。我们将Z－Gate称为量子位相翻转演算子。

演算子H是被称为Walsh-Hadamard变换或简称为Hadamard变换的演算。Hadamard变换的矩阵表示为

$$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

称为 H－Gate。Hadamard 变换矩阵满足式(2.8)

$$H^{*}H=\frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}=I$$

因此 H－Gate 演算是酉矩阵。演算子 H 在量子计算以及量子错误纠正代码中是使用最频繁的演算子。Qubit 量子状态$|0\rangle$和$|1\rangle$对于 Hadamard 变换的演算将发生以下的变化：

$$H|0\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix}=\frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

$$H|1\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix}=\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

同时，可以简单地得到下列等式：

$$H^{2}=HH=I$$

也就是说连续两次作 Hadamard 变换的演算等于一次恒等变换。同样，以下对量子状态$|\varphi\rangle$实施 H 演算所得结果用$H|\varphi\rangle$表示。我们将 H－Gate 称为 Hadamard 变换演算子。

例题 2.3　下列等式给出了的矩阵 Z(Z－Gate)与矩阵 X(X－Gate)的乘积：

$$ZX=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$$

很显然，其结果依然满足量子演算。因为有下列等式成立：

$$(ZX)(ZX)=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}=I$$

所以 ZX 也是酉矩阵。一般来说，因为酉矩阵的乘积依然是酉矩阵，所以到目前为止介绍的量子演算子的组合一定还是量子演算子。图 2－2 中集中了对于单一 qubit 量子状态变换的 3 个常用演算子(量子逻辑门)：

$$\alpha|0\rangle+\beta|1\rangle \longrightarrow \boxed{\mathrm{X}} \longrightarrow \beta|0\rangle+\alpha|1\rangle$$

$$\alpha|0\rangle+\beta|1\rangle \longrightarrow \boxed{\mathrm{Z}} \longrightarrow \alpha|0\rangle-\beta|1\rangle$$

$$\alpha|0\rangle+\beta|1\rangle \longrightarrow \boxed{\mathrm{H}} \longrightarrow \frac{\alpha+\beta}{\sqrt{2}}|0\rangle+\frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

图 2-2 对于单一 qubit 的 3 个常用演算子

回顾在第 1 章的“一个量子比特的布洛赫球表示法”中，通过对布洛赫球表示法的理解，可以将任意单个 qubit 量子状态的酉变换分解成若干个以下形式的旋转矩阵：

$$\begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{r}{2} \end{bmatrix}$$

以及绕$\hat{Z}$轴旋转的一个逻辑门

$$\begin{bmatrix} \mathrm{e}^{-\mathrm{i}\beta/2} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\beta/2} \end{bmatrix}$$

再乘上一个形式为 $\mathrm{e}^{\mathrm{i}\alpha}$（全局变换过程）因子定数倍的乘积。也就是说任意 2×2 酉矩阵都能够被分解成如下形式：

$$U=\mathrm{e}^{\mathrm{i}\alpha}\begin{bmatrix} \mathrm{e}^{-\mathrm{i}\beta/2} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\beta/2} \end{bmatrix}\begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}\cdots\begin{bmatrix} \mathrm{e}^{-\mathrm{i}\delta/2} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\delta/2} \end{bmatrix}$$

这里 α，β，γ 和 δ 都是实数。表达式中的第 2 个矩阵表示一个通常的旋转，而第一和最后一个矩阵完全可以理解为一个球在一个不同平面上的旋转。这样的分解能够用来正确地规定和理解执行一个任意单一 qubit 量子逻辑门的规则。

以上讲述了有关单一 qubit 的表示、测量与演算的基本概念，并着重介绍了针对单一 qubit 的 3 种演算及其相应的量子逻辑门。从第一章的“1.5 量子逻辑电路简介”图 1-7 中我们可以看到经典单一 bit 有且仅有一个对应逻辑非门的取反演算，而单一 qubit 对应的常用演算就有 3 个。从图 1-8 中又可以发现对于两个经典 bit 有若干个演算对应若干个逻辑门，但两个 qubit 对应的常用演算

仅有一个，即 Controlled - NOT - Gate。作为本节的最后部分，将介绍对于 qubit 对（两个 qubit）来说是最基本的一个演算：控制非门（Controlled - NOT - Gate）演算。

对应两个 qubit 的常用演算 Controlled - NOT - Gate 演算如图 2 - 3 所示：

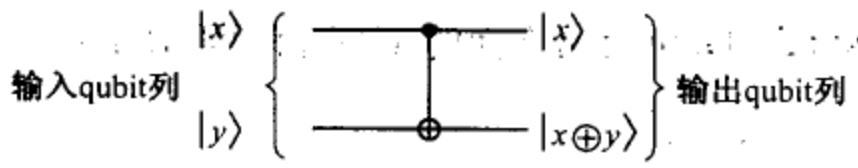


图 2 - 3　控制非门（Controlled - NOT - Gate）

Controlled - NOT - Gate 是一个 2 位 qubit 输入和 2 位 qubit 输出的量子回路，由第一章的相关内容我们也知道这是一个没有能耗的可逆运算。由状态|0⟩和|1⟩组成的 2 位 qubit 列构成输入状态列，当输入为|xy⟩（或表示为|x⟩|y⟩）时其输出为|$xx\oplus y$⟩（或表示为|x⟩|$x\oplus y$⟩）。此处⊕表示排他逻辑和。由逻辑演算规则我们可以推导出 Controlled -NOT -Gate 将给出下列的输入、输出关系：

输入状态		输出状态
|00⟩	→	|00⟩
|01⟩	→	|01⟩
|10⟩	→	|11⟩
|11⟩	→	|10⟩

分析输出状态的结果可以知道：Controlled - NOT - Gate 的控制被限制在第一个 qubit，当第一个 qubit 为 1 时，此时的第二个 qubit 若为|1⟩则反转成|0⟩，若为|0⟩时反转成|1⟩。Controlled - NOT - Gate 对于叠加状态是线性算子。也就是说当一叠加状态

$$c_{00}|00\rangle+c_{01}|01\rangle+c_{10}|10\rangle+c_{11}|11\rangle \tag{2.9}$$

被送入 Controlled - NOT - Gate 时，其输出状态将是

$$c_{00}|00\rangle+c_{01}|01\rangle+c_{10}|11\rangle+c_{11}|10\rangle \tag{2.10}$$

其次，再来看一下 Controlled - NOT - Gate 的矩阵表示。如果 qubit 对的基底状态用下列向量表示：

$$|00\rangle=\begin{bmatrix}1\\0\\0\\0\end{bmatrix},\ |01\rangle=\begin{bmatrix}0\\1\\0\\0\end{bmatrix},\ |10\rangle=\begin{bmatrix}0\\0\\1\\0\end{bmatrix},\ |11\rangle=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

则 Controlled - NOT - Gate 可由下面的 4×4 酋矩阵表示：

$$U=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} \tag{2.11}$$

实际上，式(2.9)所示状态的向量可以表示为

$$c_{00}|00\rangle+c_{01}|01\rangle+c_{10}|10\rangle+c_{11}|11\rangle=\begin{bmatrix}c_{00}\\c_{01}\\c_{10}\\c_{11}\end{bmatrix}$$

它与式(2.11)的矩阵 U 的乘积结果为

$$U\begin{bmatrix}c_{00}\\c_{01}\\c_{10}\\c_{11}\end{bmatrix}=\begin{bmatrix}c_{00}\\c_{01}\\c_{11}\\c_{10}\end{bmatrix}=c_{00}|00\rangle+c_{01}|01\rangle+c_{10}|11\rangle+c_{11}|10\rangle$$

与(2.10)式一致。

上面就 qubit 对介绍了 Controlled - NOT - Gate 演算。下面的图 2 - 4 给出了由 3 个 Controlled - NOT - Gate 组成的简单量子回路。

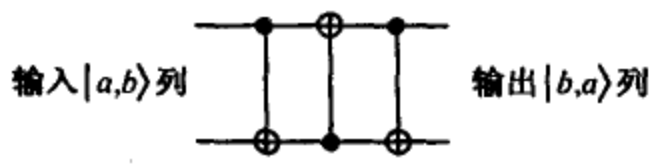


图 2 - 4　调换 qubit 对量子状态的逻辑回路

有关对量子回路的理解应该强调的是：回路的阅读从左到右，量子回路中的每一条线表示一个量子通道而并非物理上的导线，一条线上连接各变换点的线段可以理解成两个变换点之间的一次瞬间的时间经过(滞后)，或者看成是光子一样的微观粒子经过空间从一点到另一点的轨迹。图 2.4 表示的量子逻辑回路完成了一个简单但却是非常有用的任务，就是调换一个 qubit 对的量子状态。式

(2.12)给出了图 2.4 完成一个 qubit 对$|a, b\rangle$量子状态调换的分解过程。

$$|a, b\rangle \vdash\!\!\rightarrow |a, a\oplus b\rangle$$

$$\vdash\!\!\rightarrow |a\oplus(a\oplus b), a\oplus b\rangle = |b, a\oplus b\rangle$$

$$\vdash\!\!\rightarrow |b, (a\oplus b)\oplus b\rangle = |b, a\rangle$$

注意:这里的加法都是取 2 的模数,所以图 2 - 4 可以完成一个 qubit 对状态的交换。

第 3 章　量子纠缠状态及其应用

量子纠缠状态(Entangled State)指的是两个或多个量子系统之间的非定域、非经典的关联,是量子系统内各子系统或各自由度之间关联的力学属性。量子纠缠状态是微观世界物质间的特有现象,因此也是量子信息理论中特有的概念。量子态能够纠缠是实现信息高速的不可破译通信的理论基础。本章在讲述量子纠缠状态之后,解说有关量子纠缠状态的应用。

3.1　量子纠缠状态

从第一章的讨论我们知道:如果 qubit 列的叠加状态无法用各 qubit 的张量乘积表示,这种叠加状态就称为量子纠缠状态。

例题 3.1　例如有一量子叠加状态

$$\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|10\rangle=\frac{1}{\sqrt{2}}|0\rangle|0\rangle+\frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

由于其最后一位 qubit 位都是$|0\rangle$,因此能够将其写成两个 qubit $\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$与$|0\rangle$的乘积

$$\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)|0\rangle$$

但是,对于下列的叠加状态

$$\frac{1}{\sqrt{2}}|01\rangle+\frac{1}{\sqrt{2}}|10\rangle$$

无论采用什么样方法都无法写成两个 qubit 的乘积。这个叠加状态就称为量子纠缠状态。

再看下列的叠加状态:

$$\frac{1}{2}(|010\rangle+|011\rangle+|100\rangle+|101\rangle)$$

我们能够将其写成下列的乘积形式：

$$\left(\frac{1}{\sqrt{2}}|01\rangle+\frac{1}{\sqrt{2}}|10\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)$$

但乘积的左因子的最初两位 qubit 是纠缠状态，所以这个叠加状态也是纠缠状态。

从第一章的“1.4 经典解读”的 1.4.2 小节的“贝尔态基与量子隐形传态”的有关内容中，知道在量子力学中有一个著名的贝尔不等式，我们称贝尔算符的全套本征态为贝尔态基，贝尔态基由如下 4 个态矢组成：

$$|\beta_{00}\rangle=\frac{|00\rangle+|11\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}$$

$$|\beta_{01}\rangle=\frac{|01\rangle+|10\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\1\\0\end{bmatrix}$$

$$|\beta_{10}\rangle=\frac{|00\rangle-|11\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\-1\end{bmatrix}$$

$$|\beta_{11}\rangle=\frac{|01\rangle-|10\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\-1\\0\end{bmatrix}$$

显然，4 个贝尔态基都是纠缠状态。贝尔态基在量子信息理论中，特别是在量子纠错编码理论中有着不可替代的作用。为了深入地理解量子纠缠状态的性质，下面将简单地介绍量子纠缠状态的生成法。图 3-1 给出了稍微复杂的量子状态变换回路，它可以生成贝尔态基。

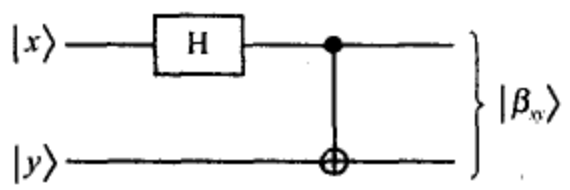


图 3-1　生成贝尔状态的量子状态变换回路

当回路的输入状态是$|xy\rangle$qubit 对，其中一个 qubit 做 Hadamard 变换后再与另一个 qubit 同时经过 Controlled - NOT - Gate 变换后得到输出结果$|\beta_{xy}\rangle$就是贝尔态基之一。4 个基底$|00\rangle$、$|01\rangle$、$|10\rangle$、$|11\rangle$经过图 3 - 1 所示的状态变换回路后输出下列 4 个结果：

输入状态	输出状态
$\|00\rangle$	$\|\beta_{00}\rangle=\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$
$\|01\rangle$	$\|\beta_{01}\rangle=\frac{\|01\rangle+\|10\rangle}{\sqrt{2}}$
$\|10\rangle$	$\|\beta_{10}\rangle=\frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$
$\|11\rangle$	$\|\beta_{11}\rangle=\frac{\|01\rangle-\|10\rangle}{\sqrt{2}}$

(3.1)

其实输入 qubit 对的状态为$|00\rangle$时，经 H - Gate 后的该 qubit 对的状态成为

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|0\rangle=\frac{|00\rangle+|10\rangle}{\sqrt{2}}$$

再经过 Controlled - NOT - Gate 变换，便可得到式(3.1)所示的状态输出结果：

$$\frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

至此我们知道对于这样的 qubit 对经过如上的状态变换回路可以生成纠缠状态。式(3.1)给出的 4 种输出状态$\{\beta_{00}, \beta_{01}, \beta_{10}, \beta_{11}\}$称为贝尔状态，也称为 EPR 状态或 EPR 对。$\{\beta_{00}, \beta_{01}, \beta_{10}, \beta_{11}\}$冠以这些名称，一是出自于发现这种状态不可思议性质的三位物理学者 Einstein，Podolsky，Rosen 姓名头文字的排列，二是出自于证明了这种状态对的相关性比经典相关性具有更强性质的物理学者贝尔(Bell)。

贝尔状态是 qubit 对的一组正规直交基底。

(1) 因为$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$是正规直交基底，如果计算内积$\langle\beta_{xy}|\beta_{xy}\rangle$，将得到以下结果：

$$\langle\beta_{00}|\beta_{00}\rangle=\frac{(\langle 00|+\langle 11|)(|00\rangle+|11\rangle)}{2}$$

$$=\frac{\langle 00|00\rangle+\langle 11|00\rangle+\langle 00|11\rangle+\langle 11|11\rangle}{2}$$

$$=\frac{1+0+0+1}{2}$$

$$=1$$

由此可知贝尔状态都已被规范化了。

(2) 另外，其正交性可从下列计算中得到：

$$\langle\beta_{00}|\beta_{10}\rangle=\frac{(\langle 00|+\langle 11|)(|00\rangle-|11\rangle)}{2}$$

$$=\frac{\langle 00|00\rangle+\langle 11|00\rangle-\langle 00|11\rangle-\langle 11|11\rangle}{2}$$

$$=\frac{1+0-0-1}{2}$$

$$=0$$

下面来看一看测定一个纠缠状态时，纠缠状态所呈现出的性质。以具有代表性的纠缠状态——贝尔状态为例：

$$|\beta_{00}\rangle=\frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

在对贝尔状态$|\beta_{00}\rangle$实施测定时，通过测定各个 qubit 列获得的概率是

输出 00 的概率为　　$|\langle 00|\beta_{00}\rangle|^2=\frac{1}{2}$

输出 01 的概率为　　$|\langle 01|\beta_{00}\rangle|^2=0$

输出 10 的概率为　　$|\langle 10|\beta_{00}\rangle|^2=0$

输出 11 的概率为　　$|\langle 11|\beta_{00}\rangle|^2=\frac{1}{2}$

从结果中可知道，贝尔状态 qubit 对的测定结果：当第一位的测定结果为 0 时，第二位也必定为 0；或者当第一位的测定结果为 1 时，第二位也必定为 1。正因为存在如此现象，便可以理解在量子纠缠状态中，qubit 对之间存在一种超强的作用力，即“量子相关作用”的相干关系。

量子密钥分配(Quantum key distribution，简称 QKD)是量子纠缠状态的最初的实际应用。现在假设有贝尔状态

$$|\beta_{00}\rangle=\frac{|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B}{\sqrt{2}}$$

其中第一位让用户 A 拥有，第二位让用户 B 拥有；式中$|\cdot\rangle_A$或$|\cdot\rangle_B$分别表示

用户 A 或用户 B 拥有的 qubit。从第一章的讨论我们知道，利用这个贝尔状态，A 和 B 通过 EPR 备制中心生成共通的密钥且共同拥有它们，这就完成了量子密钥配布。

根据量子密钥分配，用户 A 首先在基底$\{|0\rangle, |1\rangle\}$之上测定自己拥有的 qubit，此时 A 可以等概率获得 0 或 1 的测定结果。另一方面根据上面的结论，B 所拥有的 qubit 状态，服从于 A 的测定结果，以 概率 1 成为下列结果：

A 的测定结果	B 的测定结果
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$

因此，继 A 之后如果 B 也测定自己拥有的 qubit，结果与 A 的测定结果相同，所以 A 和 B 能够共同拥有等概率出现的 bit 0 和 bit 1。如果对于 n 个贝尔状态实施这样操作，A 和 B 就能够共同拥有 n 个 bit 量的随机生成的密钥。

3.2 量子高密度编码

在量子通信的领域中，我们利用量子纠缠状态实现量子高密度编码，量子高密度编码能够实现 1 个 qubit 传送 2 bit 信息的机能。本节就有关量子高密度编码的内容作一些说明。

现在假设送信者 A 希望送 2 bit 的经典信息给远处的收信者 B。此时送信者 A 仅仅只能利用惟一的一个 qubit 向收信者 B 传送信息，那么如何才能把 2 bit 的信息代换成 1 qubit 编码进行传送呢，下面来考虑这个问题。

在实现通信之前，让送信者和收信者各自拥有贝尔状态

$$|\beta_{00}\rangle=\frac{|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B}{\sqrt{2}} \tag{3.2}$$

中的 qubit 对的各自状态。此时$|\cdot\rangle_A$表示送信者 A 拥有的 qubit，$|\cdot\rangle_B$表示收信者 B 拥有的 qubit。例如，备制如此纠缠状态的 qubit 对的工作，可由例如中国移动通信或者中国联通这样的通信网络公司完成，并分配给送信者和收信者各方，使他们共有(注意在这个阶段，纠缠状态里没有包含任何送收信者的信息)。在送信者和收信者之间共同拥有纠缠状态之后，送信者 A 对应于自己想要发送的信息，在自己拥有的 qubit 上实施如下的操作：

希望发送的信息		对送信者拥有的 qubit 实施的操作
00	→	什么操作也不施加
01	→	施加 X－Gate 演算 $X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
10	→	施加 Z－Gate 演算 $Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
11	→	施加 X－Gate 演算和 Z－Gate 演算 ZX

送信者 A 通过上述操作，这个纠缠状态由式(3.2)的贝尔状态变化成下列状态：

希望发送的信息		施加操作后的纠缠状态
00	→	$\|\beta_{00}\rangle$
01	→	$X\|\beta_{00}\rangle=\dfrac{(X\|0\rangle_A)\|0\rangle_B+(X\|1\rangle_A)\|1\rangle_B}{\sqrt{2}}$ $=\dfrac{\|1\rangle_A\|0\rangle_B+\|0\rangle_A\|1\rangle_B}{\sqrt{2}}$ $=\|\beta_{01}\rangle$
10	→	$Z\|\beta_{00}\rangle=\dfrac{(Z\|0\rangle_A)\|0\rangle_B+(Z\|1\rangle_A)\|1\rangle_B}{\sqrt{2}}$ $=\dfrac{\|0\rangle_A\|0\rangle_B-\|1\rangle_A\|1\rangle_B}{\sqrt{2}}$ $=\|\beta_{10}\rangle$
11	→	$ZX\|\beta_{00}\rangle=\dfrac{(ZX\|0\rangle_A)\|0\rangle_B+(ZX\|1\rangle_A)\|1\rangle_B}{\sqrt{2}}$ $=\dfrac{-\|1\rangle_A\|0\rangle_B+\|0\rangle_A\|1\rangle_B}{\sqrt{2}}$ $=\|\beta_{11}\rangle$

送信者 A 在对自己拥有的 qubit 实施操作以后将自己拥有的 qubit 传送给收信者 B，此时收信者 B 拥有的 qubit 对的状态，依赖于送信信息，取不同的贝尔状态。如前所述贝尔状态$\{|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle\}$构成正规直交基底，因此通过基于贝尔状态的测定，收信者能够正确地(即概率为 1)知道 qubit 对的状态是 4 个状态中的哪一个，并能获取送信者发来的信息。具体的做法是，对应于

测定的结果用下面的方法对信息实施恢复操作即可。

判定结果		送信信息
$\|\beta_{00}\rangle$	→	00
$\|\beta_{01}\rangle$	→	01
$\|\beta_{10}\rangle$	→	10
$\|\beta_{11}\rangle$	→	11

由此实现一个 qubit 传送两位 bit 值的高密度编码。

例题 3.2 借助量子高密度编码原理，考虑送信者希望将 bit 列 10 传送给收信者。假设送信者将自己拥有的一位 qubit 施加 Z－Gate 演算的结果传送给收信者，此时收信者从纠缠状态里获得的 2 位 qubit 状态为

$$|\beta_{10}\rangle=\frac{(Z|0\rangle_A)|0\rangle_B+(Z|1\rangle_A)|1\rangle_B}{\sqrt{2}}$$

$$=\frac{|0\rangle_A|0\rangle_B-|1\rangle_A|1\rangle_B}{\sqrt{2}}$$

通过测定可以判定该 qubit 对是贝尔状态$\{|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle\}$中的某一个。因为有以下结论：

$$|\langle\beta_{00}|\beta_{10}\rangle|^2=0$$

$$|\langle\beta_{01}|\beta_{10}\rangle|^2=0$$

$$|\langle\beta_{10}|\beta_{10}\rangle|^2=1$$

$$|\langle\beta_{11}|\beta_{10}\rangle|^2=0$$

所以测定状态的结果能够肯定判断为$|\beta_{10}\rangle$，因此也就知道传送的信息为 bit 列 10。

量子高密度编码的特征是：即使送信者送出的 qubit 被收信者以外的第三者截获，截获者也无法得到正确的信息。这是因为：例如，在传送 2 个 bit 为 11 信息的场合，施加 X－Gate 演算和 Z－Gate 演算 ZX 后，送收信者的 qubit 对状态将变成

$$\frac{-|1\rangle_A|0\rangle_B+|0\rangle_A|1\rangle_B}{\sqrt{2}}$$

此时即使单独测定送信者 A 的 qubit，也只能概率为 0.5 地获得 0 或概率为 0.5

地获得 1，即收信者只能够等概率地获得 0 或 1，从这样的测定结果无法判断所截取的信息，所以信息能够被完全的保密。当然，在传送 11 以外的 2 个 bit 信息的场合也有同样的效果。

3.3　采用量子比特的通信界限

本节将对在前一节中论及的量子高密度编码问题进行更一般性的讨论，即如果送收信者之间存在一个能够传送 qubit 的且不产生误码的信道，让我们来考虑一下为了使送信者能够送出 n 个 bit 的信息，送收者之间需要采用几个 qubit来实现送收较为妥当。下面的定理解答了这个问题。

定理 3.1　假设 A 有 n 个 bit 的信息要传送给 B。假定 A 和 B 不共有纠缠状态，且无论是从 A 到 B 或是从 B 到 A，双向都可以无误地传送 qubit。此时设从 A 传送到 B 的 qubit 总数为 n_{AB}，从 B 传送到 A 的 qubit 总数为 n_{BA}，则 B 能够正确地获得 A 传送的 n 个 bit 的信息的充分必要条件是

$$n_{AB} \geqslant \left[\frac{n}{2}\right] \tag{3.3}$$

$$n_{AB} + n_{BA} \geqslant n \tag{3.4}$$

式(3.3)和(3.4)同时成立，而且即使 A 与 B 共有无数个纠缠状态，式(3.3)依然成立。

图 3-2 给出了实际上通信可能的 n_{AB} 和 n_{BA} 的范围。从这个定理我们立即可以获得下列的结论：

(1) 从 B 到 A 不可送信的场合，即 $n_{BA}=0$ 场合，此时 $n_{AB} \geqslant n$。这就意味着为了传送 n 个 bit 的信息至少需要 n 个 qubit，也即对应于 bit 0 和 bit 1 可以通过传送$|0\rangle$和$|1\rangle$实现通信。这样一来从传送经典 bit 的角度来看，送信时与 qubit 能够表示无限多状态的性质无关，变成了 1 个 qubit 仅能够传送 1 个 bit 的信息。

(2) 另一方面，无论如何巧妙地使用纠缠状态，传送 n 个 bit 信息时至少要传送$[n/2]$个 qubit。然而，使用量子高密度化，用$[n/2]$个 qubit 可以传送 n 个 bit 信息。

给出满足定理条件的 n_{AB} 和 n_{BA}，从 A 到 B 传送少于 n_{AB} 个 qubit 的信息，从 B 到 A 传送少于 n_{BA} 个 qubit 的信息。从 A 到 B 传送 n 个 bit 的信息时，使用下面的协议即可：

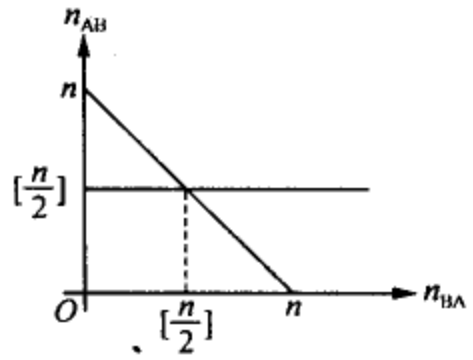


图 3-2 n 个 bit 通信的可能的领域

(1) $n_{AB} \geqslant n$ 的场合：如果把 bit 0 编码成$|0\rangle$，把 bit 1 编码成$|1\rangle$并从 A 向 B 传送$n(n \leqslant n_{AB})$个 qubit 的话，则 B 能够获取从 A 传来的 n 个 bit 的信息。

(2) $[n/2] \leqslant n_{AB} \leqslant n$ 的场合：首先 B 做成$(n-n_{AB})$对的贝尔状态，且把每一个贝尔状态对的一半 qubit 传送给 A，此时从 B 向 A 传送的 qubit 个数为 $n-n_{AB}(\leqslant n_{BA})$。由此可知，A 和 B 共同拥有$(n-n_{AB})$对的贝尔状态，因此在执行$(n-n_{AB})$回量子高密度编码后，若 A 向 B 传送$(n-n_{AB})$个 qubit，就能够传送 $2(n-n_{AB})$个 bit 位信息。在这之后，同(1)的场合一样，使用

$$n_{AB}-(n-n_{AB})=2n_{AB}-n$$

个 qubit，A 将剩余的 $2n_{AB}-n$ 个 bit 送给 B 即可。

例题 3.3 如果 A 向 B 传送 qubit 数 n_{AB}少于 6 bit，B 向 A 传送 qubit 数 n_{BA}少于 3 bit，此时来考虑 A 向 B 传送 9 个 bit 经典信息的方法。因为有 $n=9$，则

$$n_{AB}=6 \geqslant 5=[n/2]$$

以及

$$n_{AB}+n_{BA}=6+3=9=n$$

所以 n、n_{AB}以及 n_{BA}满足式(3.3)和式(3.4)，因此通过传送满足条件个数的 qubit 就能够实现经典 bit 的传送。

事实上，因为不等式$[n/2]=5<6=n_{AB}<n$ 成立，所以 B 拥有进入状态的 3(=9-6)对贝尔状态，并把每一个贝尔状态的一方合计为 3 个 qubit 传送给 A。A 方通过执行 3 次量子高密度编码，向 B 发送 3 个 qubit，就可以向 B 传送 6 位 bit 的信息。在这之后再利用 3 个 qubit 即可把剩余的 3 位 bit 的信息传送给 B。

另一方面，当 A 向 B 传送 9 位 bit 的信息时，送信的 qubit 位数不能少于 $n_{AB}=6$ 以及 $n_{BA}=3$，因为无论哪一方如果少于这个约定的话，就会有如下结果：

$$n_{AB}+n_{BA}<6+3=9$$

因此，式(3.4)不能成立。

3.4　量子瞬间传递(Teleportation 隐形传态)

在上一节的量子高密度编码的描述中，送收信双方共同拥有量子纠缠态，通过量子信道传送附载信息的量子态 qubit，实现了送信者用一个 qubit 能够向收信者传送 2 个 bit 信息的过程。另一个过程所表述的现象是：送收信双方共同拥有量子纠缠态，通过无噪声经典信道确保能够无误地传送 2 个 bit 经典信息，实现正确无误地传送 1 个 qubit 的量子状态的过程，该过程称之为量子瞬间传送(teleportation 隐形传态)。这种场合，即使没有传输量子比特的信道，送信者也能够向收信者传送 qubit，量子瞬间传送的名词由此而来。特别是 1 个 qubit 使用复数 α、β，可以写成 $\alpha|0\rangle+\beta|1\rangle$ 的形式，能够取无穷多个量子态(第一章的布洛赫球能够表示出一个 qubit 可以表示的状态全体)，仅仅传送 2 个 bit 量的信息，就可以把一个 qubit 的信息完整地传送给收信者实在令人惊叹。表 3-1 给出量子隐形传态与量子高密度代码化的对应关系。

表 3-1　量子 teleportation 与量子高密度编码的比较

	量子 teleportation	量子高密度编码
共有状态	贝尔状态	贝尔状态
利用的信道	经典信道	量子信道
发送的信息	1 个 qubit	2 位 bit
使用信道传送的信息	2 位 bit	1 个 qubit

以下讨论实际实现量子隐形传态的方法。

首先，送信者和收信者共同拥有如下的贝尔状态：

$$|\beta_{00}\rangle=\frac{|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B}{\sqrt{2}}$$

此时 $|\cdot\rangle_A$ 表示送信者 A 拥有的 qubit，$|\cdot\rangle_B$ 表示收信者 B 拥有的 qubit。设送信者期望发送的 qubit 信息为 $|\phi\rangle=\alpha|0\rangle_A+\beta|1\rangle_A$，则送信者的初始状态如下：

$$|\xi_0\rangle=|\phi\rangle|\beta_{00}\rangle=(\alpha|0\rangle_A+\beta|1\rangle_A)\left(\frac{|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B}{\sqrt{2}}\right)$$

$$=\frac{1}{\sqrt{2}}\{\alpha(|00\rangle_A|0\rangle_B+|01\rangle_A|1\rangle_B)+\beta(|10\rangle_A|0\rangle_B+|11\rangle_A|1\rangle_B)\}$$

送信者 A 将自己拥有的两个 qubit 经过控制非门(Controlled - NOT - Gate)演算变换后,此时送收信者状态将变换成如下状态:

$$|\xi_1\rangle=\frac{1}{\sqrt{2}}\{\alpha(|00\rangle_A|0\rangle_B+|01\rangle_A|1\rangle_B)+\beta(|11\rangle_A|0\rangle_B+|10\rangle_A|1\rangle_B)\}$$

接着送信者 A 再将自己拥有的两个 qubit 作 H - Gate 演算变换:

$$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

则

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

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

注意,H - Gate 演算、送收信者状态将变换成为

$$\begin{aligned}|\xi_2\rangle=&\frac{1}{\sqrt{2}}\{\alpha(H|0\rangle_A)(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B)+\beta(H|1\rangle_A)(|1\rangle_A|0\rangle_B+\\&|0\rangle_A|1\rangle_B)\}\\=&\frac{1}{2}\{\alpha(|0\rangle_A+|1\rangle_A)(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B)+\\&\beta(|0\rangle_A-|1\rangle_A)(|1\rangle_A|0\rangle_B+|0\rangle_A|1\rangle_B)\}\end{aligned}$$

此时送信者 A 拥有的两个 qubit 可以归纳整理成如下:

$$\begin{aligned}|\xi_2\rangle=&\frac{1}{2}\{|00\rangle_A(\alpha|0\rangle_B+\beta|1\rangle_B)+|01\rangle_A(\alpha|1\rangle_B+\beta|0\rangle_B)+\\&|10\rangle_A(\alpha|0\rangle_B-\beta|1\rangle_B)+|11\rangle_A(\alpha|1\rangle_B-\beta|0\rangle_B)\}\end{aligned}$$

对于这样的纠缠状态,若送信者 A 的两个 qubit 是$|00\rangle$,就意味着收信者 B 的 qubit 通常是$\alpha|0\rangle+\beta|1\rangle$。因此,如果送信者 A 测定自己拥有的两个 qubit,并能判定是$|00\rangle$,则收信者 B 的状态即可肯定是$\alpha|0\rangle+\beta|1\rangle$。

由此可知若送信者 A 测定自己拥有的两个 qubit,并能判定是 4 种状态$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$中的任何一个话,则对应于送信者 A 的测定结果,收信者 B拥有的 qubit 可以用下式来确定。

送信者的状态		收信者的 qubit
$\|00\rangle$	→	$\alpha\|0\rangle+\beta\|1\rangle$
$\|01\rangle$	→	$\alpha\|1\rangle+\beta\|0\rangle$
$\|10\rangle$	→	$\alpha\|0\rangle-\beta\|1\rangle$
$\|11\rangle$	→	$\alpha\|1\rangle-\beta\|0\rangle$

送信者 A 把根据测定所得结果，用下列两个 bit 表示并通过经典信道传送给收信者 B：

送信者的测定结果		送信 bit 列
$\|00\rangle$	→	00
$\|01\rangle$	→	01
$\|10\rangle$	→	10
$\|11\rangle$	→	11

到此为止的演算与测定流程可用图 3－3 表示：

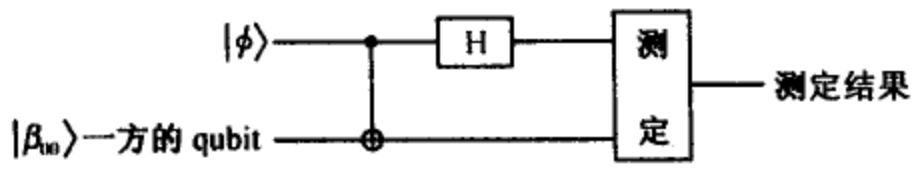


图 3－3　量子 Teleportation 回路(送信侧)

在收信者 B 一侧，根据送信者 A 传送过来的 2 bit 列，对自身拥有的 qubit 做如下的操作：

送信 bit 列		对 qubit 的操作
00	→	不作任何操作
01	→	执行 X－Gate 演算
10	→	执行 Z－Gate 演算
11	→	执行 ZX(X－Gate Z－Gate)演算

如图 3－4 所示，则收信者 B 就能够复原送信者 A 传送的 qubit：$\alpha|0\rangle+\beta|1\rangle$。量子 Teleportation 收信侧的演算与测定流程就可用图 3－4 表示。

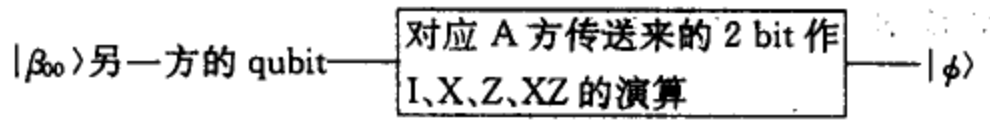


图 3-4 量子 Teleportation 回路(收信侧)

例题 3.4 设送信者 A 希望通过 Teleportation 隐形传态的方式将状态$|0\rangle$传送给收信者 B。此时送收信者的初期状态$|\xi_0\rangle$由式 3-5 设定为 $\alpha=1$，$\beta=0$，则

$$|\xi_0\rangle=\left(\frac{|00\rangle_A|0\rangle_B+|01\rangle_A|1\rangle_B}{\sqrt{2}}\right)$$

送信者 A 拥有的 2 个 qubit 经过 Controlled-NOT-Gate 演算变换，其状态变成$|\xi_1\rangle$

$$|\xi_1\rangle=\left(\frac{|00\rangle_A|0\rangle_B+|01\rangle_A|1\rangle_B}{\sqrt{2}}\right)$$

(其实没有发生变化)。然后对送信者 A 拥有状态的第一位 qubit 作 H-Gate 变换，可以获得变换后的送收信者的状态

$$|\xi_2\rangle=(H|0\rangle_A)\left(\frac{|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B}{\sqrt{2}}\right)$$

$$=\frac{1}{2}(|00\rangle_A|0\rangle_B+|01\rangle_A|1\rangle_B+|10\rangle_A|0\rangle_B+|11\rangle_A|1\rangle_B)$$

此时送信者 A 将自己拥有的 2 个 qubit 作为 2 qubit 态矢空间的基底$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$进行测量，则有

测得$|00\rangle$的概率是：$(\frac{1}{2})^2=\frac{1}{4}$

测得$|01\rangle$的概率是：$(\frac{1}{2})^2=\frac{1}{4}$

测得$|10\rangle$的概率是：$(\frac{1}{2})^2=\frac{1}{4}$

测得$|11\rangle$的概率是：$(\frac{1}{2})^2=\frac{1}{4}$

假设此时测定的结果是$|01\rangle$，则收信者 B 拥有的 qubit 状态必定是$|1\rangle$。送信者 A 将与测定结果对应的 2 个 bit 01 传送给收信者 B，收信者 B 根据送信 bit 列 01 对应执行 X-Gate 演算，对自己拥有的 qubit$|1\rangle$执行反转演算，可获得状态

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

它与送信者 A 传送的状态是一致的。有关量子隐形传态(Feleportation)值得注意的一点是:在执行测定的同时,送信者将破坏自己希望传送的 qubit。也就是说:在执行测定的瞬间送信者将失去自己的 qubit,这个 qubit 附载的信息被传送给了受信者。如此说来,是否可以说借助量子 teleportation 隐形传态技术可以超越光速传递信息,回答是"不可以"。因为收信者在测定发生的瞬间无法得知送信者传送的 qubit,只有当受信者获得送信者通过经典信道传送过来的 2 bit 信息,并对送信者的 qubit 执行复原变换后才可获知送信者的信息。从这一点上来说,利用量子隐形传态(Teleportation)技术传递信息,并非可以超越光速,这与物理法则并不矛盾。

3.5　量子纠缠(Entangled)状态的交换

在实现量子高密度编码或量子隐形传态(Teleportation)过程中,送收信者双方共同拥有纠缠(Entangled)状态是必要的。如同两国领导人之间的热线电话一样,在与特定对象通信之前,共同拥有热线是完全可能的。但若要像普通电话一样,在随时与不特定的对象通信之前,双方共同拥有纠缠状态却是十分困难的。为了解决这个问题,在纠缠态备制中心和用户之间共同拥有纠缠状态的基础上,实现任意用户间共同拥有纠缠状态的过程称为纠缠状态的交换。本节就有关纠缠状态交换做一些介绍(参阅第一章的 1.4 节贝尔态基与量子隐形传态的有关内容)。

设送信者 A 在具备量子隐形传态的基础上希望把某一状态表示的信息传送给收信者 B,但 A 与 B 之间并没有直接共同拥有贝尔状态$|\beta_{00}\rangle$。不过此时在 A 与备制中心 C 之间,及 B 与备制中心 C 之间已分别共同拥有贝尔状态$|\beta_{00}\rangle$,这种情况下使得 A 与 B 之间间接地共同拥有贝尔状态$|\beta_{00}\rangle$的拓扑结构,称之为纠缠状态交换。实际协议是备制中心 C 把与送信者 A 共同拥有的 qubit,利用量子隐形传态方式传送给收信者 B。下面通过实际跟踪信息传递过程确认纠缠状态的交换原理。

首先假设送信者 A 与收信者 B 与备制中心 C 之间有如下的初期状态:

$$|\xi_0\rangle=\frac{|0\rangle_A|0\rangle_C+|1\rangle_A|1\rangle_C}{\sqrt{2}}*\frac{|0\rangle_B|0\rangle_C+|1\rangle_B|1\rangle_C}{\sqrt{2}}$$

$$=\frac{1}{2}\{|0\rangle_A|0\rangle_B|00\rangle_C+|0\rangle_A|1\rangle_B|01\rangle_C+|1\rangle_A|0\rangle_B|10\rangle_C+$$

$$|1\rangle_A|1\rangle_B|11\rangle_C\}$$

其中$|\cdot\rangle_A$、$|\cdot\rangle_B$与$|\cdot\rangle_C$分别表示A、B、C各自拥有的qubit。这里备制中心C把与A共同拥有的qubit对的另一半通过量子隐形传态方式传送给B。量子隐形传态传送信息的过程如图3.4所示，备制中心C先将自己拥有的2 qubit输入控制非门(Controlled - NOT - Gate)，再对自己拥有的qubit列的第一位做H - Gate演算变换，其结果如下：

$$|\xi_2\rangle=\frac{1}{2}\left(\frac{|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B}{\sqrt{2}}\right)|00\rangle_C+\frac{1}{2}\left(\frac{|0\rangle_A|1\rangle_B+|1\rangle_A|0\rangle_B}{\sqrt{2}}\right)|01\rangle_C+$$
$$\frac{1}{2}\left(\frac{|0\rangle_A|0\rangle_B-|1\rangle_A|1\rangle_B}{\sqrt{2}}\right)|10\rangle_C+\frac{1}{2}\left(\frac{|0\rangle_A|1\rangle_B-|1\rangle_A|0\rangle_B}{\sqrt{2}}\right)|11\rangle_C$$

由此备制中心C以自己拥有的2 qubit的4种状态

$$\{|\beta_{00}\rangle,\ |\beta_{01}\rangle,\ |\beta_{10}\rangle,\ |\beta_{11}\rangle\}$$

作为贝尔状态的基底进行测定。根据C的测定结果，A与B的状态以如下的方式确定：

C的测定结果	A与B的状态
$\|\beta_{00}\rangle$	$\|\beta_{00}\rangle$
$\|\beta_{01}\rangle$	$\|\beta_{01}\rangle$
$\|\beta_{10}\rangle$	$\|\beta_{10}\rangle$
$\|\beta_{11}\rangle$	$\|\beta_{11}\rangle$

然后备制中心C将测定的结果用2bit表示，再通过经典信道传送给B。B将根据获得的C的测定结果，通过对自己拥有的qubit作如下的对应操作：

C的测定结果	B的操作
$\|\beta_{00}\rangle$	不作任何操作
$\|\beta_{01}\rangle$	执行X - Gate演算
$\|\beta_{10}\rangle$	执行Z - Gate演算
$\|\beta_{11}\rangle$	执行ZX(X - Gate Z - Gate)演算

此时A与B拥有的状态就都是$|\beta_{00}\rangle$。

然后，送信者A利用共同拥有的贝尔状态$|\beta_{00}\rangle$，借助量子隐形传态物理现象即可向收信者B传送信息。

利用纠缠(Entangled)状态交换原理能够构成关于qubit的交换机。如图

3－5所示，备制中心 E 与 4 个用户 A、B、C、D 共同拥有贝尔状态$|\beta_{00}\rangle$，如果用户 A 希望通过量子隐形传态方式向用户 C 传送 qubit，备制中心 E 将利用自己拥有的 qubit1 和 qubit3，通过量子隐形传态方式向用户 C 传送信息。通过这个操作，用户 A 与用户 C 就能够共同拥有纠缠(Entangled)状态$|\beta_{00}\rangle$。

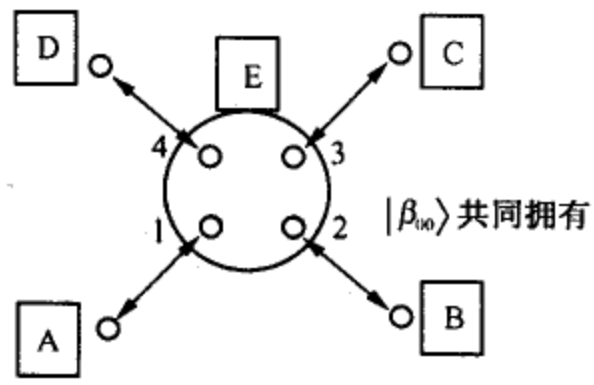


图 3－5　量子交换机

利用纠缠(Entangled)状态的交换，每一个用户仅仅需要与备制中心事先共同拥有各自的纠缠(Entangled)状态，那么任意用户两两之间就能够拥有必要的相互对应的纠缠(Entangled)状态。

第 4 章 量子纠错编码的原理

在第 3 章中讲述了量子密钥分配、量子高密度编码、量子隐形传态等概念及其相关内容，它们或是需要传送 qubit 信息，或是需要共同拥有纠缠状态，因此实现这些功能就需要有能够无失真传送 qubit 信息的量子信道。但现实中在量子信道上和量子存储设备中，由于各种噪声和量子自身的相干性，极易引发量子信息出错。为了克服由此而引发的信息出错，如同经典信息学一样，量子信息学也引入了信息的信道编码体系，即通过构造信息状态的自身重复、增加冗余方法达到系统能够自动纠正出错信息的目的，确保信息无误。

4.1 经典纠错编码

首先从经典纠错编码的重复码说起。考虑通过一个有噪声的信道向受信者传送 1 bit 的信息。作为最简单的信道模型，我们考虑二元对称信道：即当送出的信息是 1、接受的信息是 0 的概率以及送出的信息是 0、接受的信息是 1 的概率都假设为 $p(0<p<\frac{1}{2})$。那么，我们不需要动任何脑筋传送 1 bit 的信息，受信者接收到的信息与送信者发送的信息完全相同的概率是 $\bar{p}=1-p$，受信者接收到的信息与送信者发送的信息不相同的概率是 p，p 就是误码率。

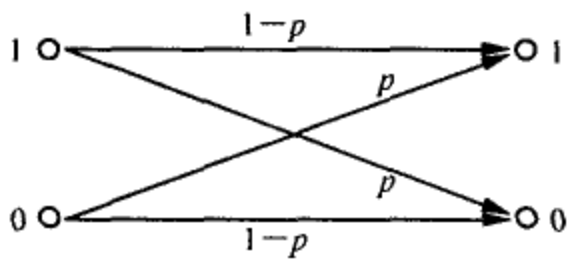


图 4-1 二元对称信道

其次，为了提高传送信息的可信度，作为信息的信道编码，其方法是：在传送 1 bit 信息之际采用将送出的 1 bit 的信息 0 或 1 重复 3 次再发送出去。也就是说按下列方法发送信息：

发送信息　　送往信道的 bit 列(信道编码)

0　→　000

1　→　111

受信者阅读接收到的由信道送出的 3 bit 的受信信息后,必须判断接收的信息是 0 还是 1。这时作为判断的方法只要数一数受信信息的 3 bit 中 0 和 1 出现的次数,并采用多数决定法解码,即次数多的一方决定发送的信息。例如,收到的信息是 001 时,0 出现 2 次、而 1 只出现 1 次,作为多数决定法判定发送的信息是 0。如果使用多数决定法对下列信息作判定,就能恢复送出的 1 bit 信息。

接收到的信息　解码结果(发送信息 bit 的推定值)

$$\left.\begin{matrix}000\\001\\010\\100\end{matrix}\right\} \longrightarrow 0 \qquad (4.1)$$

$$\left.\begin{matrix}011\\101\\110\\111\end{matrix}\right\} \longrightarrow 1$$

若使用这样的编码方式,下面来计算一下传送 1 bit 信息在解码时判定失误的概率。假定送信的 3 bit 里有 2 个以上的 bit 在信道中发生错误,那么由多数决定法解码必定失败。因此由编码・解码出现的错误概率与由信道发生的错误概率是相等的,即 $3p^2(1-p)+p^3$。

例如,设 $p=0.01$,则

$$3p^2(1-p)+p^3 = 0.000298$$

此时与不作信道编码的误码率为 0.01 的情况相比,很显然重复码的误码率得到了大幅度的改善。

4.2　有关 bit 反转信道的量子纠错编码

本节讲述量子纠错编码的有关内容。

最简单的量子信道是 bit 反转信道(如图 4-2 所示),该信道中输入的 qubit 信号为

$$|\varphi\rangle = \alpha|0\rangle+\beta|1\rangle$$

该信道以 $1-p$ 的概率原样输出，以 p 的概率对输入的 qubit 信息作 X-Gate 演算（反转演算）

$$X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

得到 $X|\varphi\rangle$ 并输出其结果。

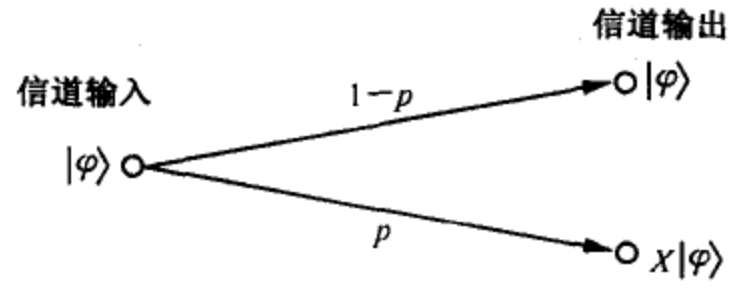


图 4-2 bit 反转信道

与经典的纠错编码一样，作为最单纯的编码，考虑将 1 qubit 用 3 qubit 列编码，也就是说用以下的方式编码：

qubit		编码
$\|0\rangle$	$\longrightarrow$	$\|0\rangle\|0\rangle\|0\rangle=\|000\rangle$
$\|1\rangle$	$\longrightarrow$	$\|1\rangle\|1\rangle\|1\rangle=\|111\rangle$

而且设编码保持线性，即 $|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$ 编码后的形式为

$$|\varphi\rangle=\alpha|000\rangle+\beta|111\rangle$$

实际的编码器如图 4-3 所示。以下根据上面所述的编码方式，演示能够订正输入的 qubit 列中至多 1 qubit 发生 bit 反转错误的情况。

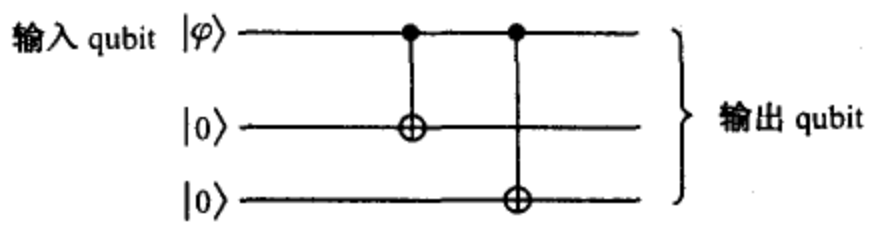


图 4-3 编码器（编码回路）

现在来说明如何订正 qubit 中发生的 bit 反转错误。首先，受信者接收到的 qubit 列是以量子状态叠加的方式来表述的：$|x_1x_2x_3\rangle$，其中 x_1 表示 0 抑或 1。这里测出 x_1、x_2、x_3 中 1 出现的个数，并判定在 $|x_1x_2x_3\rangle$ 中 1 的个数在一个以下的状态时解码成 $|000\rangle$，1 的个数在 2 个以上的状态时解码成 $|111\rangle$。也就是说解码以 D 的方式决定：

接收到的信息		解码结果
$\left.\begin{matrix}\|000\rangle\\ \|001\rangle\\ \|010\rangle\\ \|100\rangle\end{matrix}\right\}$	$\xrightarrow{D}$	$\|000\rangle$
$\left.\begin{matrix}\|110\rangle\\ \|101\rangle\\ \|110\rangle\\ \|111\rangle\end{matrix}\right\}$	$\xrightarrow{D}$	$\|111\rangle$

即

$$\begin{aligned}&D\{|000\rangle, |001\rangle, |010\rangle, |100\rangle\}\\&=|000\rangle, D\{|110\rangle, |101\rangle, |110\rangle, |111\rangle\}\\&=|111\rangle\end{aligned}\tag{4.2}$$

注意到用这样的方式解码与经典纠错编码的方式(4.1)完全对应。再假设解码操作是线性的，也就是说假设$|\varphi\rangle$解码成 $D|\varphi\rangle$，$|\varphi'\rangle$解码成 $D|\varphi'\rangle$，那么叠加状态 $\alpha|\varphi\rangle+\beta|\varphi'\rangle$的解码就转变成由 $D|\varphi\rangle$和 $D|\varphi'\rangle$决定的叠加状态表示成以下等式：

$$D(\alpha|\varphi\rangle+\beta|\varphi'\rangle)=\alpha D|\varphi\rangle+\beta D|\varphi'\rangle$$

例题 4.1　设将 qubit$|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$利用图 4.3 所示编码器完成重复编码，其量子比特列为 $\alpha|000\rangle+\beta|111\rangle$，并通过信道转送。在信道中假设第 2 个 qubit 发生 bit 反转错误，即受信者收到的量子比特列为 $\alpha|010\rangle+\beta|101\rangle$。这种场合注意到，有

$$D|010\rangle=|000\rangle, D|101\rangle=|111\rangle$$

那么，通过 D 变换

$$D(\alpha|010\rangle+\beta|101\rangle)=\alpha(D|010\rangle)+\beta(D|101\rangle)$$

$$=\alpha|000\rangle+\beta|111\rangle$$

就可以获得经过纠正的正确的信道信息。

实际的解码器 D 以图 4－4 方式实现。

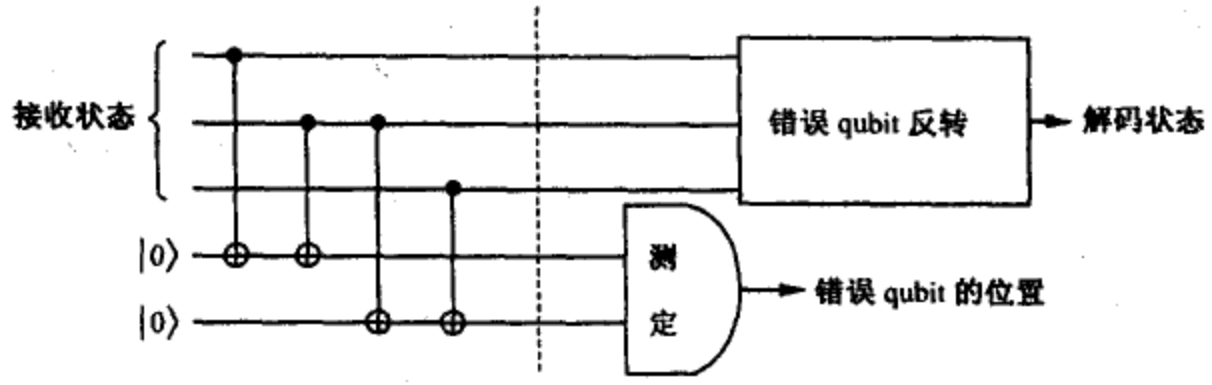


图 4－4　解码器(解码回路)

首先假设量子信道不失真，接收到的信息与发送的信息 $\alpha|000\rangle+\beta|111\rangle$ 完全相等，包含 2 位 qubit 辅助信息，其状态如下：

$$(\alpha|000\rangle+\beta|111\rangle)|00\rangle=\alpha|00000\rangle+\beta|11100\rangle$$

经过 4 个控制非门(Controlled-NOT-Gate)演算，其状态将顺序发生如下变化：

通过第 1 个控制非门后	$\alpha\|00000\rangle+\beta\|11110\rangle$
通过第 2 个控制非门后	$\alpha\|00000\rangle+\beta\|11100\rangle$
通过第 3 个控制非门后	$\alpha\|00000\rangle+\beta\|11101\rangle$
通过第 4 个控制非门后	$\alpha\|00000\rangle+\beta\|11100\rangle$

最后的状态对应于图 4.4 的点线状态，若以状态的最后 2 位 qubit{$|00\rangle$、$|01\rangle$、$|10\rangle$、$|11\rangle$}为基底进行测量，按照 2.3 节有关 qubit 对部分测定的结论，以概率 $|\alpha|^2+|\beta|^2=1$ 获得$|00\rangle$。

另一方面，如果接收到的信道信息变成 $\alpha|100\rangle+\beta|011\rangle$，再包含 2 位 qubit 辅助信息的状态，通过如图 4-4 所示的控制非门 Controlled-NOT-Gate 演算后，其状态将成为

$$\alpha|10010\rangle+\beta|01110\rangle=(\alpha|100\rangle+\beta|011\rangle)|10\rangle$$

然后测定最后 2 位 qubit，以概率$|\alpha|^2=|\beta|^2=1$ 获得$|10\rangle$。以同样的方法，接收到的信道信息中无论哪一个 qubit 发生错误，作为测定的结果都能以概率为 1 准确地判断出错误发生的位置。

测定结果	错误的位置
$\|00\rangle$	没有发生错误
$\|10\rangle$	第 1 位 qubit
$\|11\rangle$	第 2 位 qubit
$\|01\rangle$	第 3 位 qubit

这样，我们就知道当错误发生在不同的位置，其测定的结果就完全不一样；反之就能够通过测定出的结果判断出错误发生的位置。因此，对应于不同的测定结果在相应的 qubit 位上实施 bit 反转 X-Gate 演算就能够自动纠正错误。

以上讲述的纠错编码方法仅能够纠正 1 个 bit 发生反转的错误。那么，考虑至多 1 个 qubit 位上发生 bit 反转的出错概率应该是

$$(1-p)^3+3p(1-p)^2=1-3p^2+2p^3$$

则使用这种纠错编码，订正错误失败的概率 p_e 就为

$$p_e = 1-(1-3p^2+2p^3) = 3p^2-2p^3$$

这些结果与经典纠错编码场合是相同的。但是，在量子纠错编码的问题上，仅用解码错误率 p_e 作为性能评价是不充分的，其原因就在于量子状态的叠加性。因为特定的叠加状态

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

的编码应该为

$$\frac{1}{\sqrt{2}}(|000\rangle+111\rangle)$$

将其转送的时候，即使发生 2 个以上的 bit 反转错误(例如错误发生后的状态为 $\frac{1}{\sqrt{2}}(|101\rangle+|010\rangle)$，经过 D 变换再对

$$\frac{1}{\sqrt{2}}(|111\rangle+|000\rangle)$$

解码，其结果也能正确地恢复成原始的 qubit。另外，作为其他的理由，有关 qubit 的一个重要特性，就是原始 qubit 状态表示的信息与解码得到的 qubit 状态表示的信息，两者之间的相似程度如何，也就是说它们之间的距离如何。上例告诉我们，能够订正错误的种类也不是评价错误订正能力的惟一尺度。

从 qubit 状态表示信息类似程度的角度看纠错能力的性能，其评价尺度称为忠实度。所谓的忠实度 F 定义如下：设送信的 qubit 为 $|\varphi\rangle$、解码的 qubit 为 $|\varphi'\rangle$、F 被定义为

$$F = E|\langle\varphi'|\varphi\rangle|^2 \tag{4.3}$$

这里 E 表示有关信道(与测试过程)的数学期望值。很显然，有

$$0 \leqslant F \leqslant 1$$

如果 $F=1$，则送收信的 qubit 完全相等。

首先来计算没有编码情况下的忠实度。这时假设送信的 qubit 是 $\alpha|0\rangle+\beta|1\rangle$，通过信道以下面的概率输出：

$1-p$ 的概率输出状态为　　$\alpha|0\rangle+\beta|1\rangle$

p 的概率输出状态为　　$X(\alpha|0\rangle+\beta|1\rangle)=\alpha|1\rangle+\beta|0\rangle$

计算此时的忠实度 F：

$$\begin{aligned}F &= (1-p)\,|\,(\alpha\langle 0\,|+\beta\langle 1\,|)(\alpha\,|\,0\rangle+\beta\,|\,1\rangle)\,|^2+\\ &\quad p\,|\,(\alpha\langle 1\,|+\beta\langle 0\,|)(\alpha\,|\,0\rangle+\beta\,|\,1\rangle)\,|^2\\ &= (1-p)(|\,\alpha\,|^2+|\,\beta\,|^2)^2+p(\alpha^*\beta+\beta^*\alpha)^2\\ &= 1-p+p(\alpha^*\beta+\beta^*\alpha)^2 \end{aligned} \tag{4.4}$$

此处的等号使用了归一化条件$|\alpha|^2+|\beta|^2=1$。结果中由于$(\alpha^*\beta+\beta^*\alpha)^2$是非负的实数，因此获得了没有编码情况下忠实度$F$的下限：

$$\min_{|\varphi\rangle} F \geqslant 1-p$$

其次，再来计算有编码情况下的忠实度。设送信的 qubit 依然是

$$|\,\varphi\rangle = \alpha\,|\,0\rangle+\beta\,|\,1\rangle \Rightarrow \alpha\,|\,000\rangle+\beta\,|\,111\rangle$$

作为解码结果，$\alpha|0\rangle+\beta|1\rangle$输出的概率与至多发生 1 个 bit 反转错误的概率是相等的，即为$(1-p)^3+3p(1-p)^2$；由于解码错误的发生，$\alpha|1\rangle+\beta|0\rangle$输出的概率与 2 个以上 bit 反转错误发生的概率相等，即为$3p^2(1-p)+p^3$。除此以外，作为 qubit$|\varphi\rangle$的解码结果再也没有其他的输出。计算其实际忠实度F：

$$\begin{aligned}F &= [(1-p)^3+3p(1-p)^2](\alpha\langle 0\,|+\beta\langle 1\,|)(\alpha\,|\,0\rangle+\beta\,|\,1\rangle)\,|^2+\\ &\quad [3p^2(1-p)+p^3](\alpha\langle 1\,|+\beta\langle 0\,|)(\alpha\,|\,0\rangle+\beta\,|\,1\rangle)\,|^2\\ &= [(1-p)^3+3p(1-p)^2](|\,\alpha\,|^2+|\,\beta\,|^2)^2+[3p^2(1-p)+p^3]\\ &\quad (\alpha^*\beta+\beta^*\alpha)^2\\ &= (1-p)^3+3p(1-p)^2+[p^3+3p^2(1-p)](\alpha^*\beta+\beta^*\alpha)^2\end{aligned}$$

再使用归一化条件$|\alpha|^2+|\beta|^2=1$和$(\alpha^*\beta+\beta^*\alpha)^2\geqslant 0$，即可得到其忠实度$F$的下限：

$$\min_{|\varphi\rangle} F \geqslant (1-p)^3+3p(1-p)^2 = 1-3p^2+2p^3 \tag{4.5}$$

比较式(4.4)和式(4.5)，设$0<p<\frac{1}{2}$，显然下列不等式成立：

$$1-3p^2+2p^3 > 1-p$$

即信道编码增加了忠实度。

4.3 有关位相翻转信道的量子纠错编码

量子比特的 bit 反转信道有对应的经典比特的 2 元对称信道，而量子比特

的位相翻转信道却没有对应的经典比特信道。图 4－5 给出了更接近量子力学理论的位相翻转信道图示。位相翻转信道中，输入的 qubit$|\varphi\rangle$以 $1-p$ 的概率原样输出，以 p 的概率对输入的 qubit$|\varphi\rangle$信号作位相翻转 Z－Gate 演算：

$$Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

得到 qubit$Z|\varphi\rangle$并输出其结果。

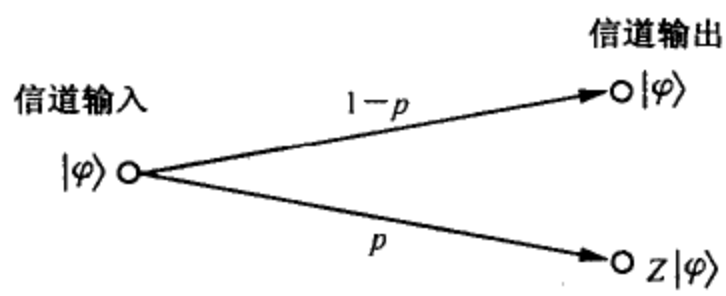


图 4－5　位相翻转信道

对于位相翻转信道来说，前面介绍的编码方法是无纠错能力的。假设对状态$\alpha|0\rangle+\beta|1\rangle$进行编码，得到的三位编码为

$$\alpha\,|\,000\rangle+\beta\,|\,111\rangle$$

经过位相翻转信道传送。如果第一位 qubit 上发生了位相翻转错误，即受信者接收的信息是

$$\alpha\,|\,000\rangle-\beta\,|\,111\rangle$$

那么，经过演算 D 得到的结果是

$$D(\alpha\,|\,000\rangle-\beta\,|\,111\rangle)=\alpha\,|\,000\rangle-\beta\,|\,111\rangle$$

这将意味着推定送信的状态是$\alpha|0\rangle-\beta|1\rangle$，也就是说它无法订正信道中发生的错误。下面就针对位相翻转信道考虑有效的信道编码方法。

对于 Hadamard 变换

$$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

显然，下面的等式成立：

$$H*H=H^2=\frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

再做一个简单的计算，就有

$$HZH = \frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

$$= \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

$$= X$$

其中，X 表示 bit 反转 X－Gate 演算。通过矩阵操作对位相翻转信道的输入系列以及输出系列添加 Hadamard 变换(如图 4－6 所示)，就可把位相翻转错误转变换成 bit 反转错误，于是就可以考虑如下的纠错编码方法。

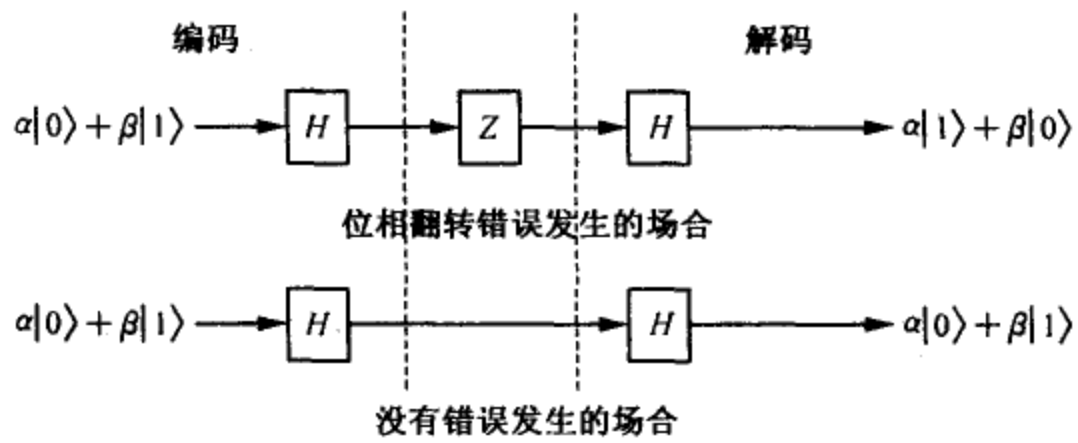


图 4－6 基于 Hadamard 变换将位相翻转错误变换成 bit 反转错误示意图

有关位相翻转的纠错编码

(1) 为了直观描述 qubit$|0\rangle$和$|1\rangle$经过 H 变换后的状态，首先用下列方法定义状态$|+\rangle$和$|-\rangle$：

$$|+\rangle = H\,|\,0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix}$$

$$|-\rangle = H\,|\,1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix}$$

(2) 对 qubit$\alpha|0\rangle+\beta|1\rangle$做下列的变换：

$$\alpha\,|\,000\rangle + \beta\,|\,111\rangle = \alpha\,|\,0\rangle\,|\,0\rangle\,|\,0\rangle + \beta\,|\,1\rangle\,|\,1\rangle\,|\,1\rangle,$$

然后对各位 qubit 实施 Hadamard 变换，就得到以下 3 位 qubit 的叠加状态：

$$\alpha H\,|0\rangle H\,|0\rangle H\,|0\rangle+\beta H\,|1\rangle H\,|1\rangle H\,|1\rangle$$
$$=\alpha\,|+\rangle\,|+\rangle 1+\rangle+\beta\,|-\rangle\,|-\rangle\,|-\rangle$$
$$=\alpha\,|+++\rangle+\beta\,|---\rangle$$

再将其送入位相翻转信道。实际的编码器如图 4-7 所示。

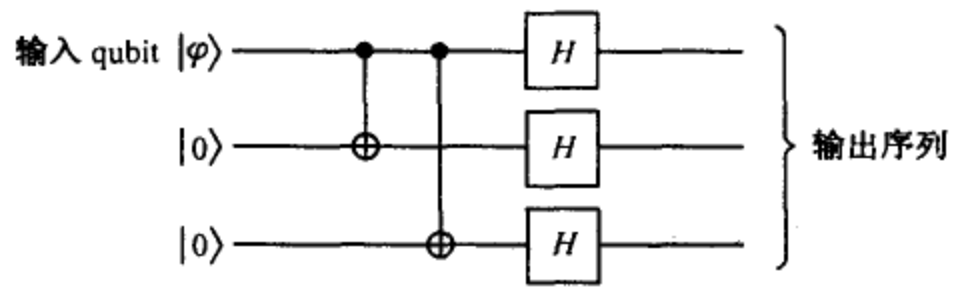


图 4-7　编码器(编码回路)

(3) 再一次对从位相翻转信道输出的 qubit 实施 Hadamard 变换,然后使用与 bit 反转信道纠错方法相同的手法实施解码操作即可纠正错误。实际的解码器如图 4-8 所示。

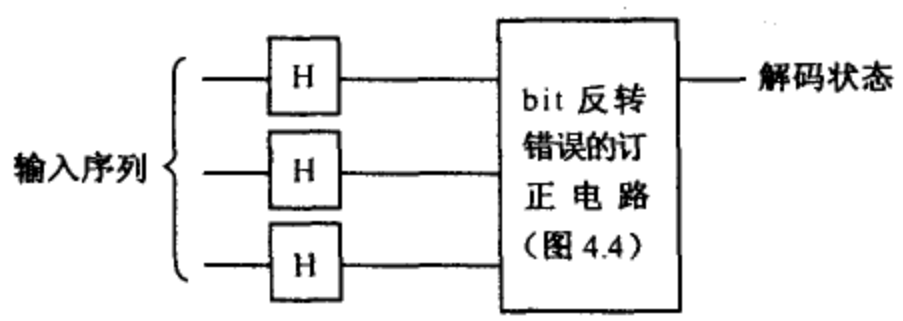


图 4-8　解码器(解码回路)

例题 4.2　将 qubit $\alpha|0\rangle+\beta|1\rangle$编码成 $\alpha|+++\rangle+\beta|---\rangle$,然后将其送入位相翻转信道,假设第 2 个 qubit 上发生位相翻转错误。因为位相翻转发生在第 2 位:

$$Z\,|+\rangle=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}=\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{bmatrix}=|-\rangle$$

$$Z\,|-\rangle=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{bmatrix}=\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}=|+\rangle$$

所以接收到的 qubit 列为 $\alpha|+-+\rangle+\beta|-+-\rangle$,即第 2 个 qubit 上发生了位相

翻转错误。再一次对接收到的 qubit 列各位做 Hadamard 变换演算：

$$H|+\rangle = H(H|0\rangle) = |0\rangle$$

$$H|-\rangle = H(H|1\rangle) = |1\rangle$$

则得到信息的叠加状态 $\alpha|010\rangle+\beta|101\rangle$，使用式(4.2)的解码方法将获得：

$$D(\alpha|010\rangle+\beta|101\rangle)\Rightarrow\alpha|000\rangle+\beta|111\rangle$$

由此得知发送的 qubit 信息是 $\alpha|0\rangle+\beta|1\rangle$。

4.4 一般性的量子纠错编码

在讲解一般性的针对量子无记忆信道纠错编码方法之前，本节中我们将给出关于 bit 反转错误、位相翻转错误以及 bit 和位相同时发生错误的三种情况中的无论哪一种情况发生在某一位 qubit 上的纠错编码的方法。

首先假设 X 为 bit 反转演算、Z 为位相翻转演算，则考虑表示 bit 反转和位相翻转同时发生错误演算的两种情况：

$$XZ = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} = \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$$

$$ZX = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} = \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$$

这里显然有 $XZ=-ZX$，在第一章里明确过 qubit 与其定数倍被认为是同一状态，因此 XZ 和 ZX 被认为是表示同样的错误。在这里选择 XZ 表示 bit 反转和位相翻转同时发生错误的演算。下面就针对任一个 qubit 位实施 X、Z 或 XZ 演算中的任何一种演算讨论实现纠错编码的方法。

这里首先介绍由 Shor 提出的、被称为是 Shor 编码的编码方法。Shor 编码可以被看成是到目前为止我们介绍的 3 位 qubit 的 bit 反转纠错编码与位相翻转纠错编码的组合编码。具体的编码方法是：首先将 qubit 进行 bit 反转纠错编码，得到

$$|0\rangle\Rightarrow|000\rangle$$

$$|1\rangle\Rightarrow|111\rangle$$

再将 qubit 按前一节的位相翻转编码方法进行编码，得到

状态$|0\rangle$编码得到$|+++\rangle$:$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)$

状态$|1\rangle$编码得到$|---\rangle$:$\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$

然后再对每一个 qubit 位进行 bit 反转纠错编码，得到

状态$|+\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}$编码得到$\frac{|000\rangle+|111\rangle}{\sqrt{2}}$

状态$|-\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}}$编码得到$\frac{|000\rangle-|111\rangle}{\sqrt{2}}$

将上面的两种编码组合起来就得到 Shor 编码，即

状态$|0\rangle$编码得到$\frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$

状态$|1\rangle$编码得到$\frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$

实际的 Shor 编码的编码器如图 4-9 所示。

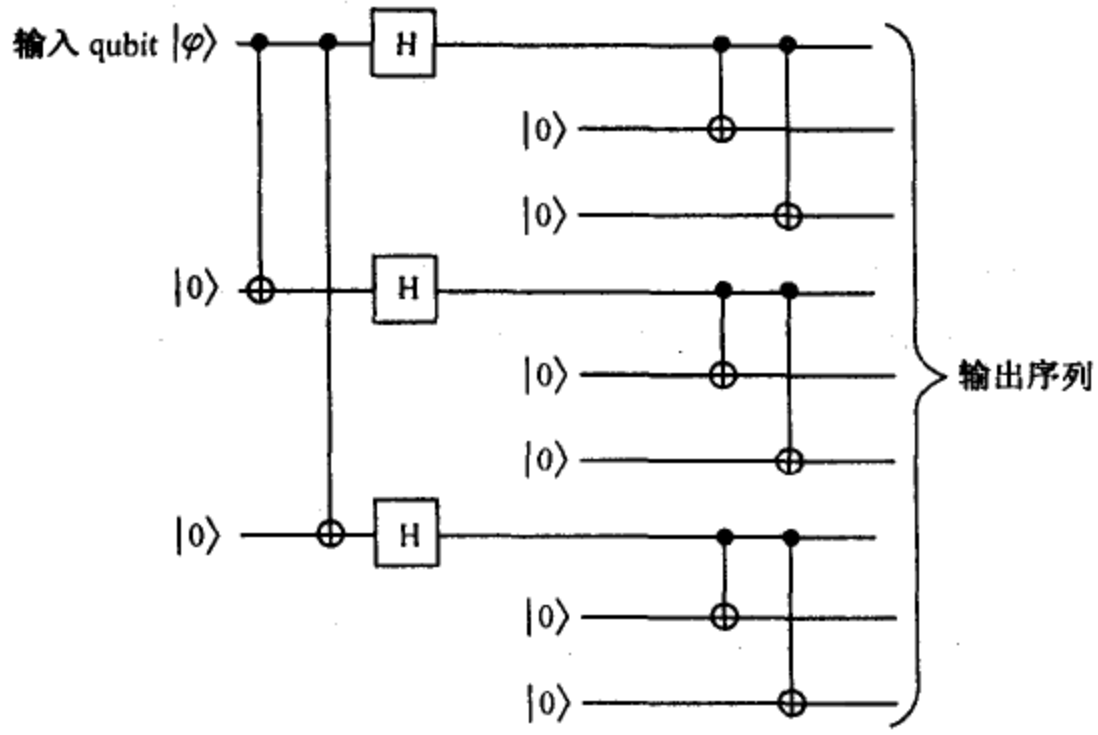


图 4-9　Shor 编码器(编码回路)

接下来讲解有关 Shor 编码中有一个以下 bit 反转错误和一个以下位相翻转错误同时发生时订正的方法。例如，发送信息的状态是$\alpha|0\rangle+\beta|1\rangle$。首先将状态$\alpha|0\rangle+\beta|1\rangle$转换成 Shor 编码

$$|\varphi\rangle = \frac{\alpha(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}} + \frac{\beta(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

再将其送入量子信道。假设结果中第 1 位 qubit 位发生 bit 反转、第 7 位 qubit 位发生位相翻转，则收信状态变成以下结果：

$$|\varphi'\rangle = \frac{\alpha(|100\rangle+|011\rangle)(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}} + \frac{\beta(|100\rangle-|011\rangle)(|000\rangle-|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

首先考虑第 1 位到第 3 位 qubit 的处理，把它们视为三位 qubit 的 bit 纠错编码，采用上一节介绍的 bit 反转纠错编码的解码方法 D，则$|100\rangle$和$|011\rangle$将被解码成$|000\rangle$和$|111\rangle$。同样考虑第 4 位到第 6 位的 qubit 以及第 7 位到第 9 位的 qubit 的处理，也把它们看成三位qubit的 bit 纠错编码，同样利用 bit 反转纠错编码方法进行解码，其结果转变成 $D(|\varphi'\rangle)=|\varphi''\rangle$

$$|\varphi''\rangle = \frac{\alpha(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}} + \frac{\beta(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

显然结果中已纠正了第 1 位 qubit 位发生 bit 反转。其次为了纠正位相翻转错误，从上面的状态中取出第 1 位、第 4 位和第 7 位三位 qubit 状态，则考虑以下状态：

$$\frac{\alpha(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)}{2\sqrt{2}} + \frac{\beta(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)}{2\sqrt{2}}$$

对此用状态$|+\rangle$和$|-\rangle$来表示。上面的状态能够写成

$$\alpha|++-\rangle+\beta|--+\rangle$$

这个结果可以看成是状态$\alpha|0\rangle+\beta|1\rangle$经过位相翻转纠错编码$\alpha|+++\rangle+\beta|---\rangle$后，通过信道时最后一位 qubit 发生位相翻转错误的结果。使用位相翻转纠错编码的解码方法就可以订正这个错误。实际上对各 qubit 位作 Hadamard 变换，就获得状态

$$\alpha|001\rangle+\beta|110\rangle$$

再一次对三位 qubit 使用 bit 反转纠错编码的解码方法，分别将|001⟩解码成|000⟩，将|110⟩解码成|111⟩就可得到最终结果

$$\alpha\,|\,000\rangle+\beta\,|\,111\rangle$$

取出结果状态中的任意一位 qubit 就能恢复发送信息的原始状态 $\alpha|0\rangle+\beta|1\rangle$。图 4－10 给出了 Shor 编码的解码器的构成图。

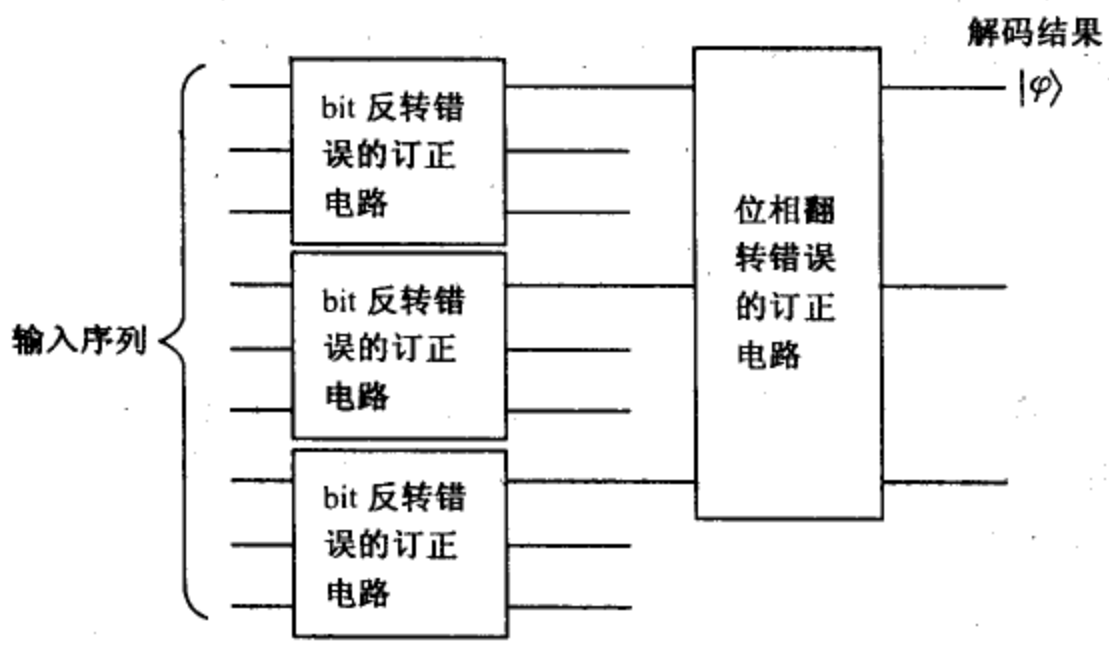


图 4－10　Shor 编码的解码器(解码电路)

下面再仔细地研究一下 Shor 编码，就会发现 Shor 编码在某些情况下能够订正或不能订正：2 个以上的 bit 反转同时发生或 2 个以上的位相翻转同时发生的错误。例如 qubit 的第 1 位和第 3 位上同时发生 bit 反转错误，解码必定失败；但若第 1 位和第 4 位上同时发生 bit 反转错误，从解码的方法上很容易知道订正是可能的。对于位相错误而言，若 qubit 的第 1 位和第 4 位上同时发生位相翻转错误，解码必定失败；但若第 1 位和第 3 位上同时发生位相翻转错误，作为最终的解码结果，它与没有发生错误一样，因此订正也是可能的。

例题 4.3　将状态 $\alpha|0\rangle+\beta|1\rangle$作成 Shor 编码

$$|\varphi\rangle=\frac{\alpha(|\,000\rangle+|\,111\rangle)(|\,000\rangle+|\,111\rangle)(|\,000\rangle+|\,111\rangle)}{2\sqrt{2}}+\frac{\beta(|\,000\rangle-|\,111\rangle)(|\,000\rangle-|\,111\rangle)(|\,000\rangle-|\,111\rangle)}{2\sqrt{2}}$$

然后送入量子信道，让我们来考虑以下情况的纠错。假设通过信道后第 1 位 qubit 位上发生 bit 反转错误、第 5 位 qubit 位上同时发生 bit 反转错误和位相翻转错误，此时接收状态为

$$|\varphi'\rangle = \frac{\alpha(|100\rangle+|011\rangle)(|010\rangle-|101\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}} + \frac{\beta(|100\rangle-|011\rangle)(|010\rangle+|101\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

首先，将 qubit 列的第 1 位到第 3 位、第 4 位到第 6 位、第 7 位到第 9 位都分别看成三位 qubit 位的纠错编码。使用 bit 反转纠错编码的解码方法可将 $|100\rangle$ 和 $|010\rangle$ 恢复成 $|000\rangle$，将 $|011\rangle$ 和 $|101\rangle$ 恢复成 $|111\rangle$。那么，有状态 $D(|\varphi'\rangle)=|\varphi''\rangle$

$$|\varphi''\rangle = \frac{\alpha(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}} + \frac{\beta(|000\rangle-|111\rangle)(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

此时 qubit 列第 1 位和第 5 位上同时发生的 bit 反转错误得以纠正。其次，为了纠正位相翻转错误，从上面的状态中取出第 1 位、第 4 位和第 7 位三位 qubit 状态，则考虑以下状态：

$$\frac{\alpha(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)}{2\sqrt{2}} + \frac{\beta(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)}{2\sqrt{2}}$$

$$= \alpha|+-+\rangle + \beta|-+-\rangle$$

为了纠正位相翻转错误，对各 qubit 位作 Hadamard 变换就获得状态

$$\alpha|010\rangle + \beta|101\rangle$$

再一次对三位 qubit 使用 bit 反转纠错编码的解码方法，分别将 $|010\rangle$ 解码成 $|000\rangle$ 和将 $|101\rangle$ 解码成 $|111\rangle$，得到的最终结果为

$$\alpha|000\rangle + \beta|111\rangle$$

取出结果状态中的任意一位 qubit 就能恢复发送信息的原始状态 $\alpha|0\rangle+\beta|1\rangle$。

4.5 更一般性的量子信道的错误纠正

到上一节为止我们列举了发生在量子信道中的代表性错误—bit 反转、位相翻转以及 bit 反转与位相翻转同时发生的情况。当然，量子信道中可能发生的错误并非仅限于这些，直观上可能的错误现象还有很多。但是，能够订正以上三种错误的量子纠错编码如果存在，以此为基础就有可能订正量子信道中发生的任何错误。本节中以 Shor 编码为例，讲解利用 Shor 编码就能够订正量子信道

中至多 1 个 qubit 位发生的任意错误。

对于 qubit 来说，一般性的量子错误必定能够用一个酉矩阵表示。这就如同在第二章里讲述的一样：能够对 qubit 实施的任何演算（操作）都可以用酉矩阵来表示。这里假设用酉矩阵 E 表示错误（此处 E 必定是单位矩阵），用矩阵 X 表示 bit 反转错误，用矩阵 Z 表示位相翻转错误，用矩阵 XZ 的线性组合表示 bit 反转与位相翻转同时发生的错误，则一定存在复数 e_0, e_1, e_2, e_3，E 可以表示成以下的线性组合：

$$E = e_0 I + e_1 X + e_2 Z + e_3 XZ \tag{4.6}$$

事实上假设

$$E = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

则有

$$E = e_0 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + e_1 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + e_2 \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} + e_3 \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} e_0 + e_2 & e_1 - e_3 \\ e_1 + e_3 & e_0 - e_2 \end{bmatrix}$$

可求得待定系数为

$$e_0 = \frac{a+d}{2}, e_1 = \frac{c+b}{2}, e_2 = \frac{a-d}{2}, e_3 = \frac{c-b}{2}$$

以下将状态 $\alpha|0\rangle + \beta|1\rangle$ 作成 Shor 编码，并假设由式(4.6)决定的错误发生在 qubit 的第 1 位上，我们将展示利用解码的方法能够订正这个错误。

显然，送入信道的编码状态是

$$\frac{\alpha(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

$$+ \frac{\beta(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$

对接收到的编码状态，用演算 E 作用 qubit 列的第一位。则有

$$e_0 \left\{ \frac{\alpha(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \right.$$

$$+\frac{\beta(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\Big\}$$

$$+e_1\Big\{\frac{\alpha(|000\rangle+|011\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle}{2\sqrt{2}}$$

$$+\frac{\beta(|100\rangle-|011\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\Big\}$$

$$+e_2\Big\{\frac{\alpha(|000\rangle-|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$+\frac{\beta(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\Big\}$$

$$+e_3\Big\{\frac{\alpha(|100\rangle-|011\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$+\frac{\beta(|100\rangle+|011\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\Big\} \tag{4.7}$$

这里如果订正 bit 反转错误，即将$|100\rangle$恢复成$|000\rangle$，将$|011\rangle$恢复成$|111\rangle$，则状态就变成

$$e_0\Big\{\frac{\alpha(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$+\frac{\beta(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\Big\}$$

$$+e_1\Big\{\frac{\alpha(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$+\frac{\beta(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle}{2\sqrt{2}}\Big\}$$

$$+e_2\Big\{\frac{\alpha(|000\rangle-|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$+\frac{\beta(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle}{2\sqrt{2}}\Big\}$$

$$+e_3\Big\{\frac{\alpha(|000\rangle-|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$+\frac{\beta(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle}{2\sqrt{2}}\Big\} \tag{4.8}$$

接着为了纠正位相翻转错误，在上面的状态中从第 1 位到第 3 位中任取一位、第 4 位到第 6 位中任取 1 位、第 7 位到第 9 位中任取一位(通常取出第 1 位、第 4 位

和第 7 位三位 qubit 状态),得到状态

$$
\begin{aligned}
& e_0\left\{\frac{\alpha(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)}{2\sqrt{2}}\right. \\
& \left.+\frac{\beta(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)}{2\sqrt{2}}\right\} \\
& +e_1\left\{\frac{\alpha(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)}{2\sqrt{2}}\right. \\
& \left.+\frac{\beta(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)}{2\sqrt{2}}\right\} \\
& +e_2\left\{\frac{\alpha(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)}{2\sqrt{2}}\right. \\
& \left.+\frac{\beta(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)}{2\sqrt{2}}\right\} \\
& +e_3\left\{\frac{\alpha(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)}{2\sqrt{2}}\right. \\
& \left.+\frac{\beta(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)}{2\sqrt{2}}\right\} \\
= & (e_0+e_1)(\alpha|+++\rangle+\beta|---\rangle)+(e_2+e_3)(\alpha|-++\rangle+\beta|+--\rangle)
\end{aligned}
$$

为了纠正位相翻转错误,对各 qubit 位作 Hadamard 变换,获得状态

$$(e_0+e_1)(\alpha|000\rangle+\beta|111\rangle)+(e_2+e_3)(\alpha|100\rangle+\beta|011\rangle)$$

再一次订正 bit 反转错误,即将$|100\rangle$恢复成$|000\rangle$、将$|011\rangle$恢复成$|111\rangle$,则结果状态变成

$$
\begin{aligned}
& (e_0+e_1)(\alpha|000\rangle+\beta|111\rangle)+(e_2+e_3)(\alpha|000\rangle+\beta|111\rangle) \\
= & (e_0+e_1+e_2+e_3)(\alpha|000\rangle+\beta|111\rangle)
\end{aligned}
$$

已知 qubit 状态的整数倍表示同一状态,那么取出结果状态 qubit 列中的任意一位就能恢复到发送信息的原始状态$\alpha|0\rangle+\beta|1\rangle$。

从以上的结论中可以知道:利用 Shor 编码能够订正 qubit 列中至多一位发生的任意量子错误。注意到以上讨论以及获得结果的本质依赖于解码操作的线性性质。也就是说,对发生式(4.7)描述的错误 X 和 Z 以及 XZ 的叠加状态解码结果,如同式(4.8)描述的取自对各个错误纠正状态的叠加状态结果。同样的讨论,能够订正 t 个为止的 bit 反转错误、位相翻转错误以及 bit 反转和位相翻转同时发生错误的量子纠错编码,就能够订正量子信道中至多 t 个 qubit 位发生的任

意错误。

4.6 无需测定的解码回路构成法

上一节作为最基本的量子信号解码器，考虑了利用 Controlled-NOT-Gate 演算和测定的方法。但是，在实际操作上根据测定结果要反转错误的 qubit，除了量子回路以外还需要其他的电子回路，仅仅使用量子演算的机理描述是不能构成解码器的。下面将讲述仅仅利用量子回路或量子门电路，不用测量就可以解码的方法。

首先将 Controlled-NOT-Gate 演算更一般化来说明“控制·控制非门”(Controlled · Controlled-NOT-Gate)的有关概念。所谓“控制·控制非门”的意思是用两位控制一位，也就是 3 位输入和 3 位输出的量子演算，其量子逻辑回路如图 4 - 11 所示。

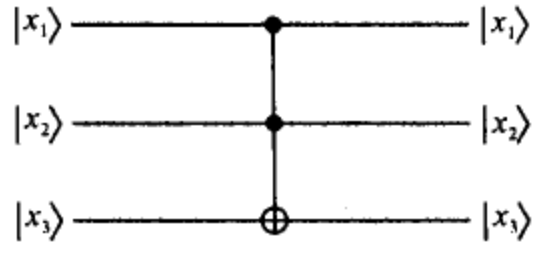


图 4 - 11 控制·控制非门(Controlled · Controlled-NOT-Gate)

“控制 · 控制非门”的量子演算为

$$|x_1x_2x_3\rangle \Rightarrow |x_1x_2((x_1 \text{ AND } x_2) \oplus x_3)\rangle$$

在三位 8 种基底状态{|000⟩,|001⟩,|010⟩,|011⟩,|100⟩,|101⟩,|110⟩,|111⟩}中，根据表达式$(x_1 \text{ AND } x_2)\oplus x_3$，8 种基底状态经过“控制 · 控制非门”后其状态将发生变化：

$$|000\rangle \Rightarrow |000\rangle,\ |001\rangle \Rightarrow |001\rangle$$

$$|010\rangle \Rightarrow |010\rangle,\ |011\rangle \Rightarrow |011\rangle$$

$$|100\rangle \Rightarrow |100\rangle,\ |101\rangle \Rightarrow |101\rangle$$

$$|110\rangle \Rightarrow |111\rangle,\ |111\rangle \Rightarrow |110\rangle$$

结果是在三位 qubit 中限定仅在前两位 qubit 的状态为|11⟩时，将第 3 位 qubit 反转，其输出状态将发生变化：

输入状态		输出状态
$\|110\rangle$	→	$\|111\rangle$

$$|111\rangle \quad \rightarrow \quad |110\rangle$$

而对于其他的基底状态输入状态和输出状态将保留一致。若令输入状态为$|x_1x_2x_3\rangle$，则输出状态为$|x_1x_2x_3'\rangle$的 Controlled・Controlled-NOT-Gate 的数学描述如下：

$$x_3' = \begin{cases} \bar{x}_3 & x_1 = x_2 = 1, \text{的场合} \\ x_3 & \text{上述以外的场合} \end{cases}$$

此处 x_1' 取值 0 或 1，$\bar{x}_3$ 表示 x_3 的否定。特别地，如果$|x_3\rangle = |0\rangle$，则对应于输入状态$|x_1x_20\rangle$的输出状态就成为$|x_1x_2(x_1 \cdot x_2)\rangle$。此处 $x_1 \cdot x_2$ 表示 AND 演算。到此我们知道“控制・控制非门”Controlled・Controlled-NOT-Gate 是对应于逻辑演算 AND 的量子演算。

现在将状态 $\alpha|0\rangle+\beta|1\rangle$用 4.2 节讲述的编码方法编成代码 $\alpha|000\rangle+\beta|111\rangle$，在信道中发生 bit 反转错误，我们讨论构成订正这类错误的解码器。

首先我们不做测定，考虑第 2 位 qubit 上发生错误的订正方法。与图 4.4 描述的那样，受信状态 $\alpha|010\rangle+\beta|101\rangle$后缀两位辅助 qubit，考虑输入状态

$$(\alpha|010\rangle+\beta|101\rangle)|00\rangle = \alpha|01000\rangle+\beta|10100\rangle$$

将这个状态输入到图 4.12 表述的量子回路，图的虚线部分表述了状态的变化，变化过程如下：

α	β
$\|\underline{0}10\rangle\|\underline{0}0\rangle$	$\|\underline{1}01\rangle\|\underline{0}0\rangle$
$\|0\ \underline{1}0\rangle\|\underline{0}0\rangle$	$\|1\ \underline{0}1\rangle\|\underline{1}0\rangle$
$\|0\ \underline{1}0\rangle\|1\ \underline{0}\rangle$	$\|1\ \underline{0}1\rangle\|1\ \underline{0}\rangle$
$\|01\ \underline{0}\rangle\|1\ \underline{1}\rangle$	$\|10\ \underline{1}\rangle\|1\ \underline{0}\rangle$
$\|010\rangle\|11\rangle$	$\|101\rangle\|11\rangle$

结果为：

$$\alpha|01011\rangle+\beta|10111\rangle = (\alpha|010\rangle+\beta|101\rangle)|11\rangle$$

辅助 qubit 的状态变成了$|11\rangle$。如前所述，辅助 qubit 的状态因错误发生的位置不同而不同。

错误发生的位置	辅助 qubit 的状态
没有错误	$\|00\rangle$
第 1 位 qubit 发生错误	$\|10\rangle$
第 2 位 qubit 发生错误	$\|11\rangle$

第 3 位 qubit 发生错误 $|01\rangle$

因此，只要对应于辅助 qubit 的状态{$|00\rangle$，$|10\rangle$，$|11\rangle$，$|01\rangle$}，反转从第 1 位到第 3 位中某个 qubit 即可订正错误。在订正第 2 个 qubit 发生的错误时，使用“控制·控制非门”和辅助 qubit 的状态是$|11\rangle$的结果，反转第 2 位 qubit 即可订正错误。如此可以获得如下的输出状态：

$$\alpha\,|\,00011\rangle+\beta\,|\,11111\rangle=(\alpha\,|\,000\rangle+\beta\,|\,111\rangle)\,|\,11\rangle$$

从这个输出状态的前 3 位 qubit 可以推断原始的发送信息。这种情况下我们知道当第 2 位 qubit 发生 bit 反转是可以订正的。另外，在图 4－12 所示的回路中我们必须注意到，如果是第 2 位 qubit 以外的 qubit 发生错误，或者说完全没有发生错误时，受信的信息将会保持原样输出。

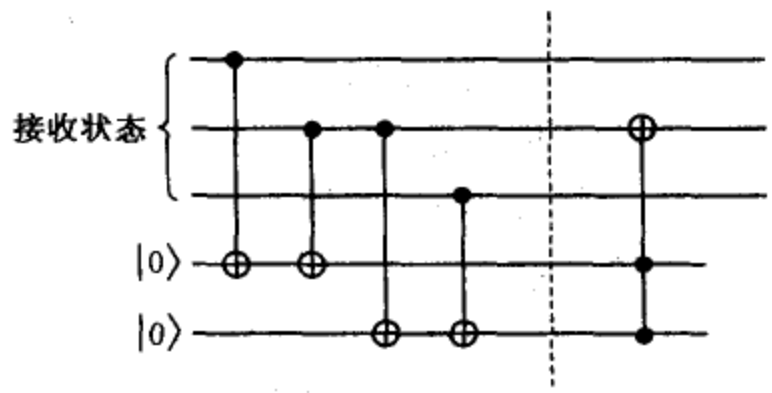


图 4－12 订正第 2 位 qubit 发生错误的回路

下面考虑第一个 qubit 发生错误的情况。此时辅助 qubit 的状态是$|10\rangle$，在这种情况并只有在这种情况下反转第 1 位 qubit 可订正错误。为了实现这个功能，使用控制非门 Controlled-NOT-Gate 的否定回路与“控制·控制非门”Controlled · Controlled-NOT-Gate 一起构成如图 4－13 所示的量子回路即可实现上述功能。事实上如果第一位 qubit 上发生错误，那么从下往上数，第 3 位 qubit 经过控制非门 Controlled-NOT-Gate 时，其状态由$|0\rangle$变成$|1\rangle$，而第 2 位和第 1 位的 qubit 各自保持本来的$|0\rangle$和$|1\rangle$。然后最后由“控制·控制非门”Controlled · Controlled-NOT-Gate 将第 1 位 qubit 反转即可订正错误。第 3 位 qubit 发生错误的订正方法与第 1 位发生错误的订正方法在概念上是一样的，同样可以订正。

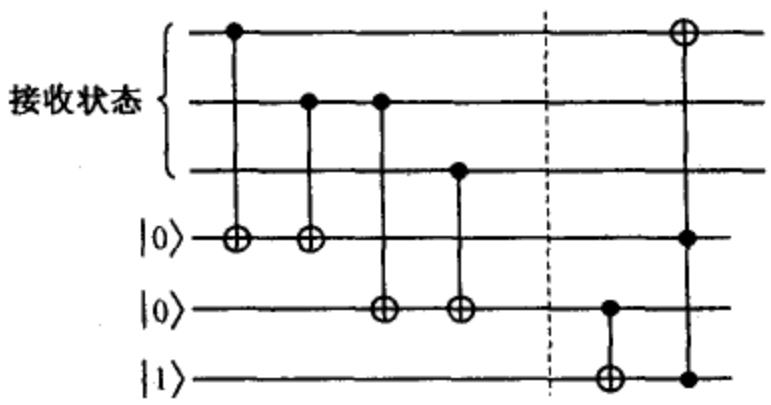


图 4－13 第 1 位 qubit 发生错误的订正回路

从以上的讨论结果，在图 4－13 中给出能够订正任意 qubit 位发生 bit 反转错误的解码器。另外，有关实际的解码，并非要将传送过来的信息编码本身复原，而是只要将传送过来的 1 个 qubit 本身复原即可。为此，例如仅仅利用如图 4－12所示的针对第 2 位 qubit 错误订正的回路，推断输出的第 2 位 qubit 就是原送信信息的 qubit 值即可。

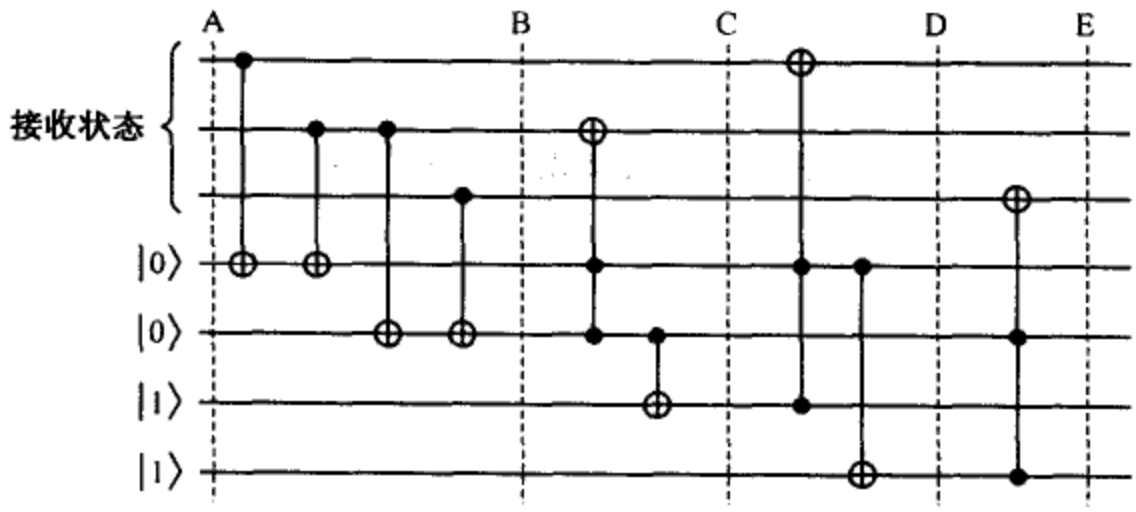


图 4－14　订正 bit 反转的回路

例题 4.4　再一次将 qubit $\alpha|0\rangle+\beta|1\rangle$编码成 $\alpha|000\rangle+\beta|111\rangle$，并将其送入信道。假设此时受信者接收到的信息是 $\alpha|001\rangle+\beta|110\rangle$，即第 3 位 qubit 发生 bit 反转错误。在此将接收到的信息 $\alpha|001\rangle+\beta|110\rangle$送入解码器，看一看它的输出状态究竟是什么。

假设解码器如图 4－14 所示，解码过程可以分段描述如下：其输入状态是到达虚线 A 的瞬间状态

$$(\alpha|001\rangle+\beta|110\rangle)|0011\rangle=\alpha|0010011\rangle+\beta|1100011\rangle$$

经过 A～B 之间的运算，达到虚线 B 的瞬间状态为

$$\alpha|0010111\rangle+\beta|1100111\rangle=(\alpha|001\rangle+\beta|110\rangle)|0111\rangle$$

此时可以看到辅助位的第 2 位发生了变化，指出了信息序列发生错误的位置。经过 B～C 之间的运算，达到虚线 C 的瞬间状态为

$$\alpha|0010101\rangle+\beta|1100101\rangle=(\alpha|001\rangle+\beta|110\rangle)|0101\rangle$$

此时可以看到即使通过虚线 B 的右侧的“控制·控制非门”，信息序列的第 2 位 qubit 也不会发生变化，但控制非门使得辅助位的第 3 位由$|1\rangle$变成了$|0\rangle$。再经过 C～D 之间的运算，达到虚线 D 的瞬间状态与达到虚线 C 的瞬间状态保持一致：

$$\alpha|0010101\rangle+\beta|1100101\rangle=(\alpha|001\rangle+\beta|110\rangle)|0101\rangle$$

没有发生任何变化，即通过虚线 C 右侧的“控制·控制非门”，信息序列的第 1 位 qubit 没有发生变化。最后经过 D～E 之间的运算，达到虚线 E 的瞬间状态是

$$\alpha\,|\,0000101\rangle+\beta\,|\,1110101\rangle=(\alpha\,|\,000\rangle+\beta\,|\,111\rangle)\,|\,0101\rangle$$

即通过虚线 E 的右侧的“控制·控制非门”，信息序列的第 3 位 qubit 被反转。最后从下列状态

$$\alpha\,|\,0000101\rangle+\beta\,|\,1110101\rangle$$

中取出前 3 位 qubit 即可得到原始的发送信息的代码 $\alpha|000\rangle+\beta|111\rangle$。

第 5 章　量子纠错编码的构成法

在第四章节中介绍了量子纠错编码的基本原理，并以经典纠错编码中的重复码为基础，分别介绍了：bit 反转纠错码的编码与解码原理；位相翻转纠错码的编码与解码原理；引入 Shor 编码和表示更一般的量子信道错误的酉矩阵 $E = e_0 I + e_1 X + e_2 Z + e_3 XZ$，讨论了一般性量子纠错码的编码与解码的原理；利用“控制·控制非门”实现无需测定的纠错码的解码回路构成法原理。本章将进一步借鉴并利用经典纠错编码中其他思想与方法，介绍 Calderbank-Shor-Steane 量子纠错编码的体系，并就量子纠错编码的性能界限等有关问题作一些简单说明。

为了使读者能够更好地理解量子纠错编码的构成方法，需要一些抽象代数的基本概念和代数演算中某些特殊知识，需要进一步了解经典纠错编码的基本概念和它的数学描述，并了解量子纠错编码基本概念及其与经典纠错编码的关系。5.1 节“量子纠错编码的发展简述及其相关数学基础”较深入地介绍了有关纠错编码的数学基础，有一定的难度，阅读时可以跳过该节，从 5.2 节开始。

5.1　量子纠错编码的发展简述及其相关数学基础

这里对量子纠错编码的发展做一个综述，介绍量子纠错编码的数学理念以及用经典纠错码构造量子码的 CRSS 方法及其他方法。在讨论量子纠错码之前，首先介绍经典纠错编码的一些基本知识，这不仅由于经典纠错码是构造量子纠错码的重要工具，而且对于理解量子纠错码也是有益的。经典纠错码和量子纠错码的物理机制很不相同，但是很多概念和结果至少在数学表现形式上有相似之处。

在数字通信中为纠正信道中产生的错误，自 20 世纪 50 年代以来发展了系统的纠错码数学理论。目前正在有效使用的这种纠错码，已经被研究量子纠错码的学者们称之为“经典”纠错码。

在量子通信和量子计算中，纠错问题同样是一个重要问题。长期以来，人们一直认为量子纠错比数字通信纠错更为困难，这是由量子通信和量子计算的机

制所造成的(表示信息的量子状态与环境的相互影响以及量子状态的连续性、纠缠性、不可克隆等性质)。但是在1995～1996年,量子纠错的研究取得重要的突破,P. W. Shor和A. M. Steane在物理层上把复杂的纠缠态量子错误归结和简化为只需考虑每个量子位上独立发生的错误,并且错误类型只有3种,即比特反转错误、位相翻转错误和比特反转加位相翻转错误,把它们抽象成3个Pauli矩阵 σ_x、σ_y 和 σ_z。基于这种物理模型的简化,构造出世界上第一个量子纠错码[[9, 1, 3]],随后不久人们把它改进为[[7, 1, 3]]和[[5, 1, 3]],后者是最佳量子码。

1997年以来,A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane等人总结了量子纠错编码理论的数学形式,并且给出一种构造量子码系统的有效的数学方法。这种方法给出了经典纠错编码和量子纠错编码之间的密切联系,从而用经典纠错码的结果构造出一批好的量子码。他们的工作极大地推动了量子纠错编码数学理论的研究,1999年以来,人们不仅利用各种经典纠错码得到一批纠错性能不断改善的量子码,而且开展了关于量子码性能的其他课题的研究。

5.1.1 抽象代数

一、基本代数系统

【代数运算】 假定对于集合 A 中的任意元素 a 与集合 B 中的任意元素 b,按照某一法则可以与某一集合 C 中惟一确定的元素 c 对应,则称这个对应为 A、B 的一个(二元)运算,集合 A、B 也可以是同一个集合,就是对 A 中的任意两个元素 a、b,可以惟一确定元素 c,使 $c = a * b$, c 可以属于 A 或不属于 A,若属于 A,则称 A 在运算"$*$"下是封闭的。

在二元运算"$*$"下,若对于 A 的任意两个元素 a 和 b, $a * b = b * a$ 成立,则称 A 是可交换的。若对于 A 的任意3个元素 a、b、c 在"$*$"下, $a * (b * c) = (a * b) * c$ 成立,则称 A 是可结合的。若运算"$*$"是通常意义下的加法或乘法,就分别记为 $a + b$ 或 $a \cdot b$,整数集合中的加法和乘法都是可交换的和可结合的,因此整数集合是可交换和可结合的。

【代数系统】 如果一个集合 A 具有满足某些法则的代数运算,就称集合 A 为代数系统,群、环、域就是3个基本的代数系统。

二、群

【群的定义】 设 G 不是空集,对 G 给定一个代数运算"$*$",若在运算"$*$"下,满足下列4个条件,则称 G 为一个群。

(1) G 在"$*$"之下是封闭的,即对每一个元素 $a \in G$, $b \in G$,则有惟一确定

的元素 $c = a * b$，且 $c \in G$。

(2) G 在“$*$”之下是可结合的。即对任意元素 a、b、c，$a \in G$，$b \in G$，$c \in G$，有

$$a * (b * c) = (a * b) * c$$

(3) 在 G 中有一个元素 e，对任一 $a \in G$，满足

$$a * e = e * a = a$$

(4) 在 G 中对任一 $a \in G$，都有一个 $a^{-1} \in G$，满足

$$a * a^{-1} = a^{-1} * a = e$$

条件(3)中的 e 称为单位元或恒等元，条件(4)中的 a^{-1} 称为 a 的逆元。

若一个群 G 的乘法“$*$”可交换，则称 G 为交换群或阿贝尔群，特别在加法之下，交换群称为加法群。在加法群中，“$*$”改为“$+$”，逆元 a^{-1} 改为负元 $-a$，单位元称为零元，记作 0。

【群的例子】

(1) 整数集 N 组成一个加法群，有理数集、实数集、复数集各组成一个加法群。

(2) 非零的实数集 R^* 对于乘法组成一个群，正的实数集 $R^{(+)}$ 对于乘法也组成一个群。

(3) 一切元在数域 F 正的 n 阶可逆矩阵对于乘法组成一个群，记作 $GL_n(F)$。

(4) 一切 n 次置换的集合组成一个群，称为置换群，记作 S_n。

事实上，若任取两个 n 次置换：

$$\sigma_1 = \begin{bmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{bmatrix}, \quad \sigma_2 = \begin{bmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{bmatrix}$$

σ_2 可以改写为

$$\sigma_2 = \begin{bmatrix} i_1 & i_2 & \cdots & i_n \\ k_1 & k_2 & \cdots & k_n \end{bmatrix}$$

对于置换 σ_1 和 σ_2，规定置换

$$\sigma_3 = \begin{bmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{bmatrix}$$

和它们对应，即 σ_3 为 σ_1 和 σ_2 的乘积，记作

$$\sigma_3 = \sigma_1\sigma_2$$

在这个乘法之下，不难推出 S_n 满足群中规定的条件，因而 S_n 组成一个群。

【子群】 设群 G 的非空子集 H 对于 G 的运算也组成一个群，则称 H 为 G 的一个子群。

群 G 的非空子集 H 是子群的充分必要条件是：若 $a \in H$，$b \in H$，则 $ab^{-1} \in H$。

任意个子集的交集是一个子群。

【循环群】 一个元 a 的一切乘幂 $a^0 = e$，a，a^2，… 的全体组成一个群，称为循环群，循环群是交换群。

若序列 e，a，a^2，…中没有两个元素相等，则称 G 为无限循环群，若有相等的元素，即

$$a^i = a^j,\ i \neq j$$

可推出 G 为 n 个元 e，a，a^2，…，a^{n-1} 的集，即

$$G = \{e, a, a^2, \cdots, a^{n-1}\}$$

这时称 G 为有限循环群，n 称为 G 的阶，即 n 为使 $a^n = e$ 的最小正整数。

循环群的子群还是循环群。

【不变子群，陪集，商群】 设 H 是群 G 的一个子群，若对每个元 $g \in G$，有

$$gH = Hg$$

（这里 gH 表示 g 与 H 中一切元素的乘积，例如 gh，$h \in H$），即 $gHg^{-1} = H$，则称 H 为 G 的一个不变子群（或正规子群），gH 和 Hg 分别称为 G 对 H 含元素 g 的左陪集和右陪集，因此含同一元素的不变子群的左陪集和右陪集是重合的。

把陪集看作元素时，一切陪集构成一个群，称为 G 对 H 的商群，记作 G/H。

拉格朗日定理：有限群 G 的子群的阶是群 G 的阶的一个因数。

G 的不变子群 H 的商群 G/H 的阶为 G 的阶被 H 的阶除所得的商。

交换群的一切子群都是不变子群。

若群 G 除自身外，无任何其他不变子群，则称 G 为单群。

三、环

【环的定义】 一个非空集 R 有加法和乘法两个二元运算，若满足下列 3 个条件，就称 R 为一个环。

（1）R 是一个加法群。

（2）对于乘法满足结合律。即对任何 a、b、c，$a \in R$，$b \in R$，$c \in R$，有

$$a(bc) = (ab)c$$

(3) 对于加法和乘法满足左、右分配律。即对任何 a、b、c，$a \in R$，$b \in R$，$c \in R$，有

$$a(b+c) = ab + ac,\ (b+c)a = ba + ca$$

一个环若满足乘法的交换律 $ab = ba$，则称 R 为交换环。

【环的例子】

(1) 一切整数全体是一个环，称为整数环。

(2) 设 F 是一个数域，则域 F 上的多项式的全体是一个环，记作 $F[x]$。

(3) 如果数集 R 中任意两个数的和、差、积仍属于 R，则 R 也是一个环，称为数环。单个数零也是一个数环，称为零环。显然，数环总是交换环。

四、域

【域的定义】 一个具有单位元的交换环 R，若至少含有一个非零元，并且每个非零元 a 恒有逆 a^{-1}，则称 R 为一个域。

【环的例子】

(1) 数域 F(有理数域 Q、实数域 R、复数域 C)都是域。

(2) 数域 F 上的一切有理分式 $f(x)/g(x)(f(x)/g(x) \in F[x]$，且 $g(x) \neq 0)$ 在有理分式的加法和乘法之下组成一个域，称为数域 F 上的有理分式域。

5.1.2　经典纠错编码的基本概念

自 1948 年香农文章发表后，很长一段时间内人们在探寻那种能够简单地、有效地编码和译码的好码，由此形成了一套经典纠错编码的理论。

纠错编码的目的是引入剩余度(冗余度)。直观地看，所谓的纠错编码就是在待传输的信源码的码元(称为信息码元，例如 0010)之后增加(后缀)一些多余的码元(称为校验码元，例如 110)，构成该信源码的纠错码(称为信道编码 0010110)，使得该编码在有噪信道传输中即使发生信息损失或错误仍能在接收端加以恢复。

根据信息码元和校验码元之间的不同关系，经典纠错码按结构大致可分类如下(图 5-1)：

- 线性码：信息码元与校验码元之间呈线形关系。
- 非线性码：信息码元与校验码元之间不存在线性关系。
- 分组码：把信息序列以每 k 个码元分组，然后把每组 k 个信息元按一定规律产生 r 个多余的校验元。输出序列每组长 $n = k + r$，则每一码字的 r 个校验元只与本码字的 k 个信息元有关，与别的码字的信息元无关，用二元组(n, k)

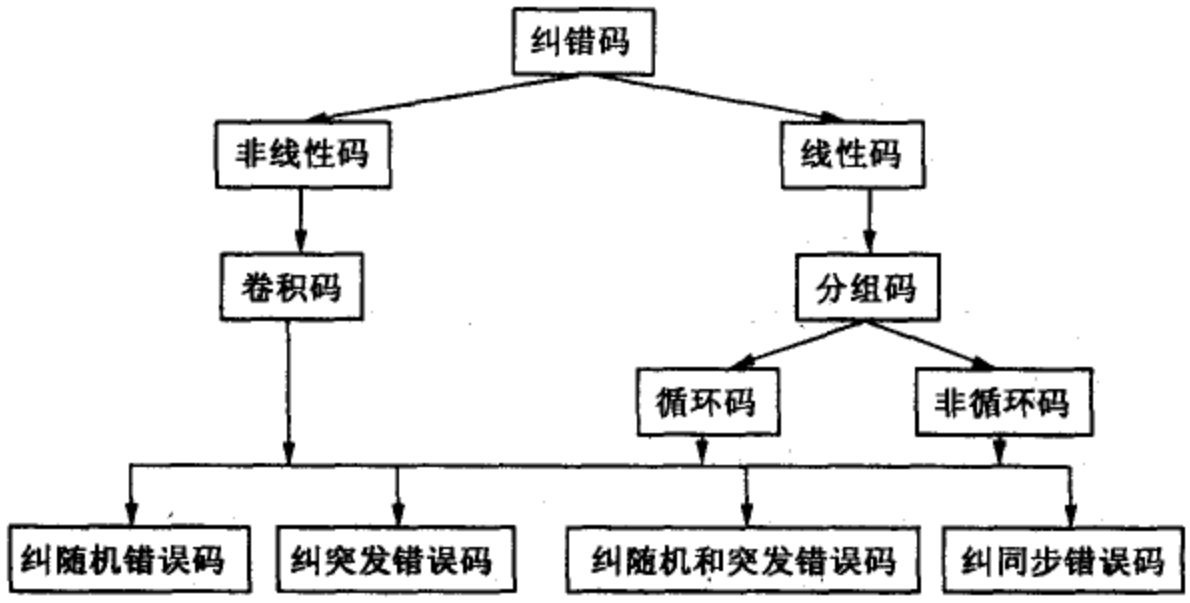


图 5-1 经典纠错码的分类

表示分组码。

• 卷积码:把信息序列以每 k_0 个码元分段,编码器输出该段的校验元 $r = n - k_0$,校验元不但与本段的 k_0 个信息元有关,而且还与其前面 m 段的信息元有关,故用三元组(n, k, m)表示卷积码。

• 循环码:该码(消息编码的全体)的特点是,若将其全部码字分成若干组,则每一组中任一码字的码元循环移位后仍是这组的码字。

• 非循环码:任一码字中码元循环移位不一定再是该码书中的码字。

5.1.3 从数学角度看经典代数纠错码

在数字通信中,信息用有限个离散状态(数字位)表示,每个位(bit)是有限集合 S 中的元素。若 S 有 m 个元素 $(m \geqslant 2)$,可以取 S 为整数模 m 的同余类 $\bar{0}, \bar{1}, \cdots, \overline{m-1}$(注意 $\bar{m} = \bar{0}$) 形成的环,表示成 Z_m。这时 Z_m 中有加减乘运算,从而可使用数论工具。当 $m = p$ 是某个素数 p 的方幂时 $(l \geqslant 1)$,通常取 S 为 $q = p$ 元有限域,表示成 F_q,这时可以对 F_q 中的元素进行四则运算,使用有限域和有限域理论一系列代数性质。

这里只介绍 q 元有限域 F_q 上的经典纠错码。事实上,在通信领域最常使用的是 $q = 2$ 的情形,即最简单的二元域 $F_2 = \{0, 1\}$,其中 $1 + 1 = 0$(从而 $1 = -1$,于是加法和减法一样),其余运算都是自然的。

对每个正整数 k,以 F_q^k 表示有限域 F_q 上的 k 维向量空间,其中元素是长为 k 的向量:$v = (v_1, v_2, \cdots, v_k)$ $(v \in F_q)$。这样的向量共有 q^k 个,用来表示信息。例如,8 个信息$\{0, 1, \cdots, 7\}$可以用 F_2 上长为 3 的 8 个向量来表示:

$$0 = (000),\ 1 = (100),\ 2 = (010),\ 3 = (110)$$

$$4=(001),\ 5=(101),\ 6=(011),\ 7=(111)$$

一般地，q^k 个信息可以用 F_q 上长为 k 的向量来表示。但是用这种方式通信是不能纠错的，这是因为 F_q^k 中每个向量都代表某种信息，都是有意义的。设想发方把信息 $1=(100)$ 通过信道传给收方，如果信道传输时第 2 位 0 错成 1，收到(110)，而(110)代表信息 3(数学上表示成：发方发出信息 $x=(100)$，信道出错错误向量为 $\varepsilon=(010)$，收方收到 $y=x+\varepsilon=(100)+(010)=(110)$)，收方无法判别是否出错。

为使通信系统有纠错能力，办法是：将 q^k 个信息用比 k 长的向量来表示，取 $n>k$，q^k 个信息用 F_q^n 中 q^n 个向量当中的一部分向量(q^k 个)来表示，它们形成 F_q^n 的一个 q^k 元子集 S。S 中向量代表信息，而其余 q^n-q^k 个向量是没有意义的。要将 S 选取得好，使得发方发出信息 $x\in S$，在信道产生少数几位错误 ε 时(即向量 ε 只有少数几位为 1，其余位均为 0)，收到的 $y=x+\varepsilon$ 不属于 S，所以收方检查到出错(因为 y 不代表信息)，并且还能够纠正错误。

例 5.1　(重复码)将上述{0，1，…，7}代表的向量均重复 3 次：

$$0=(000000000),\ 1=(100100100),\ 2=(010010010),\ \cdots,$$
$$6=(011011011),\ 7=(111111111)$$

把 8 个信息用 F_2^9 中上述 8 个向量表示，它们代表信息，这 8 个向量形成集合 S，其余 2^9-8 个向量不代表信息。每个 $x\in S$ 在其中 1 位或 2 位出错时，如 $x=(100100100)$ 变成 $y=(101110100)$，它都不属于 S，因为 S 中任意两个不同向量至少有 3 位是不同的。进而，若 $x=(100100100)$ 只有 1 位出错，成为 $y=(100110100)$，容易看出发出的为 $x=(100100100)$，因为 S 中只有 x 和 y 只相差 1 位，而 S 中其余向量($\neq x$)与 y 均至少有 2 位不同。综合上述可知，S 可以检查 2 位错误，纠正 1 位错误。

有了以上直观的概念，现在给出数学的形式化定义。

定义 5.1　F_q^n 中每个子集 S 都叫作一个纠错码。S 中向量叫作码字，n 叫作 S 的码长，$K=|S|$ 表示码字个数，$k=\log_q K$ 叫作信息位数(如果不考虑纠错性能，K 个信息(码字)用长为 k 的向量即可)。

除了 n 和 K(或 k)之外，S 还有另一个参数 d，用来反映纠错能力。

定义 5.2　对于 $u=(u_1,\cdots,u_n)\in F_q^n$，$v=(v_1,\cdots,v_n)\in F_q^n$，定义向量 u 的汉明权(Hamming weight)为非零分量 u_1 的个数：

$$w_H(u)=\#\{i\mid 1\leqslant i\leqslant n,\ u_1\neq 0\mid\}$$

而向量 u 和 v 的汉明(Hamming)距离 $d_H(u,v)$ 为它们相异位的个数：

$$d_H(u, v) = \#\{i \mid 1 \leqslant i \leqslant n, u_i \neq v_i\} = w_H(u-v)$$

容易验证，Hamming 距离满足数学上一个距离所具有的以下 3 个性质：

对于 $u, v, w \in F_q^n$

(1) $d_H(u, v) \geqslant 0$，并且 $d_H(u, v) = 0$（当且仅当 $u = v$）；

(2) $d_H(u, v) = d_H(v, u)$（对称性）；

(3) $d_H(u, w) \leqslant d_H(u, v) + d_H(v, w)$。

定义 5.3 对于码长为 n 的 q 元码 S（即 S 为 F_q^n 的非空子集合），S 的最小距离 $d = d(S)$ 定义为 S 中任意两个不同码字之间 Hamming 距离的最小值，即

$$d = d(S) = \min\{d_H(u, v) \mid u, v \in S, u \neq v\}$$

下面结果是经典纠错编码的基础，它表明一个码 S 的最小距离恰好反映了纠错能力。

定理 5.1 若 d 为码 S 的最小距离，则码 S 可用来检查小于等于 $d-1$ 位错误，也可纠正小于等于 $\left[\frac{d-1}{2}\right]$ 位错误（这里对实数 α，$[\alpha]$ 表示 α 的整数部分，即不超过 α 的最大整数）。于是

$$\left[\frac{d-1}{2}\right] = \begin{cases} l & d = 2l+1 \\ l-1 & d = 2l \end{cases}$$

证明：发方把码字 $x \in S$ 发给收方。如果信道发生错误 $0 \neq \varepsilon \in F_q^n$，并且错位数不超过 $d-1$，即 $1 \leqslant w_H(\varepsilon) \leqslant d-1$，则收方得到的 $y = x + \varepsilon$ 不是码字。因为由 $\varepsilon \neq 0$ 可知，$y = x + \varepsilon \neq x$，又由于 S 中的其他码字 $x'(\neq x)$ 与 x 的 Hamming 距离都大于等于 d，而 $d_H(y, x) = w_H(y-x) = w_H(\varepsilon) \leqslant d-1$，所以 y 也不是 x'。因此，收方发现出错，即可检查小于等于 $d-1$ 位错误。

现在设码字 x 在信道中发生小于等于 $\left[\frac{d-1}{2}\right]$ 位错误，即 $w_H(\varepsilon) \leqslant \left[\frac{d-1}{2}\right]$。收方得到 $y = x + \varepsilon$，它与 x 的距离为 $d_H(y, x) = w_H(\varepsilon) \leqslant \left[\frac{d-1}{2}\right]$。而对于 S 中其他码字 $x'(\neq x)$，由三角形不等式图 5-2：

$$d \leqslant d_H(x, x') \leqslant d_H(y, x) + d_H(y, x')$$

于是

$$d_H(y, x') \geqslant d - d_H(y, x) \geqslant d - \left[\frac{d-1}{2}\right] > \left[\frac{d-1}{2}\right]$$

这表明：在 S 的所有码字当中，只有 x 与收到的向量 y 最近。将 y 译成 x，就完

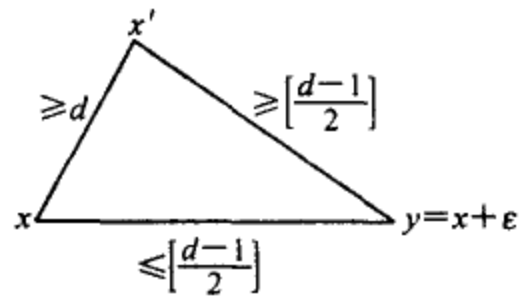


图 5-2　编码与最小距离的关系

成了纠错功能。

对于一个 q 元(即 F_q 上)纠错码 S,码长 n、码字数 K(或用信息位数 $k=\log_q K$)和最小距离 d 是 3 个基本参数,这个码可表示成(n, K, d)或者$[n, k, d]$。

由于 $K=|S|\leqslant|F_q^n|=q^n$,可知 $k=\log_q K\leqslant n$。如果不考虑纠错,一个信息用 k 位向量传送即可。现在为了有纠错能力,改用 n 位向量来传送,$\frac{k}{n}$表示纠错码的效率,因此,我们是在损失效率(增加传送时间)之下得到了纠错功能。一个好的纠错码就是指有大的$\frac{k}{n}$(高效率)和大的 d(纠错性能强)。

例 5.2　考虑由以下 16 个码字组成的二元码 C(码长 $n=7$,码字数 $K=16$,信息位数$k=\log_2 K=4$):

0010111	1101000
1001011	0110100
1100101	0011010
1110010	0001101
0111001	1000110
1011100	0100011
0101110	1010001
0000000	1111111

可以验证,这个码 C 的最小距离为 3,即 C 为二元码$[n, k, d]=[7, 4, 3]$;效率为 4/7,可纠正 1 位错。

例 5.1 中的重复码是二元码$[9, 3, 3]$。码 C 和这个重复码有同样的纠错性能,但是 C 的 k 值大(可传送 16 个信息,而重复码只能传送 8 个信息),并且 C 的效率高(对于 C, $k/n=4/7$;而重复码的效率为 $3/9=1/3$)。这表明:构造好的纠错码是很有学问的。

构造好的纠错码是经典纠错码理论的一个重要数学课题,从工程角度考虑,另一个重要课题是对于纠错码 S 要有好的纠错译码算法。看一下定理 5.1 的证

明：当收到 y 之后，要将 y 与 S 中所有码字相比较，找到与 y 距离最近的那个码字 x。这个算法太花时间。所以，尽管有好的纠错码，如果没有好的译码算法，工程上也不实用。

为了寻求性能好的纠错码和好的译码算法，我们要研究 F_q^n 的一些特殊的子集合 S，即将 S 加上某些代数结构，从而可使用更多的代数工具。一个自然的想法是考虑 F_q^n 的 F_q 一向量子空间，从而可采用线性代数工具。

定义 5.4 F_q^n 的一个 F_q 向量子空间 C 叫作是码长为 n 的 q 元线性码。

设 k 是向量子空间 C 的维数 $(1 \leqslant k \leqslant n)$，则 C 存在一组基 $u_1, \cdots, u_k$，其中：

$$u_1 = (a_{i1}, \cdots, a_{in}) \ (1 \leqslant i \leqslant k) \ (a_{ij} \in F_q)$$

而 C 中每个码字均惟一地表示成它们的 F_q 线性组合：

$$c = b_1 u_1 + \cdots + b_k u_k (b_i \in F_q)$$

所以 C 中的码字个数为 $K = q^k$，而 $k = \log_q K$，这表明向量子空间 C 的维数 k 就是信息位数。

以 $u_1, \cdots, u_k$ 为行的矩阵

$$G = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{bmatrix}$$

称作线性码 C 的一个生成矩阵。这是 F_q 上（即元素属于 F_q）的一个 k 行 n 列矩阵，并且矩阵 G 的秩为 k。

对于每个 $c \in F_q^n$，c 是码字 $(c \in C)$，$\Leftrightarrow c = b_1 u_1 + \cdots + b_k u_k$

$$\Leftrightarrow c = (b_1 + b_2 + \cdots + b_k) \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{bmatrix} = (b_1 + b_2 + \cdots + b_k) G$$

$K = q^k$ 个信息本来可以用 F_q^k 中长为 k 的向量 $(b_1, b_2, \cdots, b_k)$ 表示，现在为了有纠错能力，将每个 $(b_1, b_2, \cdots, b_k)$ 改用 F_q^n 中长为 n 的向量 $c = (b_1, b_2, \cdots, b_k)G$。这叫作“纠错编码”，所以对于线性码，纠错编码相当于乘以生成矩阵 G。

另一方面，从线性代数知道，F_q^n 的一个 k 维线性子空间还可以看成是变量 $x_1 \sim x_n$ 在 F_q 上(即系数属于 F_q)$n-k$ 个齐次线性方程组

$$\begin{cases} b_{11}x_1 + b_{12}x_2 + \cdots + b_{1n}x_n = 0 \\ b_{21}x_1 + b_{22}x_2 + \cdots + b_{2n}x_n = 0 \\ \cdots \\ b_{n-k,1}x_1 + b_{n-k,2}x_2 + \cdots + b_{n-k,n}x_n = 0 \end{cases} \tag{5.1}$$

的解空间。其中系数矩阵

$$H = (b_{ij})_{1 \leqslant i \leqslant n-k,\ 1 \leqslant j \leqslant n} \tag{5.2}$$

是 F_q 上 $n-k$ 行 n 列的矩阵，并且 H 的秩为 $n-k$(即方程组(5.1)中 $n-k$ 个线性方程都是独立的)。H 叫作线性码 C 的一个校验矩阵。由于方程组(5.1)可以写成

$$H\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = Hx^T = 0 \in F_q^{n-k}$$

其中 $x = (x_1, \cdots, x_n)$，x^T 表示向量 x 的转置(列向量)。所以对每个 $v \in F_q^n$，

$$v \in C \Leftrightarrow Hv^T = 0$$

也就是说，用校验矩阵乘以 v^T 可以判断 v 是否为码字。即线性码的检错问题只需简单地乘以校验阵即可：若收到 y，而 $Hy^T \neq 0$，则 y 不属于 C，从而信道产生错误。

校验阵 H 的功能不仅于此，它还可以用来决定线性码的最小距离。

定理 5.2　设 C 是参数$[n, k, d]$的 q 元线性码，则

(1) C 的最小距离 d 等于 C 中非零码字 Hamming 权的最小值

$$d = \min\{w_H(c) \mid 0 \neq c \in C\}$$

(2) 将 C 的校验阵 H 写成 n 个列向量

$$H = [v_1 \quad v_2 \quad \cdots \quad v_n],\ v_j = \begin{pmatrix} b_{1,j} \\ b_{2,j} \\ \vdots \\ b_{n-k,j} \end{pmatrix} \in F_q^{n-k}$$

则线性码 C 的最小距离 d 是满足以下两个条件的正整数 d：

(i) H 中任意 $d-1$ 个不同的列向量都是 F_q—线性无关的；

(ii) 存在 H 中 d 个不同的列向量，它们是 F_q—线性相关的。

证明思路：

(1) 根据定义，d 是 C 中不同码字 c 和 c'(共有 $K(K-1)/2$ 对)的 Hamming 距离 $d_H(c, c') = w_H(c-c')$ 的最小值。但是对于线性码 C，$c-c'$ 是 C 中非零码字，所以 d 为 C 中所有非零码字(共 $K-1$ 个)Hamming 权的最小值。

(2) H 中有 l 个不同的列向量线性相关，当且仅当 C 中有 Hamming 权为 l 的码字。比如，$H=[v_1 \quad v_2 \quad \cdots \quad v_n]$ 的前 l 个向量 $v_1 \quad v_2 \quad \cdots \quad v_l$ 线性相关，

$$b_1v_1+b_2v_2+\cdots+b_lv_l=0 \ (b_1, b_2, \cdots, b_l \in F_q; \text{为 } F_q \text{ 中非零元素})$$

则

$$H\begin{bmatrix} b \\ \vdots \\ b_l \\ 0 \\ \vdots \\ 0 \end{bmatrix} = [v_1 \quad v_2 \quad \cdots \quad v_n]\begin{bmatrix} b \\ \vdots \\ b_l \\ 0 \\ \vdots \\ 0 \end{bmatrix} = b_1v_1+b_2v_2+\cdots+b_lv_l=0$$

即 $c=(b_1, \cdots, b_l, 0, \cdots, 0) \in C$，而 $w_H(c)=l$。由本定理的(1)知，C 中有权为 d 的码字，但是没有权为 $1, 2, \cdots, d-1$ 的码字，这就相当于条件(i)和(ii)。

例 5.3 设 C 是以 H 为校验阵的二元线性码，

$$H=\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

H 是 $n-k=3$ 行、$n=7$ 列，元素属于二元域 $F_2=\{0, 1\}$，并且 H 的秩为 3(由于后三列线性无关)，于是 C 的码长为 $n=7$，信息位数为 $k=7-3=4$，所以 C 共有 16 个码字。H 的 7 个列向量是不同的非零向量，所以任意两列均线性无关。但是

$$\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}+\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}=\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

即 H 的第 1、2、4 列线性相关。由定理 2.5(2)可知线性码 C 的最小距离 d 为

3，即 C 为二元线性码 $[n, k, d]=[7, 4, 3]$。

将 H 记成

$$H=[P \quad I_3],\ P=\begin{bmatrix}1&0&1&1\\1&1&1&0\\0&1&1&1\end{bmatrix},\ I_3=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

则

$$G=[I_4 \quad P^T]=\begin{bmatrix}1&0&0&0&1&1&0\\0&1&0&0&0&1&1\\0&0&1&0&1&1&1\\0&0&0&1&1&0&1\end{bmatrix}$$

是 C 的一个生成矩阵，这是由于 $HG^T=0$（$n-k$ 行 k 列的零矩阵）。算出 G 的 4 个行向量（这是 C 的一组基）的所有 16 个线性组合，便给出 C 中全部码字。可以验证，这 16 个码字就是例 5.2 中的那些码字，也就是说，例 5.2 中的纠错码 C 是这样构造出来的二元线性码。

例 5.3 中的线性码是“最优”码。如何判别一个纠错码是好码？在 3 个基本参数 n、k、d 之间有互相制约的关系。这些关系用不等式来刻画，称作是纠错码的界（bound）。使不等式达到等式的码就是某种意义上的最优码。下面是经典纠错码的 3 个最著名的界。

定理 5.3

（1）若存在参数为 $[n, k, d]$ 的 q 元纠错码，则

（i）（Hamming 界）$q^{n-k}\geqslant\sum_{i=0}^{\left[\frac{d-1}{2}\right]}(q-1)^i\binom{n}{i}$，其中 $\binom{n}{i}$ 为 n 个物体中取 i 个的组合，即

$$\binom{n}{i}=\frac{n(n-1)\cdots(n-i+1)}{i!}$$

（ii）（Singleton 界）$n\geqslant k+d-1$

（2）（Gilber-Varshamov 界）设 $1\leqslant d\leqslant n$，$2\leqslant K\leqslant q^n$，$q$ 为素数幂。如果

$$(k-1)\left(\sum_{i=1}^{d-1}(q-1)^i\binom{n}{i}\right)<q^n$$

则必存在参数为(n, K, d)的q元纠错码。

证明思路：

(1) 对于F_q^n中的每个向量v和整数l,用$B(v; l)$表示以v为中心以l为半径的球：

$$B(v; l) = \{x \in F_q^n \mid d_H(v, x) \leqslant l\}$$

这个球的体积为

$$b(l) = \mid B(v; l) \mid = \sum_{i=0}^{l} (q-1)^i \binom{n}{i}$$

若C是q元纠错码$[n, k, d]$,则以q^k个码字为中心,半径为$\left[\frac{d-1}{2}\right]$的$q^k$个球两两不相交。它们的体积之和应不超过整个空间$F_q^n$的体积$q^n$,即$q^n \geqslant q^k \times b\left(\left[\frac{d-1}{2}\right]\right)$。这就是Hamming界。

考虑由C给出的新码。对每个$a \in F_q$,记

$$C_a = \{(c_1, \cdots, c_{n-1}) \in F_q^{n-1} \mid (c_1, \cdots, c_{n-1}, a) \in C\}$$

这个码的码长为$n-1$,最小距离$\geqslant d$。由于$C = \sum_{a \in F_q} \mid C_a \mid$,所以存在$a \in F_q$,使得$\mid C_a \mid \geqslant \mid C \mid /q = q^{k-1}$。这表明$C_a$的参数为$[n-1, \geqslant k-1, \geqslant d]$。递推下去,可知存在纠错码$[d, k-n+d, d]$,于是必然$k-n+d \leqslant 1$,即$n \geqslant k+d-1$。这为Singleton界。

(2) 如果存在q元码(n, N, d),其中$1 \leqslant N < K$,以N个码字为中心,$d-1$为半径的N个球总体积不超过$N \times b(d-1)$。由假设,$N \times b(d-1) \leqslant (K-1)b(d-1) < q^n$。所以,在这$N$个球之外还有向量$v \in F_q^n$。$v$与所有码字的距离均$\geqslant d$。将$v$加入之后,新的码为$(n, N+1, d)$。由此可知必存在$q$元码$(n, K, d)$。

Hamming界和Singleton界都是码的必要性条件。达到等式的码都是最优码。满足$q^{n-k} = b\left(\left[\frac{d-1}{2}\right]\right)$的码叫作完全码(perfect),满足$n = k+d-1$的码叫作极大距离可分码(maximal Distance Separable,简称MDS码)。这是两类好的纠错码,对于例5.3中的二元码$[7, 4, 3]$,$\left[\frac{d-1}{2}\right] = 1$,而

$$q^{n-k} = 2^{7-4} = 8 \qquad b(1) = \sum_{i=0}^{1} (2-1)^i \binom{7}{i} = 1+7 = 8$$

所以这是完全码。

G－V 界是纠错码存在的充分性条件。当 $q^{n-k} \geqslant b(d-1)$ 时，一定存在 q 元码$[n, k, d]$。但是证明本身没有给出这种码的具体构造方式。G－V 界是 1952 年建立的。直到 30 年后，在发明代数几何码以后，人们才于 1982 年具体给出达到和超过 G－V 界的一批纠错码。

利用抽象代数工具人们研究了线性码的一个子类——循环码。其中特别一类循环码(叫 BCH 码)可以设计出最小距离 d 很大的码，并且有很实用的纠错译码算法，目前在数字通信中被普遍采用。1980 年以后用代数几何构造出的代数几何码，其性能比 BCH 码要好，但目前译码算法还不能达到实用程度。

5.1.4　从编码本身看(7, 4)汉明码的构造方法及其相关概念

从上一节的讨论我们了解汉明码在纠错编码中的代表性，下面从编码本身的角度来了解汉明码的构造方法。

汉明码是线形分组码。汉明码的编码宗旨在于：在信道输入端的 2^n 个 n 长的二元序列中找一组 2^k 个码字，使码字的 $r=n-k$ 个校验元与其 k 个信息元之间满足一定的线性关系，并使码书中码字之间的最小距离最大。

例如：(7, 4)汉明码中 $n=7$，$k=4$，$r=n-k=7-4=3$。根据汉明码的编码规则，在信道输入端的 2^7 个 7 个 bit 长的二元序列集合

$$C=\{(c_6c_5c_4c_3c_2c_1c_0) \mid c_i \in \{0, 1\}, i=0, 1, \cdots, 6\}$$

中找出一组 $2^4(=16)$ 个码字

0000000	0100101	1000011	1100110
0001111	0101010	1001100	1101001
0010110	0110011	1010101	1110000
0011001	0111100	1011010	1111111

其特点是 16 个码字是所有码长为 7 的二元序列中的一个封闭子集，它的封闭性表现为 C_i，$C_j \in C$，则 $C_i+C_j=C_k \in C$，$i, j, k=1, 2, \cdots, 16$。且任一 $C_i=(c_6c_5c_4c_3c_2c_1c_0)$ $i=1, 2, \cdots, 16$ 的前 4 位$(c_6c_5c_4c_3)$即信源码，与后 $(r=n-k)$ 3 位$(c_2c_1c_0)$即校验码应满足一线性关系。

为了说明如何度量码字之间的距离以及如何描述经过有噪信道后编码的出错情况，上一节中引入了汉明权 $w_H(u)$和汉明距离 $d_H(u, v)$的概念。码字的汉明距离可理解为：长度为 n 的两个序列(码字)C_i 和 C_j 之间的距离是指 C_i 和 C_j 之间对应位置上不同码元的个数，用符号 $d_H(C_i, C_j)$表示。

例如：$C_i = 101111$，$C_j = 111100$，则 $d_H(C_i, C_j) = 3$。

码字的汉明权重可理解为：码字的汉明权重是指码字中含非零码元的个数，在二元码中码字是 n 长的二元序列，所以码字的汉明权重即为码字中含“1”的个数。

令码字 $u = (c_6c_5c_4c_3c_2c_1c_0)$，则码字权重为

$$w_H(u) = \sum_{i=0}^{n-1} c_i \qquad c_i \in \{0, 1\}$$

因此，码字 C_i 和 C_j 间的距离可以写成

$$d_H(C_i, C_j) = w_H(C_i \oplus C_j)$$

（注：⊕表示模二运算）

码的最小距离可理解为：码书中码的最小距离等于非零码字的最小权重，即

$$d_{\min} = \min w_H(C_i) \qquad C_i \in C, C_j \neq 0$$

错误图样意思是在二元无记忆 n 次扩展信道中，差错的形式也可以用二元序列来描述。这种差错的描述称为错误图样。即 $E = (e_{n-1}e_{n-2}\cdots e_1e_0)$，其中：

$$e_i = \begin{cases} 0 \\ 1 \end{cases} \qquad i = n-1, n-2, \cdots, 1, 0$$

当 e_i 取 0 值时表示该码元没有发生错误，当 e_i 取 1 值时表示该码元发生了错误。

因为在二元信道中码元传输发生错误情况就是“0”变成“1”或“1”变成“0”。令 R 表示输出端接收的二元序列，则

$$R = E \oplus C \text{ 或 } E = C \oplus R$$

设二元对称信道中，p 为错误发生的概率（$p < \frac{1}{2}$），$\bar{p} = 1 - p$ 为正确的传递概率，则二元无记忆 n 次扩展信道中错误图样 E 出现的概率为

$$P(E) = \bar{p}^{n-W(E)} p^{W(E)}$$

由此可得信道编码在有噪信道传输中：

发生一位错误：$w_H(E_1) = 1$　　$P(E_1) = \bar{p}^{n-1} p$

发生二位错误：$w_H(E_2) = 2$　　$P(E_2) = \bar{p}^{n-2} p^2$

……

发生 e 位错误：$w_H(E_e) = e$　　$P(E_e) = \bar{p}^{n-e} p^e$

……

全错：$w_H(E_n)=n \qquad P(E_n)=p^n$

因为 $p<\frac{1}{2}$，所以发生一位错误、两位错误的概率大于发生多位错误的概率。

(7，4)汉明码的校验矩阵：(7，4)汉明码其码长 $n=7$，其中信源码长 $k=4$，校验码长 $r=3$。

长为 3 的二元序列共有 $2^3=8$，将其中的 7 个非零向量序列按列排列成如下矩阵：

$$H_{(7,4)}=\begin{bmatrix}1&0&0&0&1&1&1\\0&1&0&1&0&1&1\\0&0&1&1&1&0&1\end{bmatrix}$$

该矩阵称为(7，4)的校验矩阵，设码字 $C_i=(c_6c_5c_4c_3c_2c_1c_0)$，则

$$H\cdot C^T=0^T$$

其中 $0=(0\quad 0\quad 0)$，0^T 是 0 矢量的转置，C^T 是码字 C 的转置。即满足下列方程组：

$$\begin{cases}c_3+c_2+c_1+c_0=0\\c_5+c_4+c_1+c_0=0\\c_6+c_4+c_2+c_0=0\end{cases}$$

上面 3 个方程表示了码字 $C_i=(c_6c_5c_4c_3c_2c_1c_0)$ 的码元(信源码和校验码)之间的线性关系，因为信源码长 $k=4$，所以不同码字有 $M=2^4=16$ 个。令码字 C 中前 4 位码元为信源码，即得如下的 16 个码字：

0000000	0100101	1000011	1100110
0001111	0101010	1001100	1101001
0010110	0110011	1010101	1110000
0011001	0111100	1011010	1111111

从(7，4)汉明码中可知 $\min w_H(C_i)=3$，则 $d_{\min}=3$。这也可以从 $H_{(7,4)}$ 中看出，校验矩阵中各列都不相同，任意两列之和都不等于 $0=(0\quad 0\quad 0)$，但任意两列之和一定等于矩阵中的某一列，所以码字的最小权重为 3。

这 16 个码字中只有 $k=4$ 个码字是独立码字，其他码字可由这 4 个独立码字线性组合而来，将这 4 个独立码字按行排列成如下矩阵：

$$G=\begin{bmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{bmatrix}$$

该矩阵称为生成矩阵，它满足

$$(c_6c_5c_4c_3)G=(c_6c_5c_4c_3c_2c_1c_0) \tag{5.3}$$

可得

$$H\cdot G^T=0^T \text{ 或 } G^T\cdot H=0$$

式中 0 是一个 4×3 阶($k\times(n-k)$) 矩阵。我们可由式(5.3)生成全体码字，因此编码可由生成矩阵来实现，即 F_2^7 的子集 F_2^4 可由 G 生成。

假设信道中发生随机错误，并设错误图样为 E，即接收序列 $R=E\oplus C$，则应有

$$H\cdot R^T=H\cdot E^T\oplus H\cdot C^T=H\cdot E^T\neq 0^T \tag{5.4}$$

若设 $E=(e_6e_5e_4e_3e_2e_1e_0)=(0001000)$，即 $e_3=1$，表示码字中第 4 位码元发生错误，代入式(5.4)有

$$H\cdot E^T=\begin{bmatrix}s_2\\s_1\\s_0\end{bmatrix}=\begin{bmatrix}1\\0\\0\end{bmatrix}$$

正好是 H 矩阵中第 4 列，由此可见：

$$H\cdot E^T=S^T \qquad S^T=\begin{bmatrix}s_2\\s_1\\s_0\end{bmatrix}$$

这里的 S^T 一定是 H 矩阵的某一列，此 S 称为伴随式。由此可得由矩阵 H 进行译码，根据所得伴随式就可以判断码字中哪一位码元出现了错误。

由以上介绍可知，汉明码有 r 个校验元，就有 2^r-1 个不同的非全零向量，将它们按列排成矩阵则可以得到一个校验矩阵 H，有了矩阵 H 就可生成码字并进行译码了。

5.1.5 量子纠错编码的基本概念

一个量子位(quantum bit，简称 qubit)是二维复向量空间 C^2 中的非零向

量，量子物理中把 C^2 的一组基表示成$|0\rangle$和$|1\rangle$，所以一个量子位为

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (\alpha \in C, \beta \in C, (\alpha, \beta) \neq (0, 0))$$

一个量子状态是 n 个 C^2 的张量积$(C^2)^{\otimes n}$中的非零向量。这是 2^n 维复向量空间，它有一组基

$$|a_1\rangle \otimes |a_2\rangle \otimes \cdots \otimes |a_n, (a_i \in \{0, 1\} = F_2, (1 \leqslant i \leqslant n))$$

这个向量也简单记成 $|a_1 a_2 \cdots a_n\rangle = |a\rangle$，其中 $a = (a_1, a_2, \cdots, a_n) \in F_2^n$。所以，每个量子状态$|\varphi\rangle$是它们的复线性组合：

$$|\varphi\rangle = \sum_{(a_1, a_2, \cdots, a_n) \in F_2^n} c(a_1, a_2, \cdots, a_n)|a_1 a_2 \cdots a_n\rangle = \sum_{a \in F_2^n} c(a)|a\rangle$$

其中 $c(a_1, a_2, \cdots, a_n) = c(a) \in C$（不全为零）。

在 2^n 维复向量空间中有厄米特内积$\langle v|u\rangle$，对于

$$|v\rangle = \sum_a c(a)|a\rangle, \quad |u\rangle = \sum_a d(a)|a\rangle$$

则它们的厄米特内积定义为

$$\langle v|u\rangle = \sum_{a \in F_2^n} \overline{c(a)} d(a) \in C$$

其中$\overline{c(a)}$表示复数 $c(a)$的共轭复数。

在量子物理中：

(1) 彼此相差一个非零复数因子的两个非零向量看成是同一个量子态。即若 $|v\rangle = \alpha|u\rangle$（相当于对每个 $a \in F_2^n$，$c(a) = \alpha d(a)$），其中 α 是非零复数，则$|v\rangle$和$|u\rangle$为同一个量子态。

(2) $|v\rangle$和$|u\rangle$是完全可区分的，是指 $\langle v|u\rangle = 0$（正交）。

定义 5.5　$V = (C^2)^{\otimes n} = C^{2n}$ 中每个复向量子空间 Q 都叫作一个量子码。n 叫作 Q 的码长，Q 的维数记为 $K = \dim Q$，而令 $k = \log_2 K$。由 $1 \leqslant K \leqslant 2^n$ 可知 $0 \leqslant k \leqslant n$。

除了 n 和 K（或 k）之外，量子码还应该有一个参数反映纠错能力。这里需要解释什么是量子错误。

在经典的数字通信中，信息 $x = (x_1, \cdots, x_n)$ 和错误 $\varepsilon = (\varepsilon_1, \cdots, \varepsilon_n)$ 都是 F_q^n 中的向量，错误 ε 对信息 x 的作用是相加：$y = x + \varepsilon$。在量子通信中，信息是 V 中的非零向量$|v\rangle$，而错误是复空间 V 上的酋线性算子 e，e 在 V 上的作用是酋线性变换 $e|v\rangle$。

每个量子位为 $|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$，根据 P. Shor 的简化，只需考虑 3 种错误作用，它们的矩阵表示为 3 个 Pauli 阵：

$$\sigma_x=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},\ \sigma_z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

$$\sigma_y=i\sigma_x\sigma_z=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}\ (i=\sqrt{-1})$$

所以，在$|\varphi\rangle$上的作用为

$$\sigma_x|\varphi\rangle=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}=\begin{bmatrix}\beta\\ \alpha\end{bmatrix}=\beta|0\rangle+\alpha|1\rangle$$

$$\sigma_z|\varphi\rangle=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}=\begin{bmatrix}\alpha\\ -\beta\end{bmatrix}=\alpha|0\rangle-\beta|1\rangle$$

$$\sigma_y|\varphi\rangle=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}=\begin{bmatrix}-i\beta\\ i\alpha\end{bmatrix}=i(-\beta|0\rangle+\alpha|1\rangle)$$

这 3 个作用都是酉作用，并且满足

$$\sigma_x^2=\sigma_y^2=\sigma_z^2=I_2(\text{单位阵}),\sigma_x\sigma_z=-\sigma_z\sigma_y$$

由于

$$\sigma_x|0\rangle=|1\rangle,\ \sigma_x|1\rangle=|0\rangle,\ \sigma_z|0\rangle=|0\rangle,\ \sigma_z|1\rangle=-|1\rangle$$

这可以写成

$$\sigma_x|a\rangle=|a+1\rangle,\ \sigma_z|a\rangle=(-1)^a|a\rangle\ (a\in F_2=\{0,1\})$$

注意，$\sigma_y=i\sigma_x\sigma_z$ 和$\sigma_x\sigma_z$ 是同样的量子作用。因为 $i\sigma_x\sigma_z|\varphi\rangle=i(\sigma_x\sigma_z|\varphi\rangle)$，而 $\sigma_x\sigma_z|\varphi$ 和$\sigma_x\sigma_z|\varphi\rangle$是同一个量子态，将 $\sigma_x\sigma_z$ 乘以 i 是由于

$$i\sigma_x\sigma_z=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$$

不但为酉矩阵，而且是厄米特阵，它的本征值均为实数。

在复空间 $V=C^2\otimes C^2\otimes\cdots\otimes C^2=(C^2)^{\otimes n}$ 上的错误作用有形式

$$e=i^\lambda w_1\otimes\cdots\otimes w_n$$

其中 $0 \leqslant \lambda \leqslant 3$，$w_1 \in \{I_2, \sigma_x, \sigma_y, \sigma_z\}$，$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ 表示无错误。

e 在基向量

$$|a\rangle = |a_1\rangle \otimes |a_2\rangle \otimes \cdots \otimes |a_n\rangle \quad (a = (a_1, a_2, \cdots, a_n) \in F_2^n)$$

上的作用是按分量作用：

$$e|a\rangle = i^{\lambda}(w_1|a_1\rangle) \otimes (w_2|a_2\rangle) \otimes \cdots \otimes (w_n|a_n\rangle)$$

由于 e 是酋线性变换，所以 e 在任意量子态 $|\varphi\rangle = \sum_{a \in F_2^n} c(a)|a\rangle$ 上的作用为

$$e|\varphi\rangle = \sum_{a \in F_2^n} c(a) e|a\rangle$$

例如，当 $n = 2$ 时，对于 $e = \sigma_x \otimes \sigma_y$，$|\varphi\rangle = \alpha|00\rangle + \beta|10\rangle$，则

$$\begin{aligned} e|\varphi\rangle &= (\sigma_x \otimes \sigma_y)(\alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |0\rangle) \\ &= \alpha(\sigma_x|0\rangle \otimes \sigma_y|0\rangle) + \beta(\sigma_x|1\rangle \otimes \sigma_y|0\rangle) \\ &= \alpha|1\rangle \otimes i|1\rangle + \beta|0\rangle \otimes i|1\rangle \\ &= \alpha i|11\rangle + \beta i|01\rangle \end{aligned}$$

所有错误算子组成的集合 $E = E_n$

$$E_n = \{i^{\lambda} w_1 \otimes w_2 \otimes \cdots \otimes w_n \mid 0 \leqslant \lambda \leqslant 3,\ w_i \in \{I_2, \sigma_x, \sigma_y, \sigma_z\} \ (1 \leqslant i \leqslant n)\}$$

形成一个乘法群，其中 $e = i^{\lambda} w_1 \otimes \cdots \otimes w_n$ 和 $e' = i^{\lambda'} w_1' \otimes \cdots \otimes w_n'$ 的乘法定义为

$$ee' = i^{\lambda+\lambda'}(w_1 w_1') \otimes \cdots \otimes (w_n w_n')$$

例如，当 $n = 2$ 时，对于 $e = I_2 \otimes \sigma_x$ 和 $e' = \sigma_y \otimes \sigma_z$，有

$$ee' = \sigma_y \otimes \sigma_x\sigma_z = -i\sigma_y \otimes \sigma_y = i^3 \sigma_y \otimes \sigma_y$$

$$e'e = \sigma_y \otimes \sigma_z\sigma_x = i\sigma_y \otimes \sigma_y$$

（注意：$\sigma_y = i\sigma_x\sigma_z$，$\sigma_x\sigma_z = -\sigma_z\sigma_x$。于是，$\sigma_x\sigma_z = -i\sigma_y$，$\sigma_z\sigma_x = i\sigma_y$）

所以 E_n 不是交换群。容易看出，对任何 $e, e' \in E_n$，均有 $ee' = e'e$ 或 $ee' = -e'e$，$e^2 = \pm I_2$，$|E_n| = 4^{n+1}$，所以 E_n 是 4^{n+1} 阶非交换群。这个群的中心为 4 元群

$$C(E) = \{i^{\lambda} = i^{\lambda} I_2 \otimes \cdots \otimes I_2 \mid 0 \leqslant \lambda \leqslant 3\}$$

而商群

$$\overline{E}_n = E_n/C(E),\ (|\ \overline{E}_n\ | = |\ E_n\ |/4 = 4^n)$$

中元素($e \in E_n$)有关系

$$\overline{e}^2 = I_2,\ \overline{e}\overline{e}' = \overline{e}'\overline{e},\ (\text{由于} -1 \in C(E_n))$$

所以 $\overline{E}_n$ 是 4^n 阶交换群,并且每个元素的平方均为 1,从而它应当是 $2n$ 个 2 阶循环群的直积,于是同构于 F_2^{2n} 的加法群。

为了进一步弄清非交换群 E_n 的结构,Calderbank 等人引入一种新的符号。将错误算子

$$e = i^\lambda w_1 \otimes \cdots \otimes w_n \qquad w_i \in \{I_2, \sigma_x, \sigma_y, \sigma_z\}$$

表示成

$$e = i^\lambda X(a)Z(b) \quad a = (a_1, \cdots, a_n) \in F_2^n,\ b = (b_1, \cdots, b_n) \in F_2^n$$

其中:

$$(a_i, b_i) = \begin{cases} (0,0) & w_i = I_2 \\ (1,0) & w_i = \sigma_x \\ (0,1) & w_i = \sigma_z \\ (1,1) & w_i = \sigma_y \end{cases} \qquad (1 \leqslant i \leqslant n)$$

例如,$e = i\sigma_y \otimes I_2 \otimes \sigma_x = iX(101)Z(100)$。

下面引理表明,这种新的符号在运算时有好的表达式。

引理 5.1:

(1) $X(a)$和 $Z(b)$ ($a = (a_1, \cdots, a_n) \in F_2^n,\ b = (b_1, \cdots, b_n) \in F_2^n$) 在 $V = C^2 \otimes C^2 \otimes \cdots \otimes C^2$ 的基元上的作用为 $|\ v\rangle = |\ v_1, \cdots, v_n\rangle$ ($v = (v_1, \cdots, v_n) \in F_2^n$)

$$X(a)\ |\ v\rangle = |\ a + v\rangle,\ Z(b)\ |\ v\rangle = (-1)^{b \cdot v}\ |\ v\rangle$$

其中 $b \cdot v = \sum_{i=0}^{n} b_i v_i \in F_2$ 为 F_2^n 中的通常内积。

(2) 对于 E_n 中的两个错误算子 $e = i^\lambda X(a)Z(b)$ 和 $e' = i^{\lambda'}X(a')Z(b')$,

$$ee' = (-1)^{a \cdot b' + a' \cdot b} e'e$$

于是 e 和 e' 可交换当且仅当 $a \cdot b' + a' \cdot b = 0 \in F_2$。

(3) 映射

$$\varphi: E_n \to F_2^{2n},\ e = i^{\lambda} X(a) Z(b) \to \varphi(e) = \langle a \mid b \rangle$$

给出群 $\overline{E}_n$ 和加法群 F_2^n 的同构

$$\overline{\varphi}: \overline{E}_n = E_n / \{\pm 1, \pm i\} \xrightarrow{\sim} F_2^{2n},\ \overline{\varphi}(\overline{e}) = \varphi(e) = \langle a \mid b \rangle$$

证明：

(1) 设 $X(a) = X(a_1, \cdots, a_n) = w_1 \otimes w_2 \otimes \cdots \otimes w_n$，由定义可知 $a_i = 0$ 时，$w_i = I_2$，$w_i \mid v_i\rangle = \mid v_i\rangle$。而当 $a_i = 1$ 时，$w_i = \sigma_x$，$w_i \mid v_i\rangle = \sigma_x \mid v_i\rangle = \mid v_i + 1\rangle$，所以总有 $w_i \mid v_i\rangle = \sigma_x \mid v_i\rangle = \mid v_i + a_i\rangle$。因此

$$\begin{aligned} X(a) \mid v\rangle &= (w_1 \mid v_1\rangle) \otimes \cdots \otimes (w_n \mid v_n\rangle) \\ &= \mid v_1 + a_1\rangle \otimes \cdots \otimes \mid v_n + a_n\rangle = \mid v + a\rangle \end{aligned}$$

同样地，令 $Z(b) = Z(b_1, \cdots, b_n) = w_1 \otimes w_2 \otimes \cdots \otimes w_n$，则当 $b_i = 0$ 时，$w_i = I_2$，$w_i \mid v_i\rangle = \mid v_i\rangle$。而当 $b_i = 1$ 时，$w_i = \sigma_z$，$w_i \mid v_i\rangle = \sigma_z \mid v_i\rangle = (-1)^{v_i} \mid v_i\rangle$，所以总有 $w_i \mid v_i\rangle = (-1)^{b_i v_i} \mid v_i\rangle$。于是

$$\begin{aligned} Z(b) \mid v\rangle &= (w_1 \mid v_1\rangle) \otimes \cdots \otimes (w_n \mid v_n\rangle) \\ &= ((-1)^{b_1 v_1} \mid v_1\rangle) \otimes \cdots \otimes ((-1)^{b_n v_n} \mid v_n\rangle) \\ &= (-1)^{b \cdot v} \mid v + a\rangle \end{aligned}$$

(2) 对每个基元 $\mid v\rangle = \mid v_1, \cdots, v_n\rangle$ $(v = (v_1, \cdots, v_n) \in F_2^n)$，

$$\begin{aligned} ee' \mid v\rangle &= i^{\lambda+\lambda'} X(a) Z(b) X(a') Z(b') \mid v\rangle \\ &= i^{\lambda+\lambda'} X(a) Z(b) X(a') (-1)^{b' \cdot v} \mid v\rangle \\ &= i^{\lambda+\lambda'} (-1)^{b' \cdot v} X(a) Z(b) \mid a' + v\rangle \\ &= i^{\lambda+\lambda'} (-1)^{b' \cdot v} X(a) (-1)^{b' \cdot (a'+v)} \mid a' + v\rangle \\ &= i^{\lambda+\lambda'} (-1)^{a' \cdot b + (b+b') \cdot v} \mid a + a' + v\rangle \end{aligned}$$

同样地有

$$e'e \mid v\rangle = i^{\lambda+\lambda'} (-1)^{a \cdot b' + (b+b') \cdot v} \mid a + a' + v\rangle = (-1)^{a' \cdot b + a' \cdot b} ee' \mid v\rangle$$

于是 $ee' = (-1)^{a \cdot b' + a' \cdot b} e'e$。

(3) 由于

$$X(a) Z(b) X(a') Z(b') = \pm X(a) X(a') Z(b) Z(b') = X(a + a') Z(b + b')$$

所以

$$\varphi(ee') = \varphi(X(a + a') Z(b + b')) = \langle a + a' \mid b + b'\rangle$$

$$= \langle a \mid b \rangle + \langle a' \mid b' \rangle = \varphi(e) + \varphi(e')$$

同样 φ 是群的(满)同态。它的核 $\ker\varphi$ 为 $\{\pm 1, \pm i\}$，所以 $\tilde{\varphi}$ 是群 $\overline{E}_n$ 到加法群 F_2^{2n} 的同构。

定义 5.6 对于 F_2^{2n} 中的向量 $u = \langle a \mid b \rangle$ 和 $u' = \langle a' \mid b' \rangle$ $(a, a', b, b' \in F_2^n)$，n 和 u' 的辛(symplectic)内积定义为

$$(u, u')_s = a \cdot b' + a' \cdot b = (a \quad b) \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix} \begin{bmatrix} a' \\ b' \end{bmatrix}$$

$$= \sum (a_i b_i' + a_i' b_i) \in F_2$$

当 (u, u') 时，称 u 和 u' 是辛正交的。对于 F_2^{2n} 的每个向量子空间 C，

$$(C)_s^{\perp} = \{u \in F_2^{2n} \mid (u, c)_s = 0, \text{ for all } c \in C\}$$

也是 F_2^{2n} 的向量子空间，叫作 C 辛对偶子空间。如果 $C \subseteq (C)_s^{\perp}$ (即 C 中任何两个向量均辛正交)，称 C 为 F_2^{2n} 的辛自正交子空间。由线性代数易知：

$$\dim C + \dim (C)_s^{\perp} = 2n$$

若 $C \subseteq C'$，则 $(C')_s^{\perp} \subseteq (C)_s^{\perp}$。由此可知 $(C)_s^{\perp}$ 的辛对偶为 C。以后把 $\bar{e} \in \overline{E}_n$ 等同于同构象 $\bar{\varphi}(\bar{e}) = \langle a \mid b \rangle \in F_2^{2n}$。

对于 E_n 中的 $e = i^{\lambda} X(a) Z(b)$ 和 $e' = i^{\lambda'} X(a') Z(b')$，则 $\bar{e} = \langle a \mid b \rangle$，$\bar{e}' = \langle a' \mid b' \rangle$。由引理 5.1 知：$e$ 和 e' 可交换当且仅当 $\bar{e}$ 和 $\bar{e}'$ 辛正交。因此，有以下一个重要的结果。

定理 5.4 E_n 的子群 G 是交换群当且仅当 G 在 $\overline{E}_n = F_2^{2n}$ 中的象 $\overline{G}$ 是辛自正交子空间。

这个结果在构造量子码时起到重要作用。

对于一个错误算子 $e = i^{\lambda} w_1 \otimes w_2 \otimes \cdots \otimes w_n \in E_n$，当 $w_i \in I_2$ 时，表示第 i 个量子位没有错误作用。而当 $w_i = \sigma_x, \sigma_y, \sigma_z$ 时，表示第 i 个量子位有错误作用。我们用 $\omega_Q(e)$ 表示 e 中有错误作用的量子位个数，叫作 e 的量子权，即

$$w_Q(e) = \#\{i \mid 1 \leqslant i \leqslant n, w_i \neq I_2\}$$

如果 $e = i^{\lambda} X(a) Z(b)$，$a = (a_1, \cdots, a_n) \in F_2^n$，$b = (b_1, \cdots, b_n) \in F_2^n$，则 $w_i = I_2$，当且仅当 $(a_i, b_i) = (0, 0)$，因此

$$w_Q(e) = \#\{i \mid 1 \leqslant i \leqslant n, (a_i, b_i) = (0, 0)\}$$

由于 $\bar{e} = \langle a \mid b \rangle \in F_2^{2n}$，在 F_2^{2n} 中引入与经典 Hamming 权不同的量子权：

$$w_Q\langle a \mid b\rangle = w_Q(\bar{e}) = \#\{i \mid 1 \leqslant i \leqslant n,\ (a_i,\ b_i) = (0,\ 0)\}$$

则　　$w_Q(e) = w_Q(\bar{e})$

定义错误作用群的子集合(对于 $0 \leqslant l \leqslant n$)

$$E_n(l) = \{e \in E_n \mid w_Q(e) \leqslant l\}$$
$$\overline{E}_n(l) = \{\bar{e} \in \overline{E}_n \mid w_Q(\bar{e}) \leqslant l\}$$

则 $E_n(l) = 4 * \sum_{i=0}^{l} 3^i \binom{n}{i}$，$\overline{E}_n(l) = \frac{1}{4}E_n(l)$。(这是由于:从 n 个量子位中取 i 位共有 $\binom{n}{i}$ 种方法,而这 i 位中每位均可能有 3 种错误算子 σ_x，σ_y，σ_z,所以量子权为 i 的 $w_1 \otimes w_2 \otimes \cdots \otimes w_n$ 共有 $3^i \binom{n}{i}$ 个。)

现在看一下量子码 Q 的纠错能力。在经典情形,一个经典纠错码 $C \in F_q^n$ 能纠正 $\leqslant l$ 位错,可以表达成以下形式:

对任何两个不同的码字 c 和 c'(即 c，$c' \in C$，$c \neq c'$)，对任何错误向量 ε、ε'，$w_H(\varepsilon) \leqslant l$，$w_H(\varepsilon') \leqslant l$,均有 $c + \varepsilon \neq c' + \varepsilon'$。

这是因为:在发方将码字 c 传出去,信道发生不超过 l 位错误 ε(即 $w_H(\varepsilon) \leqslant l$),则收方得到 $y = c + \varepsilon$。码字 c 与 y 的距离不超过 l,因为 $d_H(y,\ c) \leqslant w_H(y - c) = w_H(\varepsilon) \leqslant l$。而 y 与 c' ($\neq c$)其他码字的距离均大于 l。若 $d_H(y,\ c') \leqslant l$,令 $\varepsilon' = y - c'$，$w_H(\varepsilon') = d_H(y,\ c') \leqslant l$,但是 $\varepsilon' + c' = y = c + \varepsilon$,与条件相矛盾,于是 c 是与收到向量 y 的 Hamming 距离最近的惟一码字。将 y 译成码字 c 是正确的译码。

现在定义量子码的纠错能力,只需把经典情形的条件稍加改动,即把“不同”码字 ($c' \neq c$) 改成“完全可区分”量子态 ($\langle v_1 \mid v_2\rangle = 0$),把 Hamming 权改成量子权即可。

定义 5.7　设 Q 是码长为 n 的量子码(即 Q 为 C^{2n} 中的一个复向量子空间),称 Q 可以纠正 $\leqslant l$ 位错,是指对任何 $(e,\ e') \in E_n(l)$ 和 $(|\ v\rangle,\ |\ v'\rangle) \in Q$,如果 $\langle v \mid v'\rangle = 0$,则 $\langle v \mid ee' \mid v'\rangle = 0$。(注意 e 和 e' 均为酉线性作用,$\bar{e}^T = e$，$\bar{e}'^T = e'$。可知 $\langle v \mid ee' \mid v'\rangle = 0$,即表示 $e|v\rangle$ 和 $e'|v'\rangle$ 正交,也表示 $|v\rangle$ 和 $ee'|v'\rangle$ 正交(对于厄米特内积)。)

量子码 Q 的最小距离 $d = d(Q)$ 是满足下述性质的最大正整数 d:对于 $|v\rangle$ 和 $|\ v'\rangle \in Q$,如果 $\langle v \mid v'\rangle = 0$,则对每个 $e \in E_n(d-1)$,均有 $\langle v \mid e \mid v'\rangle = 0$。

显然由不等式 $w_H(ee') \leqslant w_H(e) + w_H(e')$，便可得到与经典情形相类似的量子纠错码基本结果:

定理 5.5 最小距离为 d 的量子码 Q 可以纠正$\leqslant\left[\frac{d-1}{2}\right]$个量子位的错。

至此，我们介绍完量子码 Q 的 3 个基本参数：码长 n、维数 K(或用 $k=\log_2 K$)和最小距离 d。我们把这个量子码表示成$((n, K, d))$或者$[[n, k, d]]$。

一个好的量子码要求$\frac{k}{n}$和 d 很大，它们之间也有一些界，并且这些界形式上与经典界有相似之处。

定理 5.6

(1) 若存在量子码 $Q=[[n, k, d]]$，并且

(i) (量子 Hamming 界)Q 是纯量子码，则 $2^{n-k} \geqslant \sum_{i=0}^{\left[\frac{d-1}{2}\right]} 3^i \binom{n}{i}$

(ii) (量子 Singleton 界)若 $d \leqslant \frac{n}{2}-1$，则 $n \geqslant k+2d-2$

(2)(量子 G－V 界) 如果 $2 \mid n-k \geqslant 1$，$1 \leqslant d \leqslant n$，并且 $2^{n-k}-1 \geqslant \sum_{i=0}^{d-1} 3^i \binom{n}{i}$，则存在参数为$[[n, k, d]]$的量子码。

证明：

(1) 量子码 Q 称作纯(pure)的，是指对 $\overline{E}_n(d-1)$ 中元素 $\bar{e} \neq I_2$ 和任意 $|v\rangle$，$|v'\rangle \in Q$，(不必$\langle v \mid v'\rangle = 0$)，均有$\langle v \mid e \mid v'\rangle = 0$。以下构造的 CRSS 量子码多数情形都是纯量子码。对于纯量子码，令 $l=\left[\frac{d-1}{2}\right]$，则 $\overline{E}_n(l)$ 中有 $N=\sum_{i=0}^{l} 3^i \binom{n}{i}$个元素$\{e_i \mid 1 \leqslant i \leqslant N\}$，可以看出 e_iQ $(1 \leqslant i \leqslant N)$ 都是 C^{2^n} 的 2^k 维复向量子空间，并且彼此正交。于是它们的总维数 2^kN 应当不超过 2^k，即 $2^{n-k} \geqslant N$。

(2) 经典纠错编码的 Singleton 界 $(n \geqslant k+d-1)$ 证明很容易，但是量子码的 Singleton 界 $(n \geqslant k+2d-2)$ 的证明较为困难。证明可见题为“Quantum error correction via codes over GF(4)”的论文，1998 年发表在 IEEE Trans. Information Theory, vol. 44, no. 4, pp. 1369—1387，作者为 A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane。以及题为“Quantum Error-Correcting Codes”的论文，2002 年发表在 Coding Theory and Cryptography, Lecture Notes Series 1, Institute for Mathematical Sciences, National University of Singapore, edited by H. Niederreiter, World Scientific, pp. 91—142. 作者是 K. Feng。

(3) 证明见发表在 2005 年 IEEE Trans. Information Theory 的题为“Finite quantum Gilbert-Varshamov bound”论文，作者是 K. Feng and Z. Ma，证明要用到有限域上矩阵群一些精细的计算结果。

定义 5.8　一个量子码 $Q=[[n, k, d]]$ 叫作是 MDS 码，是指它达到量子 Singleton 界，即 $n=k+2d-2$。如果 Q 是纯量子码并且达到量子 Hamming 界，即 $2^{n-k} \geqslant \sum_{i=0}^{\left[\frac{d-1}{2}\right]} 3^i \binom{n}{i}$ 则 Q 叫作是完全量子码。

我们下一节要介绍的[[5, 1, 3]]量子码是纯码，它同时为完全量子码和 MDS 量子码。与经典码情形一样，量子 $G-V$ 界是某些量子码存在的充分性条件。利用这个界，K. Feng 和 Z. Ma 在论文“Finite quantum Gilbert-Varshamov bound”中给出了一些量子码的存在性，其参数改进了前人的结果。

5.1.6　CRSS 量子码构建的数学描述

本节介绍 Calderbank, Rains, Shor 和 Sloane 在 1998 年给出的一种构造量子码的系统方法，他们的结果如下：

定理 5.7　(CRSS, 1998)设 C 是 F_2^{2n} 中的辛自交线性码(即 C 为 F_2^{2n} 的线性子空间并且 $C \subseteq (C)_s^{\perp}$)，$\dim C=n-k$ $(0 \leqslant k \leqslant n)$，则存在参数[[n, k, d]]的量子码，其中

$$d \geqslant \min\{w_Q(c) \mid c \in (C)_s^{\perp} \backslash C\}$$

证明思路：证明利用了有限交换群的表示理论，即特征标理论。首先，由于 $\dim C \leqslant \dim(C)_s^{\perp} (=2n-\dim C)$，可知 $0 \leqslant \dim C \leqslant n$。于是，$\dim C=n-k$，其中 $0 \leqslant k \leqslant n$。将 C 看成是 $\overline{E}_n(F_2^{2n})$ 的子群。由于 C 是辛自正交的，根据定理 5.4，C 可以提升成 E_H 的一个交换子群 G，即存在 E_H 的一个 $2^{n-k}=|C|$ 阶交换子群 G，使得 $\overline{G}=C$。现在考虑子群 G 在 $V=(C^2)^{\otimes n}=C^{2n}$ 上的作用。由于 G 是交换群，根据线性代数，G 中元素的作用方阵可以同时对角化。换句话说，V 可以分解成一些线性子空间的直和，每个子空间都是 G 的公共本征子空间。这件事用表示理论可以具体表示出来(G 给出在 V 上的表示是完全可约的)：

$$V=\bigotimes_{\chi \in \hat{G}} V(\chi) \text{ (直和)}$$

其中 $\hat{G}$ 是 G 的特征标群。并且对每个特征标 $\chi \in \hat{G}$，

$$V(\chi)=\{|\varphi\rangle \in V : e|\varphi\rangle=\chi(e)|\varphi\rangle,\ \forall e \in G\}$$

即 $V(\chi)$ 是 G 的公共本征子空间，e 在 $V(\chi)$ 上的本征值为 $\chi(e)(\pm 1)$。我们要证

明对每个 $\chi \in \hat{G}$，子空间 $V(\chi)$都是参数为$[[n, k, d]]$的量子码。

考虑 $2^{n-k} = |\hat{G}| = |G| = |C|$ 个本征子空间$\{V(\chi) \mid \chi \in \hat{G}\}$ 所构成的集合 M，可以证明 E_n 中每个元素 e 把每个 $V(\chi)$变成 $V(\chi')$，即对每个 $e \in E_n$，e 都是集合 M 的一个置换。还可证明 E_n 在 M 上的作用是传递的，即对任何 $V(\chi)$和 $V(\chi')$，均存在 $e \in E_n$，使得 $e(V(\chi)) = V(\chi')$，于是 $\dim V(\chi) = \dim V(\chi')$。这表明 2^{n-k}个 $V(\chi)(\chi \in \hat{G})$有相同的维数。由于它们的直和为 V，$\dim V = 2^n$，可知对每个 $\chi \in \hat{G}$，$V(\chi)$ 的维数均为 $K = 2^k$。

令 $d' = \min\{w_Q(c) \mid c \in (C)_s^{\perp} \backslash C\} = \min\{w_Q(c) \mid c \in (C)_s^{\perp}, c \notin C\}$。我们只需再证对每个 $Q = V(\chi)$，Q的最小距离 $d \geqslant d'$。根据定义，只需证：若$|v\rangle$，$|v'\rangle \in V(\chi)$，$\langle v \mid v' \rangle = 0$，$e \in E_n(d'-1)$，则$\langle v \mid e \mid v' \rangle = 0$。证明分两种情况：

(1) 若 $\bar{e} \in \bar{G} = C$，由 $|v'\rangle \in V(\chi)$ 和 $e \in G$ 可知，$e|v'\rangle = \chi(e)|v'\rangle$，于是$\langle v \mid e \mid v' \rangle = \chi(e)\langle v \mid v' \rangle = 0$。

(2) 若 $\bar{e} \notin \bar{G} = C$，由 d'的定义可知$(C)_s^{\perp} \backslash C$ 与 $\bar{E}_n(d'-1)$不相交，从而由 $\bar{e} \notin C$和$\bar{e} \in \bar{E}_n(d'-1)$ 可推出 $\bar{e} \notin (C)_s^{\perp}$。这表明 $\bar{e}$ 和C 中某个向量不是辛自正交的，所以 e 与G 中某个元素 g 不可交换(定理 5.4)，即 $eg = -ge$。于是，对于 $|v'\rangle \in V(\chi)$，

$$eg|v'\rangle = -ge|v'\rangle - \chi(g)e|v'\rangle \neq \chi(g)e|v'\rangle$$

这表明 $e|v'\rangle \notin V(\chi)$。但是 e 把 $V(\chi)$映射成某个 $V(\chi')$，于是 $e|v'\rangle \in V(\chi')$，其中 $\chi \neq \chi'$。但是 $\chi \neq \chi'$ 时，$V(\chi)$ 和 $V(\chi')$ 正交。由于 $|v\rangle \in V(\chi)$，$e|v'\rangle \in V(\chi')$，于是$\langle v \mid e \mid v' \rangle = 0$。这就证明了定理。

现在对这个定理做一些评注。

注记 1　这个定理的证明是构造性的。由辛自正交二元线性码 $C \subseteq F_2^{2n}$ 给出构造量子码 $Q = V(\chi)$ 的具体方法。由 $V(\chi)$的构造方式，可以给出纠错译码的方法。

发方将 $|v\rangle \in Q$给出，收方得到 $|u\rangle = e|v\rangle$，其中 $e \in E_n(l)$。我们假定错位不超过$\left[\frac{d'-1}{2}\right]$个，即 $l = \left[\frac{d'-1}{2}\right]$ $(w_Q(e) \leqslant l)$。

第一步：由定理证明知 $|u\rangle = e|v\rangle$ 必属于某个 $V(\chi')$，$\chi' \in \hat{G}$。首先决定特征标 χ'，这可利用 G 在收到向量$|u\rangle$上的作用：对每个 $g \in G$，由 $|u\rangle \in V(\chi')$可知，$g|u\rangle = \chi'(g)|u\rangle$。另一方面，

$$g|u\rangle = ge|v\rangle = (-1)^{(\bar{g},\bar{e})_s} eg|v\rangle = (-1)^{(\bar{g},\bar{e})_s} \chi(g)e|v\rangle$$

$$= (-1)^{(\bar{g},\bar{e})_s}\chi(g) \mid u\rangle$$

因此，$\chi'(g) = \chi(g)(-1)^{(\bar{g},\bar{e})_s}$(对每个 $g \in G$)，由此可决定 χ'。

第二步：如果 $\chi = \chi'$，则由上式知 $(-1)^{(\bar{g},\bar{e})_s} = 1$，即 $(\bar{g},\bar{e})_s = 0$(对每个 $\bar{g} \in \bar{G} = C$)。这表明 $\bar{e} \in (C)_s^{\perp}$。但是，由 $w_Q(\bar{e}) \leqslant l \leqslant d' - 1$ 和 d' 的定义，可知 $\bar{e} \in C = \bar{G}$，因此 $e \in G$。于是 $\mid u\rangle = e \mid v\rangle = \chi(g) \mid v\rangle$。所以，当 $\chi = \chi'$ 时，$\mid u\rangle$即为发出的码字$\mid v\rangle$(相当一个非零因子 $\chi(g) = \pm 1$)。

如果 $\chi \neq \chi'$，对于 e 和 e'，可以证明：

e 和 e'把 $Q = V(\chi)$ 映射成同一个 $V(\chi') \Leftrightarrow e$ 和 e'属于 F_2^{2n} 对 $(C)_s^{\perp}$ 的一个陪集。

由于 $\mid F_2^{2n}/(C)_s^{\perp} \mid = \mid C \mid = 2^{n-k}$，可以取 E_n 中 2^{n-k}个元素 $\{e_1, \cdots, e_t\}$ $(t = 2^{n-k})$，使得 $\bar{e}_i (1 \leqslant i \leqslant t)$ 分别在对 $(C)_s^{\perp}$ 的不同陪集之中。这时 $e_i Q$ $(1 \leqslant i \leqslant t)$ 恰好是 2^{n-k}个不同的子空间 $Q(\chi)$ $(\chi \in \hat{G})$。我们取$\bar{e}_i$ 为所在陪集中量子权最小者。

现在 $e(Q) = e(V(\chi)) = V(\chi')$。则有惟一的 i $(1 \leqslant i \leqslant t)$，使 $e(Q) = V(\chi')$。于是 $e_i^{-1}e$ 将 $Q = V(\chi)$ 变成自身，所以 $\bar{e} - \bar{e}_i \in (C)_s^{\perp}$，即 $\bar{e}$ 和 $\bar{e}_i$ 属于 F_2^{2n} 对 $(C)_s^{\perp}$ 的同一陪集。由于 $w_Q(\bar{e}) \leqslant l$，而$\bar{e}_i$ 在 $\bar{e}$ 的陪集中是量子权最小者，从而 $w_Q(\bar{e}_i) \leqslant w_Q(\bar{e}) \leqslant l$。所以 $w_Q(\bar{e} - \bar{e}_i) \leqslant w_Q(\bar{e}) + w_Q(\bar{e}_i) \leqslant 2l \leqslant d' - 1$。但是 $\bar{e} - \bar{e}_i \in (C)_s^{\perp}$，而 $(C)_s^{\perp} \backslash C$ 和 $\bar{E}_n(d' - 1)$ 不相交，于是 $\bar{e} - \bar{e}_i \in C$，即 $e_i^{-1}e \in G$，这表明 $e_i^{-1} \mid u\rangle = e_i^{-1}e \mid v\rangle = \chi(e_i^{-1}e) \mid v\rangle$，所以用 e_i^{-1} 作用收到的向量$\mid u\rangle$，就给出正确的发出码字$\mid v\rangle$。

注记 2　在经典情形，若信道中产生错误，即 $\varepsilon \in F_q^n$，$e \neq 0$，则 ε 对发出的信息 $c \in C$ 一定产生影响，因为 $c + \varepsilon \neq c$。但是在量子情形，即使 e 有错误作用 $(w_Q(e) \geqslant 1)$，如果 $\bar{e} \in \bar{G} = C$ 时，它对发出信息 $\mid v\rangle \in Q = V(\chi)$ 的作用为 $e \mid v\rangle = \chi(e) \mid v\rangle$，收到 $\chi(e)\mid v\rangle$和发出的$\mid v\rangle$是同一物理状态，也就是说，错误作用可以对发出信息不产生影响。

根据定义，$Q = V(\chi)$ 的最小距离 $d \geqslant d'$，其中 d'是集合 $(C)_s^{\perp} \backslash C$ 中向量的最小量子权。如果 $(C)_s^{\perp}$ 中有量子权$\leqslant d' - 1$ 的向量，它必属于 C。换句话说，如果 C 中每个非零向量的量子权均$\geqslant d'$，则 $(C)_s^{\perp}$ 中每个非零向量也$\geqslant d'$。这时，若 $e \in E_n$，$1 \leqslant w_Q(e) \leqslant d' - 1$，则 $\bar{e} \notin (C)_s^{\perp}$。所以，对任意 $\mid v\rangle$ 和 $\mid v'\rangle$，$\mid v\rangle \in Q$，$\mid v'\rangle \in Q$，$Q = V(\chi)$，$e \mid v'\rangle \in V(\chi')$，其中 $\chi' \neq \chi$，于是 $\mid v\rangle$ 和$e \mid v'\rangle$正交，即$\langle v \mid e \mid v'\rangle = 0$(无论 $Q = V(\chi)$ 中的$\mid v\rangle$和$\mid v'\rangle$是否正交)。综合上述可知：若 C 中每个非零向量的量子权均$\geqslant d'$，则 $Q = V(\chi)$ 是纯量子码。特别地，它应该满足量子 Hamming 界。

现在举一些例子。

例 5.4 考虑 F_2^{10} 中以

$$M=\begin{bmatrix}u_1\\u_2\\u_3\\u_4\end{bmatrix}=\left[\begin{array}{ccccc|ccccc}1&1&0&0&0&0&0&1&0&1\\0&1&1&0&0&1&0&0&1&0\\0&0&1&1&0&0&1&0&0&1\\0&0&0&1&1&1&0&1&0&0\end{array}\right]$$

为生成矩阵的二元线性码，则 $n=5$，而 $n-k=\dim C=4$，于是 $k=1$。C 是辛自正交码，这只需验证 C 的基向量 $u_i=\langle a_i\mid b_i\rangle$ $(1\leqslant i\leqslant 4)$ 彼此是辛自正交的。注意，每个向量 $u=\langle a\mid b\rangle$ $(a,b\in F_2^n)$ 与自身都是辛正交的，因为 $(u,u)_s=a\cdot b+a\cdot b=0$。又如，$u_1=\langle 11000\mid 00101\rangle=\langle a_1\mid b_1\rangle$ 和 $u_2=\langle a_2\mid b_2\rangle=\langle 01100\mid 10010\rangle$ 的辛内积为

$$(u,u)_s=a_1\cdot b_2+a_2\cdot b_1=1+1=0$$

进而决定 C 的辛对偶码 $(C)_s^{\perp}$。由于 $C\subseteq(C)_s^{\perp}$ 并且 $\dim(C)_s^{\perp}=10-\dim C=6$，所以需要在 $\{u_1,u_2,u_3,u_4\}$ 中再加入两个向量构成 $(C)_s^{\perp}$ 的一组基。直接验证 $u_5=\langle 11111\mid 00000\rangle$ 及 $u_6=\langle 00000\mid 11111\rangle$ 均和 $u_i(1\leqslant i\leqslant 4)$ 辛正交，于是 $(u_5,u_6)\in(C)_s^{\perp}$。再由 $u_i(1\leqslant i\leqslant 6)$ 线性无关，所以它们形成 $(C)_s^{\perp}$ 的一组基，即

$$(C)_s^{\perp}=C\oplus F_2\langle 11111\mid 00000\rangle\oplus F_2\langle 00000\mid 11111\rangle$$

可以验证 C 中非零向量的量子权均$\geqslant 4$，$(C)_s^{\perp}$ 中非零向量的量子权均$\geqslant 3$，并且 $(C)_s^{\perp}$ 中存在量子权为 3 的向量，例如 $v=\langle 00111\mid 00101\rangle=u_1+u_6\in(C)_s^{\perp}$，而 $w_Q(v)=3$，从而 $Q=V(\chi)$ 是参数 $[[n,k,d]]=[[5,1,3]]$ 的纯量子码。由于

$$\sum_{i=0}^{1}3^i\binom{n}{i}=1+3\cdot 5=16=2^{n-k}$$

可知这是完全量子码。这是 Calderbank 和 Shor 等人作出的第一个完全量子码。

取 χ 为平凡特征标 1 为例，具体写出量子码

$$Q=V(1)=\{\mid v\rangle\in C^{32}:\forall\ \bar{e}\in C,\ e\mid v\rangle=\mid v\rangle\}$$

将 C 的生成阵 M 中基向量 $u_i=\langle a_i\mid b_i\rangle$ $(1\leqslant i\leqslant 4)$，提升成 $e_i=X(a_i)Z(b_i)$，由于 $\{e_i\mid 1\leqslant i\leqslant 4\}$ 生成 E_n 的 16 阶交换子群

$$G=\{e_1^{i_1}e_2^{i_2}e_3^{i_3}e_4^{i_4}\mid i_1i_2i_3i_4\in\{0,1\}\}\ (e_i^2=1,\ e_ie_j=e_je_i)$$

$Q=\{|v\rangle\in C^{32}$:对每个 $g\in G$, $g|v\rangle=|v\rangle\}$ 应该为 $K=2^k=2$ 维复向量子空间。对每个 $|v\rangle\in C^{32}$, $|u\rangle=\sum_{g\in G}g|v\rangle$ 属于 Q,因为当 $g\in G$ 时

$$g|u\rangle=g\Big(\sum_{h\in G}h|v\rangle\Big)=\sum_{h\in G}gh|v\rangle=\sum_{s\in G}s|v\rangle=|u\rangle$$

于是,量子码 Q 有以下的$|u_1\rangle$和$|u_2\rangle$为基,其中

$$\begin{aligned}|u_1\rangle&=\sum_{g\in G}g|00000\rangle\\&=|00000\rangle+(|11000\rangle+|01100\rangle+|00110\rangle+|00011\rangle+|10001\rangle)\\&\quad-(|10100\rangle+|01010\rangle+|00101\rangle+|10010\rangle+|01001\rangle)\\&\quad-(|11110\rangle+|01111\rangle+|10111\rangle+|11011\rangle+|11101\rangle)\\|u_2\rangle&=\sum_{g\in G}g|11111\rangle\\&=|11111\rangle+(|00111\rangle+|10011\rangle+|11001\rangle+|11100\rangle+|01110\rangle)\\&\quad-(|01011\rangle+|10101\rangle+|11010\rangle+|01101\rangle+|10110\rangle)\\&\quad-(|00001\rangle+|10000\rangle+|01000\rangle+|00100\rangle+|00010\rangle)\end{aligned}$$

这个码 Q 是 C^{32} 中一个二维复子空间,它可以纠正 5 个量子位当中任何一个出现的错误,而错误可以是 σ_x、σ_y、σ_z 当中任何一种。

例 5.5　考虑 $F_2^{16}(n=8)$ 中以

$$G=\left[\begin{array}{cccccccc|cccccccc}0&0&1&1&1&0&1&0&1&0&0&1&1&1&0&0\\1&0&0&1&1&1&0&0&0&1&0&0&1&1&1&0\\0&1&0&0&1&1&1&0&1&0&1&0&0&1&1&0\\1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\end{array}\right]$$

为生成矩阵的二元线性码 C,是辛自正交码,$n-k=\dim C=5$,从而 $k=n-5=3$。$(C)_s^{\perp}$ 中有量子权为 3 的向量$\langle 11000000|01100000\rangle$,没有量子权小于等于 2 的非零向量,于是得到纯量子码$[[8,3,3]]$。这也是好的量子码,因为由 Singleton 界知,不存在量子码$[[8,3,4]]$,由 Hamming 界知不存在纯量子码$[[8,4,3]]$和$[[7,3,3]]$。

定理 5.7 有许多推论。利用这些推论,在用经典二元线性码 C 构作量子码时,不需要辛内积和量子权,只需要 F_q^n 上的通常内积和 Hamming 权,从而使用起来更为方便。

定理 5.8 如果存在参数为$[n, k, d]$的二元线性码 C,并且 $C \supset C^{\perp}$，这里 $C^{\perp}$是经典纠错码中 C 对于通常内积 $(u, v) = \sum_{i=1}^{n} u_i v_i$ 的对偶码。则存在参数为$[[n, 2k-n, d]]$的纯量子码。

证明：考虑 F_2^{2n} 中的线性码

$$S = \{\langle v_1 \mid v_2 \rangle \in F_2^{2n} \mid v_1, v_2 \in C^{\perp}\} = C^{\perp} \oplus C^{\perp}$$

则

$$\dim S = 2\dim C^{\perp} = 2(n-k)$$

由于

$$(S)_s^{\perp} = C \oplus C \supset C^{\perp} \oplus C^{\perp} = S$$

可知，S 是辛自正交码。由定理 5.7 给出量子码$[[n, k', d']]$,其中：

$$k' = n - \dim S = n - 2(n-k) = 2k - n(\text{由 } C \supset C^{\perp} \text{ 可知 } 2k \leqslant n)$$

$$d' = \min\{w_H(c) \mid c \in (S)_s^{\perp} \backslash S\} = \min\{w_H(c) \mid c \in C \backslash C^{\perp}\} \geqslant d$$

由于线性码 $C^{\perp}$的最小距离大于等于 d,所以得到的是纯量子码。

定理 5.9 如果存在二元线性码 C_1 和 C_2，参数分别为$[n, k_1, d_1]$和$[n, k_2, d_2]$,并且 $C_1^{\perp} \subseteq C_2$(于是 $n-k_1 \leqslant k_2$,即 $n \leqslant k_1 + k_2$)，则存在参数为$[[n, k_1 + k_2 - n, \min\{d_1, d_2\}]]$ 的量子码。

证明：以 G_i 和 H_i 分别表示二元线性码 C_i 的生成矩阵和校验矩阵 $(i = 1, 2)$。考虑以

$$G = \begin{bmatrix} \overset{n}{H_1} & \overset{n}{0} \\ 0 & H_2 \end{bmatrix} \begin{matrix} n-k_1 \\ n-k_2 \end{matrix}$$

为生成矩阵的 F_2^{2n} 中二元线性码 C,码长为 $2n$，$\dim C = n - k_1 + n - k_2 = 2n - k_1 - k_2$。由 $C_1^{\perp} \subseteq C_2$ 可知 $H_1 H_2^T = 0$，$(C)_s^{\perp} = C^{\perp}$，并且 $C^{\perp}$的校验矩阵和生成矩阵分别为

$$\begin{bmatrix} H_1 & 0 \\ 0 & H_2 \end{bmatrix} \text{和} \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}$$

由此可知 $C \subseteq (C)_s^{\perp}$。根据定理 5.7 得到参数为$[[n, k', d']]$的量子码。其中：

$$k' = n - \dim C = k_1 - k_2 - n$$

$$d' = \min\{w_Q(c) \mid c \in (C)_s^{\perp} \backslash C\} \geqslant \min\{w_Q(c) \mid c \in (C)_s^{\perp}\} = \min\{d_1, d_2\}$$

Steane 采用更为精确的技巧，将定理 5.9 作如下的改进。

定理 5.10　设 C 和 C' 分别是参数 $[n, k, d]$ 和 $[n, k', d']$ 的二元线性码，并且 $C^{\perp} \subseteq C \subseteq C'$（于是 $k' \geqslant k \geqslant n-k$）。如果 $k' \geqslant k+2$，则存在参数 $\left[\left[n, k+k'-n, \min\left\{d, \frac{3}{2}d'\right\}\right]\right]$ 的量子码。

上述 4 个定理建立了经典二元线性码和量子码之间的联系。从 1999 年起，借助于经典二元线性码的已知成果（Reed-Muller 码，Hamming 码，Reed-Solomon 码，BCH 码，代数几何码……）构作出丰富的量子纠错码。

5.2　经典纠错编码的基础

作为经典纠错编码的基本知识，首先介绍关于环 F_2 上的矢量与符号。根据 5.1 节的介绍，在 $\{0, 1\}$ 两个元素组成的集合之上实现加法运算和乘法运算的代数系统被称为环 F_2。

$$0+0=0 \quad 1+0=1 \quad 0+1=1 \quad 1+1=0$$
$$0*0=0 \quad 1*0=1 \quad 0*1=1 \quad 1*1=1$$

在环 F_2 上对 0 和 1 实施如上所示的通常的整数和与整数积的运算，得到的结果除以 2 取余，即所谓的模 2 运算。

环 F_2 上的长度为 n 的矢量 $\boldsymbol{v}=(v_1, v_2, \cdots, v_n)$ 是各分量元素取 0 或 1 的长度为 n 的矢量。矢量 $\boldsymbol{v}$ 里包含的 1 的个数称为矢量 $\boldsymbol{v}$ 的 Hamming 权重，用 $w_{\mathrm{H}}(v)$ 表示。例如有矢量

$$v=(111001)$$

则 $w_{\mathrm{H}}(v)=4$。

两个矢量 $\boldsymbol{v}$ 和 $\boldsymbol{\omega}$ 之间的 Hamming 距离由 $d_{\mathrm{H}}(v, \omega)$ 决定

$$d_{\mathrm{H}}(v, \omega)=w_H(v+\omega)$$

这里矢量 $\boldsymbol{v}+\boldsymbol{\omega}$ 的各分量元素用矢量 $\boldsymbol{v}$ 与 $\boldsymbol{\omega}$ 的各分量元素（在环 F_2 上）的和表示。例如有矢量 $\boldsymbol{v}$ 和 $\boldsymbol{\omega}$

$$v=(111001)、\omega=(100010)$$

则

$$v+\omega=(011011)$$

此时 $d_{\mathrm{H}}(v, \omega)=4$。

长度为 n 的二元($\{0, 1\}$)代码集合 C 被定义为 F_2 上长度为 n 的矢量集合(码书)。代码集合 C 的元素称为代码。特别地,对于二元代码集合 C 的任意两个代码 υ 和 ω,如果总有 $\upsilon+\omega \in C$ 的话,则称 C 为线性代码集合。

代码集合 C 的最小距离 $d(C)$ 被定义为集合上不同代码间的 Hamming 距离的最小值。特别是线性代码集合 C 的最小距离 $d(C)$ 与非零代码的 Hamming 权重的最小值是一致的。

用 F_2 上长度为 k 的矢量表示由 k 个 bit 的信息编制成长度为 n ($n \geqslant k$) 的代码,代码的全体构成线性代码集合 $C(|C|=2^k)$, C 具有被称为是 F_2 上的 $k\times n$ 生成矩阵 G 的全部特征。如果使用生成矩阵 G,则长度为 k bit 的信息系列:

$$(x_1, x_2, \cdots, x_k),\ x_i \in \{0, 1\},\ i = 1, 2, \cdots, k$$

能够表示成如下的代码:

$$\upsilon = (x_1, x_2, \cdots, x_k)G_{k\times n}$$

特别是,如果用 k 个行矢量 $g_1, g_2, \cdots, g_k$ 表示线性代码集合 C 的生成矩阵 G,即

$$G_{k\times n} = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{bmatrix}$$

则对应信息 $(x_1, x_2, \cdots, x_k)$ 的代码 υ 将表示成为

$$\upsilon = (x_1, x_2, \cdots, x_k)G_{k\times n} = x_1 g_1 + x_2 g_2 + \cdots x_k g_k$$

由此可得知代码 υ 是 $g_1, g_2, \cdots, g_k$ 的线性组合。行矢量 $g_1, g_2, \cdots, g_k$ 的一次性线性独立的最大个数用 $\dim(C)$ 表示, $\dim(C)$ 也是线性代码集合 C 的维数。

例题 5.6 考虑由生成矩阵 G

$$G = [1 \quad 1 \quad 1]$$

决定的线性代码集。此时因为生成矩阵 G 是 1×3 的矩阵,则长度 k 为 1 bit 的信息将变换成长度 n 为 3 bit 的代码。这个代码集合中的代码是由下式决定的 (0 0 0)和(1 1 1)两个代码组成

$$(0)G = (0 \quad 0 \quad 0) \qquad (1)G = (1 \quad 1 \quad 1)$$

再来考虑由以下稍许复杂一些的生成矩阵 G 决定的线性代码集。

$$G=\begin{bmatrix}0 & 1 & 1 & 1\\ 1 & 0 & 1 & 0\end{bmatrix}$$

此时因为生成矩阵 G 是 2×4 的矩阵，则 k 为 2 bit 的信息将变换成长度 n 为 4 bit 的代码。在这个代码集中如果考虑希望发送的两位信息是(0　0)，(0　1)，(1　0)，(1　1)，则代码集合由以下 4 个代码组成：

$$\begin{aligned}&(0\quad 0)G=(0\quad 0\quad 0\quad 0)\\ &(0\quad 1)G=(1\quad 0\quad 1\quad 0)\\ &(1\quad 0)G=(0\quad 1\quad 1\quad 1)\\ &(1\quad 1)G=(1\quad 1\quad 0\quad 1)\end{aligned}$$

环 F_2 上的 n 维矢量 $\upsilon=(\upsilon_1,\upsilon_2,\cdots,\upsilon_n)$ 和 $\omega=(w_1,w_2,\cdots,w_n)$ 的内积 $\upsilon\cdot\omega$ 被定义为

$$\upsilon\cdot\omega=\upsilon_1w_1+\upsilon_2w_2+\cdots+\upsilon_nw_n \tag{5.5}$$

其中等式右边的和与积是 F_2 上的两个运算。当 $\upsilon\cdot\omega=0$ 时，称两个矢量 υ 和 ω 直交。

与线性代码集合 C 中所有代码直交的矢量全体组成的集合称为 C 的对偶代码集合，用记号 $C^{\perp}$ 表示，此时 $C^{\perp}$ 也是线性代码集。因为，如有 ω_1 和 ω_2 是 $C^{\perp}$ 中的代码，则对任意的 $\upsilon\in C$，以下等式成立：

$$\upsilon\cdot(\omega_1+\omega_2)=\upsilon\cdot\omega_1+\upsilon\cdot\omega_2=0+0=0$$

即 $\omega_1+\omega_2$ 也与线性代码集合 C 的所有代码直交，所以 $\omega_1+\omega_2\in C^{\perp}$。

由线性代数学基础知识我们知道长度为 n 的线性代码集合 C 与其对偶代码集合 $C^{\perp}$ 的维数之间的关系满足下式：

$$\dim(C)+\dim(C^{\perp})=n \tag{5.6}$$

以下将长度为 n、维数为 k 的线性代码集合记为$[n,k]$。由式(5.6)得知线性代码集合$[n,k]$的对偶代码集合应记为$[n,n-k]$。

线性代码集合 C 的对偶代码集合 $C^{\perp}$ 被称为是 C 的奇偶校验矩阵或简称为校验矩阵，$[n,k]$线性代码集合的奇偶校验矩阵是 $(n-k)\times n$ 矩阵。假设代码集合 C 的奇偶校验矩阵为 H，则从定义我们可以直接得到代码集合 C 的所有代码 υ 一定满足以下等式：

$$\upsilon H^{T}=0$$

此处 H^T 表示矩阵 H 的转置。反之，由近代代数的基础知识很容易知道：满足上列等式的所有二元矢量必定与代码集合 C 一致。

例题 5.7 考虑由生成矩阵 $G=[1\quad 1\quad 1]$ 定义的[3，1]线性代码集合的奇偶校验矩阵。首先考虑与惟一非零编码(1 1 1)直交的矢量有 4 个：(1 0 1)，(0 1 1)，(1 1 0)，(0 0 0)，且这 4 个矢量都可以用(1 0 1)和(1 1 0)线性表示。所以对偶代码集合的生成矩阵为

$$H=\begin{bmatrix}1 & 1 & 0\\ 1 & 0 & 1\end{bmatrix}$$

该矩阵就是所要求的奇偶校验矩阵。很显然，$(1\quad 1\quad 1)H^T=0$ 成立。

一般情况下，根据矩阵的基本变换规律，线性代码集合 C 的生成矩阵一定可以写成下列形式：

$$G=[I_k\quad P]$$

此处 I_k 表示 $k\times k$ 的单位矩阵，P 表示 $k\times(n-k)$ 矩阵。此时，代码集合 C 的奇偶校验矩阵可由下列等式给出：

$$H=[P^T I_{n-k}]$$

此处 P^T 表示 P 的转置，I_{n-k} 表示 $(n-k)\times(n-k)$ 的单位矩阵。

可以利用奇偶校验矩阵来纠正线性代码的错误。现在使用生成矩阵 G 的 $[n,k]$线性代码集合，假设信息 $x=(x_1,x_2,\cdots,x_k)$ 借助生成矩阵 G 转换成代码 $\upsilon=xG$。将 υ 通过信道传送，再加上 F_2 上长度为 n 的表示错误矢量的 e，则接收方收到的信息可表示成为

$$y=\upsilon+e$$

此处“+”表示各元素在 F_2 上的模 2 加法运算。假设用 H 表示该线性代码集合的奇偶校验矩阵，因为关于代码 υ 的等式 $\upsilon H^T=0$ 一定成立，能够得到下列等式：

$$yH^T=(\upsilon+e)H^T=\upsilon H^T+eH^T=eH^T$$

显然，决定 yH^T 的仅仅是错误矢量的 e 而与发送信息的代码 υ 无关。我们称 yH^T 为伴随式。伴随式中仅包含错误矢量 e 的信息，如果能够很好地利用伴随式，就有可能推断出通过信道传送过来的 υ。

下面用一个例子描述用伴随式订正错误的方法。考虑具有下列奇偶校验矩阵 H 被称为是[7，4] Hamming(汉明)码的编码集合

$$H=\begin{bmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{bmatrix} \tag{5.7}$$

如果没有发生错误，则从 $e=0$ 直接得到伴随式是

$$yH^T=eH^T=0$$

另一方面，如果第 j 位 bit 上发生错误，则使用 e_j 表示第 j 位 bit 为 1、其他 bit 位上全为 0 的矢量，就能够得到

$$yH^T=e_jH^T=(H\text{ 的第 }j\text{ 位的列矢量})^T$$

这里因为奇偶校验矩阵 H 的所有列矢量都各不相同，因此错误矢量 $e_1\sim e_7$ 上对应着不同的伴随式。从具体的结果可以获得以下的错误位置与伴随式的对应关系：

错误发生的位置		伴随式
没有错误	→	(0　0　0)
第一位 bit	→	(0　0　1)
第二位 bit	→	(0　1　0)
第三位 bit	→	(0　1　1)
第四位 bit	→	(1　0　0)
第五位 bit	→	(1　0　1)
第六位 bit	→	(1　1　0)
第七位 bit	→	(1　1　1)

由以上结果知，编码的 7 位 bit 中无论哪一位 bit 上发生错误，都可以通过伴随式准确地知道错误发生的位置，然后对错误位置上的 bit 状态值的 1 和 0 实施反转操作，就能够获得通过信道传送过来的正确代码。

例题 5.8　[7，4] Hamming 编码的代码集合 C 为

$$\begin{aligned}C=\{&(0000000),(1110000),(1001100),(0101010),\\&(1101001),(0111100),(1011010),(0011001),\\&(1100110),(0100101),(0010110),(1010101),\\&(0110011),(0001111),(1000011),(1111111)\}\end{aligned} \tag{5.8}$$

例如编码(1111111)，因为满足下列等式所以是 Hamming 码。

$$(1111111)H^T=(000)$$

进一步假设将(1111111)送入信道，接收到的代码是(1011111)，试着使用伴随式来纠正代码发生的错误。伴随式结果为

$$(1011111)H^T = (1011111)\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = (010)$$

此时我们知道错误发生在第 2 位上，因此可以确定发送信息的代码是

$$(1011111) + (0100000) = (1111111)$$

但是，如果发送同样的信息代码(1111111)，而接收到的代码却是(1011110)，即第 2 位和第 7 位同时发生错误，此时再用伴随式来纠正代码发生的错误，结果会是如何呢？伴随式结果为

$$(1011111)H^T = (1011110)\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = (101)$$

此时，根据结果可以判断错误是发生在第 5 位上，与实际错误发生的位置不符。因此，我们知道[7，4]Hamming 编码对于 7 位 bit 中有两位以上的 bit 发生错误时是无法获得正确的发送信息代码的。

5.3 CSS 编码的构成方法

CSS 编码有时也称 CRSS 编码。CSS 编码于 1996 年由 Calderbank、Shor 两人与 Stoane 独立发现，CSS 编码问世数月后，Calderbank、Rains、Shor、Stoane 4 人又在 1998 年共同提出了 Stabilizer 编码，即 CRSS 编码。Stabilizer 编码是 CSS 编码的一般化，也是到目前为止所有量子编码代数构成方法提案中

最广泛引人注目的方法之一。CSS 编码是基于经典纠错编码方法体系的量子纠错编码的构成方法。CSS 编码是由 2 个经典纠错编码构成的能够纠正 t 位为止的量子纠错编码，它能够同时订正 t 位为止的 bit 反转错误以及 t 位为止的位相翻转错误。一般用$[[n, k]]$表示由 k 个 qubit 组成的信源编码序列转换成由 n 个 qubit 组成的信道编码序列(即量子纠错编码)的量子编码集合。

现在假设有 2 个经典纠错编码集合：$[n, k_1]$线性编码集合 C_1 和$[n, k_2]$线性编码集合 C_2，它们满足以下两个条件：

(1) $C_2 \subset C_1$

(2) $d(C_1) \geqslant 2t+1$, $d(C_2^{\perp}) \geqslant 2t+1$

条件(1)表示 C_2 的全体代码包含在 C_1 代码集合中，条件(2)分别表示 C_1 和 C_2 的对偶代码集合同时都能订正 t 个为止错误。CSS 编码就是由这些代码集合构成的，它是能够订正 t 个以下 qubit 上发生错误的量子编码集合$[[n, k_1-k_2]]$。

首先，对于代码集合 C_1 中的任意代码 $x \in C_1$，其量子状态 $|x+C_2\rangle$ 由下式定义

$$|x+C_2\rangle = \frac{1}{2^{k_2/2}} \sum_{y \in C_2} |x+y\rangle \tag{5.9}$$

其中等式(5.9)右边之和满足定义在 F_2 上的模 2 计算。此时量子状态 $|x+C_2\rangle$ 具有下列性质：

性质 1　如果 C_1 中代码 x'满足条件 $(x+x') \in C_2$，则下列等式成立：

$$|x'+C_2\rangle = |x+C_2\rangle$$

因为假定存在一个 $y' \in C_2$ 满足等式 $y' = x+x'$，此时因为 C_2 是线性的，因此有集合 $\{y+y' : y \in C_2\}$ 与代码集合 C_2 一致。由此能够得到下列的等式成立：

$$\{x+y : y \in C_2\} = \{x+y+y' : y \in C_2\} = \{x'+y : y \in C_2\}$$

考察等式的两端与出现在等式(5.9)右边的和，就知道该等式表示的 $|x+C_2\rangle$ 与 $|x'+C_2\rangle$ 相等。

性质 2　如果 $(x+x') \notin C_2$，则状态 $|x+C_2\rangle$ 与 $|x'+C_2\rangle$ 直交。也就是说下列等式成立：

$$\langle x'+C_2 \mid x+C_2\rangle = 0$$

显然要想证明这个结论，只要证明下式成立即可：

$$\{x+y : y \in C_2\} \cap \{x'+y : y \in C_2\} = \varnothing \tag{5.10}$$

如果式(5.10)成立，则 $|x+C_2\rangle$ 与 $|x'+C_2\rangle$ 不含有同一的基底状态，那么直交的结论就十分自然。以下由悖理法论证：如果有 $x+x' \notin C_2$，则式(5.6)一定成立。即：首先有条件 $x+x' \notin C_2$，但式(5.6)不成立，此时一定存在 $(y, y') \in C_2$ 且等式 $x+y=x'+y'$ 成立。由条件立即可以得到下列等式成立：

$$x+x'=y+y', (y+y') \in C_2$$

与假设矛盾，所以 $(x+x') \notin C_2$ 时式(5.6)成立。

由以上的性质，我们取遍 C_1 中所有的 $x \in C_1$，可以得到的直交状态 $|x+C_2\rangle$ 的个数为

$$\frac{2^{k_1}}{2^{k_2}}=2^{k_1-k_2}$$

这里 k_1 代表 C_1 的代码长，k_2 代表 C_2 的代码长。这些相异的状态由以下的集合表示：

$$\{|x_0+C_2\rangle, |x_1+C_2\rangle, \cdots, |x_{2^{k_1-k_2}-1}+C_2\rangle\}$$

CSS代码就是将 k_1-k_2 个 qubit 的重叠状态

$$\alpha_0|0\cdots00\rangle+\alpha_1|0\cdots01\rangle+\alpha_2|0\cdots10\rangle+\cdots+\alpha_{2^{k_1-k_2}-1}|1\cdots11\rangle$$

转换成 n 个 qubit 的重叠状态

$$\alpha_0|x_0+C_2\rangle+\alpha_1|x_1+C_2\rangle+\alpha_2|x_2+C_2\rangle+\cdots+\alpha_{2^{k_1-k_2}-1}|x_{2^{k_1-k_2}-1}+C_2\rangle$$

的编码体系。因此，CSS代码是在$[n, k_1]$线性编码集合 C_1 和$[n, k_2]$线性编码集合 C_2 满足 $C_2 \subset C_1$ 时，由 C_1 和 C_2 构成的$[[n, k_1-k_2]]$量子线性编码集合。

例题 5.9 作为线性编码集合 C_1，选择$[7, 4]$Hamming 编码集合，它的奇偶校验矩阵如 H_1 所示。另一个线性编码集合 C_2，我们假设它是奇偶校验矩阵为 H_2 的$[7, 3]$Hamming 代码集合。

$$H_1=\begin{bmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{bmatrix} \quad H_2=\begin{bmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{bmatrix}$$

显然，C_2 表示的线性编码集合如下：

$$C_2=\{(0000000), (1010101), (0110011), (1100110),$$
$$(0001111), (1011010), (0111100), (1101001)\}$$

与[7，4]Hamming 编码 C_1 的线性编码集合作比较，

$$\begin{aligned}C_1 = \{&(0000000),(1110000),(1001100),(0101010),\\&(1101001),(0111100),(1011010),(0011001),\\&(1100110),(0100101),(0010110),(1010101),\\&(0110011),(0001111),(1000011),(1111111)\}\end{aligned}$$

显然满足 $C_2 \subset C_1$。现在对应于代码 $(0000000) \in C_1$ 构成的状态 $|0000000+C_2\rangle$，我们立即可以得到 $|s_0\rangle$：

$$\begin{aligned}|s_0\rangle &= |0000000+C_2\rangle\\&= \frac{1}{\sqrt{8}}\sum_{y\in C_2}|0000000+y\rangle\\&= \frac{1}{\sqrt{8}}\{|0000000\rangle+|1010101\rangle+|0110011\rangle+|1100110\rangle+\\&\quad |0001111\rangle+|1011010\rangle+|0111100\rangle+|1101001\rangle\}\end{aligned}$$

若再任取 C_1 与 C_2 交集中的任意元素，例如(1010101)，它也构成下列的状态：

$$\begin{aligned}&|1010101+C_2\rangle\\&= \frac{1}{\sqrt{8}}\sum_{y\in C_2}|1010101+y\rangle\\&= \frac{1}{\sqrt{8}}\{|1010101\rangle+|0000000\rangle+|1100110\rangle+|0110011\rangle+\\&\quad |1011010\rangle+|0001111\rangle+|1101001\rangle+|0111100\rangle\}\end{aligned}$$

该结果与(0000000)对应的状态 $|s_0\rangle$ 是一致的。即

$$|0000000+C_2\rangle = |1010101+C_2\rangle$$

另一方面，如果选择包含在 C_1 中但不包含在 C_2 中的 $|1111111\rangle$，能够获得第 2 个状态 $|s_1\rangle$：

$$\begin{aligned}|s_1\rangle &= |1111111+C_2\rangle\\&= \frac{1}{\sqrt{8}}\sum_{y\in C_2}|1111111+y\rangle\\&= \frac{1}{\sqrt{8}}\{|1111111\rangle+|0101010\rangle+|1001100\rangle+|0011001\rangle+\\&\quad |1110000\rangle+|0100101\rangle+|1000011\rangle+|0010110\rangle\}\end{aligned}$$

因为

$$\begin{aligned}\langle s_0 \mid s_1\rangle &= \langle C_2 + 1010101 \mid 1111111 + C_2\rangle \\ &= \langle C_2 \mid 1111111\rangle + \langle 1010101 \mid 1111111\rangle + \langle C_2 \mid C_2\rangle + \\ &\quad \langle 1010101 \mid C_2\rangle \\ &= 0\end{aligned}$$

所以，$|s_0\rangle$与$|s_1\rangle$直交。若再取 $(1001100) \in C_1 (\notin C_2$，有 $|1001100 + C_2\rangle = |1111111 + C_2\rangle$，即不可能再找到一个$|s'\rangle$与$|s_0\rangle$、$|s_1\rangle$都直交，这是因为此时有

$$\frac{2^{k_1}}{2^{k_2}} = 2^{k_1 - k_2} = 2^{4-3} = 2$$

即对应于 C_1 的代码集合，除了 2 个状态$\{|s_0\rangle, |s_1\rangle\}$以外，其他状态是不存在的。因此，对应的量子纠错编码集合是 $[[7, 4-3]] = [[7, 1]]$ 量子代码集合，则一个 qubit 的状态 $\alpha|0\rangle + \beta|1\rangle$ 可以转换成以下代码：

$$\alpha|s_0\rangle + \beta|s_1\rangle$$

5.4 CSS 编码的解码

本节主要讲解 CSS 编码的解码方法。当线性编码集合 C_1 与 $C_2^{\perp}$ 能够订正 t 个 bit 错误时，让我们来说明并演示由 C_1 和 C_2 构成的 CSS 代码是怎样订正至多 t 个 bit 反转以及 t 个位相翻转错误的。

以下为了简单起见，我们着重说明 bit 反转和位相翻转各自至多发生一个错误时的解码方法，当一个以上的错误发生时使用同样的方法可以实现解码。

首先考虑下式状态的编码：

$$|x + C_2\rangle = \frac{1}{2^{k_2/2}} \sum_{y \in C_2} |x + y\rangle \tag{5.11}$$

这里假设线性编码集合 C_1 的奇偶校验矩阵为 H_1，因为 $x \in C_1$，则

$$xH_1^T = 0$$

又因为 $C_2 \subset C_1$，所以对于任意的 $y \in C_2$，同样有

$$yH_1^T = 0$$

成立。因此，对应于等式(5.11)，状态 $|x + C_2\rangle$ 等式的右边状态 $|x + y\rangle$ 矢量 $x + y$ 的伴随式，即使 $y \in C_2$ 不成立，也有下面的等式成立：

$$(x + y)H_1^T = xH_1^T + yH_1^T = 0$$

另一方面，假设用 e_i 表示长度为 n 的、仅在第 i 位为 1、其他各位均为 0 的矢量，则$|x\rangle$的第 i 位 qubit 上发生 bit 反转后的状态可用 $|x+e_i\rangle$ 表示。所以，状态 $|x+C_2\rangle$ 的第 i 位上 qubit 发生 bit 反转错误时，我们接收到的状态可用下式表示：

$$|\varphi\rangle = \frac{1}{2^{k_2/2}} \sum_{y \in C_2} |x+y+e_i\rangle \tag{5.12}$$

此时如若计算式(5.12)右边的状态 $|x+y+e_i\rangle$ 对应矢量 $x+y+e_i$ 的伴随式，即使 $y \notin C_2$，也能得到下面的等式：

$$(x+y+e_i)H_1^T = xH_1^T + yH_1^T + e_iH_1^T = e_iH_1^T$$

也就是说集合中的代码全体拥有同一个伴随式 $e_iH_1^T$。这里因为线性编码集合 C_1 能够订正 t 个错误，所以对应于惟一一个错误的伴随式 $e_1H_1^T$，$e_2H_1^T$，…，$e_nH_1^T$ 当然是相互不同的。显然，如果能够从接收到的信息状态$|\varphi\rangle$中求出伴随式 $e_iH_1^T$，使用经典纠错编码的解码方法就能够知道在哪一位 qubit 上发生了错误(此时是第 i 位上 qubit 发生了错误)，在错误发生的 qubit 位上通过 X－Gate 执行 bit 反转演算，就可以订正相应的错误。

对应于例题 4.4 中描述的量子编码，实际执行伴随式计算的量子门电路如图 5－3 所示。

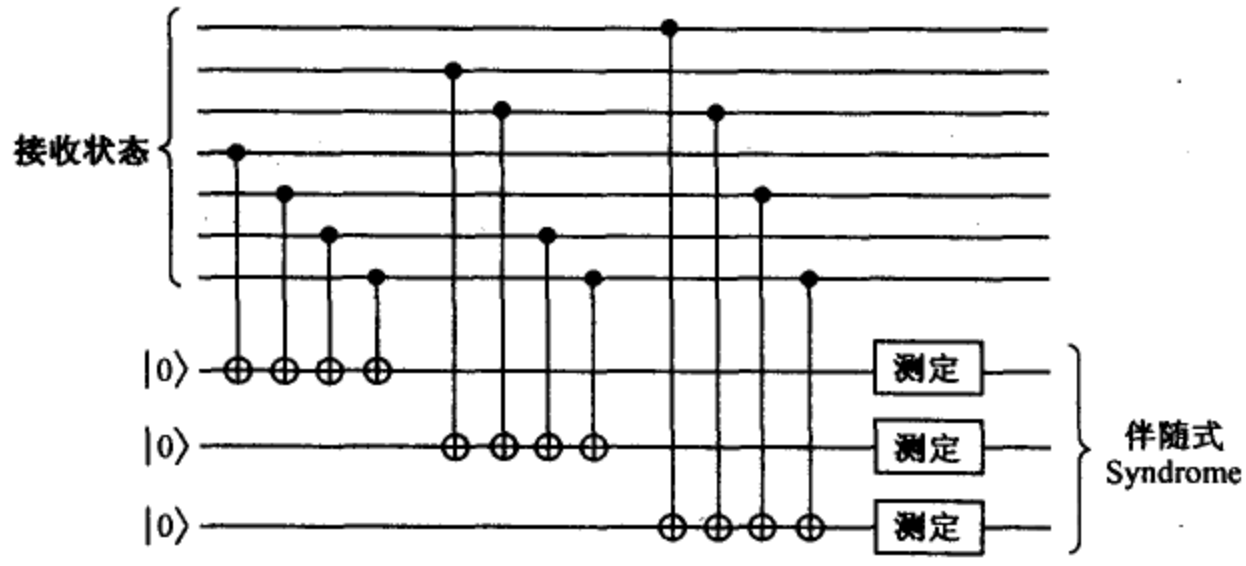


图 5－3　计算伴随式的量子门电路

此时对应于线性编码集合 C_1 的奇偶校验矩阵为

$$H_1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

该量子门电路的动作本质上与 4.2 节中讲述的 3 个 qubit 编码的解码器同样。因此，对应于伴随式的 3 个 qubit 如果能够基于基底状态{|0⟩，|1⟩}进行测定，判定它们是 0 或 1，就能够以概率 1 得知伴随式 $e_i H_1^T$。

例题 5.10 以例 5.4 构成的 CSS 编码为例，将状态 $\alpha|0\rangle+\beta|1\rangle$ 编码成为 $\alpha|s_0\rangle+\beta|s_1\rangle$ 并送入信道。假设第 3 位 qubit 上发生 bit 反转错误，则接收到的 qubit 列的重叠状态可表示如下：

$$\begin{aligned}&\frac{\alpha}{2\sqrt{2}}\{|0010000\rangle+|1000101\rangle+|0100011\rangle+|1110110\rangle+\\&|0011111\rangle+|1001010\rangle+|0101100\rangle+|1111001\rangle\}+\\&\frac{\beta}{2\sqrt{2}}\{|1101111\rangle+|0111010\rangle+|1011100\rangle+|0001001\rangle+\\&|1100000\rangle+|0110101\rangle+|1010011\rangle+|0010110\rangle\}\end{aligned}$$

求解伴随式即可得到(011)，此时便可知道是 qubit 列的第 3 位上发生了错误，之后只要对第 3 位上的 qubit 实施 bit 反转演算 X-Gate 即可订正该错误。

下面再讨论订正位相翻转错误，为此每一个 qubit 位执行 Hadamard 变换演算。此时对$|x\rangle$实施 *Hadamard* 变换演算的结果如下式所示：

$$|x\rangle \overset{\text{Hadamard}}{\Rightarrow} \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle \tag{5.13}$$

式(5.13)的成立与两个序列 $y=(y_1, y_2, \cdots, y_n)$、$x=(x_1, x_2, \cdots, x_n)$ 有关，$|y\rangle$的正负由 $y_i=1$ 且 $x_i=1$ 的 bit 位置有几个来决定，如果是偶数个则为正，奇数个则为负。例如，将 $|01\rangle=|0\rangle|1\rangle$ 实施 Hadamard 变换演算，其结果为

$$\begin{aligned}(H|0\rangle)(H|1\rangle)&=\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\\&=\frac{1}{2}(|00\rangle-|01\rangle+|10\rangle-|11\rangle)\\&=\frac{1}{2}((-1)^{(01)\cdot(00)}|00\rangle+(-1)^{(01)\cdot(01)}|01\rangle+\\&\quad(-1)^{(01)\cdot(10)}|10\rangle+(-1)^{(01)\cdot(11)}|11\rangle)\end{aligned}$$

因此，可以确认式(5.13)的成立。

那么，利用编码对状态

$$|x+C_2\rangle=\frac{1}{2^{k_2/2}}\sum_{y\in C_2}|x+y\rangle$$

的各个 qubit 实施 Hadamard 变换演算，由式(5.13)得到下式：

$$\frac{1}{2^{k_2/2}2^{n/2}}\sum_{x\in\{0,1\}^n}\sum_{y\in C_2}(-1)^{(x+y)\cdot z}\mid z\rangle \tag{5.14}$$

这里，如果使用线性编码集合 C_2 的线性性质导出的关系式：

$$\sum_{y\in C_2}(-1)^{y\cdot z}=\begin{cases}2^{k_2} & if\ z\in C_2^{\perp}\\ 0 & if\ z\notin C_2^{\perp}\end{cases} \tag{5.15}$$

则式(5.15)可以写成下列形式：

$$\frac{1}{2^{k_2/2}2^{n/2}}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot z}\sum_{y\in C_2}(-1)^{y\cdot z}\mid z\rangle$$
$$=\frac{2^{k_2/2}}{2^{n/2}}\sum_{x\in C_2^{\perp}}(-1)^{x\cdot z}\mid z\rangle$$

上式右边出现的状态$|z\rangle$所对应的矢量 z 已都是 $C_2^{\perp}$ 或者说是线性编码集合 C_2 的对偶编码集合的元素了。

另一方面，再一次用 e_j 表示长度为 n 仅在第 j 位为 1，其他各位均为 0 的矢量，那么注意到矢量 xe_j，当 x 的第 j 位为 1 时 xe_j 为 1，当 x 的第 j 位为 0 时则 xe_j 就为 0；当第 j 位 qubit 上发生位相翻转错误时，$|x\rangle$就变成$(-1)^{x\cdot e_j}|x\rangle$。因此，如果状态$|x+C_2\rangle$的第 j 位 qubit 上发生位相翻转错误时，将得到下列状态：

$$\frac{1}{2^{k_2/2}}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_j}\mid x+y\rangle$$

对该状态的各个 qubit 实施 Hadamard 变换演算，由式(5.9)得到

$$\frac{1}{2^{k_2/2}2^{n/2}}\sum_{x\in\{0,1\}^n}\sum_{y\in C_2}(-1)^{(x+y)\cdot(e_j+z)}\mid z\rangle$$
$$=\frac{1}{2^{k_2/2}2^{n/2}}\sum_{z'\in\{0,1\}^n}\sum_{y\in C_2}(-1)^{(x+y)\cdot z'}\mid z'+e_j\rangle,$$

此处设 $z'=z+e_j$。再一次利用式(5.11)可得到下面的结果：

$$\frac{2^{k_2/2}}{2^{n/2}}\sum_{z'\in C_2^{\perp}}(-1)^{x\cdot z'}\mid z'+e_j\rangle \tag{5.16}$$

从式(5.16)可以看出，经过 Hadamard 变换演算，位相翻转错误可以转换成 bit 反转错误。因此，对于式(5.16)的状态，只要订正 bit 反转错误就可以订正位相翻转的错误。实际上利用代码集合 $C_2^{\perp}$ 的奇偶校验矩阵为 H_2，求解状态 $|z'+$

$e_j\rangle$ 对应矢量 $z'+e_j$ 的伴随式为 $e_jH_2^T$，因为 $C_2^{\perp}$ 能够订正 t 个以下错误，因此，从伴随式可以确定错误 e_j 并能够订正它。作为结果，得到下列状态：

$$\frac{2^{k_2/2}}{2^{n/2}}\sum_{z'\in C_2^{\perp}}(-1)^{(x+y)\cdot z'}\mid z'\rangle$$

然后再一次对该状态的各个 qubit 实施 Hadamard 变换演算，就能够获得纠错后的正确的送信的原始状态信息。

例题 5.11 再一次以例 5.4 构成的 CSS 编码为例，将状态 $\alpha\mid 0\rangle+\beta\mid 1\rangle$ 编码成为 $\alpha\mid s_0\rangle+\beta\mid s_1\rangle$ 并送入信道。假设第一位 qubit 上发生位相翻转错误，接收到的 qubit 列的重叠状态如下：

$$\begin{aligned}&\frac{\alpha}{2\sqrt{2}}\{\mid 0000000\rangle-\mid 1010101\rangle+\mid 0110011\rangle-\mid 1100110\rangle+\\&\quad\mid 0001111\rangle-\mid 1011010\rangle+\mid 0111100\rangle-\mid 1101001\rangle\}+\\&\quad\frac{\beta}{2\sqrt{2}}\{-\mid 1111111\rangle+\mid 0101010\rangle-\mid 1001100\rangle+\mid 0011001\rangle-\\&\quad\mid 1110000\rangle+\mid 0100101\rangle-\mid 1000011\rangle+\mid 0000110\rangle\}。\end{aligned}$$

求解伴随式得到(000)，从结果中可以知道接收状态中没有 bit 反转错误。

紧接着对接收状态的各个 qubit 实施 Hadamard 变换演算，由于能够非常容易地确认等式 $C_2^{\perp}=C_1$ 的成立，因此得到下列的等式：

$$\begin{aligned}&\frac{\alpha}{4}\{\mid 1000000\rangle+\mid 0110000\rangle+\mid 0001100\rangle+\mid 1101010\rangle+\\&\quad\mid 0101001\rangle+\mid 1111100\rangle+\mid 0011010\rangle+\mid 1011001\rangle+\\&\quad\mid 0100110\rangle+\mid 1100101\rangle+\mid 1010110\rangle+\mid 0010101\rangle+\\&\quad\mid 1110011\rangle+\mid 1001111\rangle+\mid 0000011\rangle+\mid 0111111\rangle\}\\&\frac{\beta}{4}\{\mid 1000000\rangle-\mid 0110000\rangle-\mid 0001100\rangle-\mid 1101010\rangle+\\&\quad\mid 0101001\rangle+\mid 1111100\rangle+\mid 0011010\rangle-\mid 1011001\rangle+\\&\quad\mid 0100110\rangle-\mid 1100101\rangle-\mid 1010110\rangle+\mid 0010101\rangle+\\&\quad\mid 1110011\rangle+\mid 1001111\rangle-\mid 0000011\rangle-\mid 0111111\rangle\}\end{aligned}$$

再一次求解伴随式就得到(001)，此时便可知道是第一位 qubit 上发生

bit 反转错误。然后，只要对第一位上的 qubit 实施 bit 反转演算 X－Gate，在订正该错误后再一次实施 Hadamard 变换演算，即可恢复原始的送信状态。

以上讲解了用 CSS 编码如何订正 bit 反转错误和位相翻转错误，最后演示用 CSS 编码订正两者同时发生的错误。如果状态 $|x+C_2\rangle$ 第 i 位 qubit 上发生 bit 反转错误、第 j 位 qubit 上发生位相翻转错误时，将得到下列状态：

$$\frac{1}{2^{k_2/2}}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_j}\ |x+y+e_i\rangle$$

如果计算该状态 $|x+y+e_i\rangle$ 所对应的矢量 $x+y+e_i$ 的伴随式，将得到 $e_iH_1^T$，由线性编码集合 C_1 的解码方法能够确认在第 i 位 qubit 上发生 bit 反转错误，因此对第 i 位上的 qubit 实施 bit 反转演算 X－Gate，订正 bit 反转错误后的状态就变成如下：

$$\frac{1}{2^{k_2/2}}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_j}\ |x+y\rangle$$

此时的状态仅包含位相翻转错误，同样的道理，使用前述的订正位相翻转错误的方法，自然能够恢复发送信息的原始状态。

5.5　量子纠错编码的性能界限

直到上一节为止我们讲述了 CSS 编码以及更一般性的量子纠错编码，这些纠错编码体系的纠错能力究竟有多大呢？这一节就来讨论量子纠错编码的性能界限。

当给定代码长度为 n，码字 qubit 数为 k 时，我们用该体系最多可以订正几个 qubit 位上发生错误的尺度来衡量该量子纠错编码体系的性能？显然能够订正的错误个数越多其量子编码的性能就越高。下面首先介绍关于量子编码可达到性能的下界，它是经典纠错编码Gilbert-Varshamov界限的量子版。

定理 5.11　（量子 Gilbert-Varshamov 界限）当代码长度 n 足够大时，能够订正 t 个qubit位上发生错误的量子编码在 CSS 编码中是存在，该编码是编码参数(n, k, t)满足下列不等式的$[[n, k]]$量子编码体系。

$$\frac{k}{n}\geqslant 1-2H\left(\frac{2t}{n}\right)$$

其中函数 $H(x)$由下列等式定义：

$$H(x)=-x\log x-(1-x)\log(1-x)$$

这个定理说明量子编码的错误订正能力保持在 t/n 的一定水准时，其编码的效率能够保持在一定值 k/n 以上。

另一方面，量子编码可达到的性能上界是经典纠错编码的 Hamming 界限的量子版。

定理 5.12 （量子 Hamming 界限）任意的[[n, k]]量子编码体系，能够订正错误的 qubit 数 t 满足下列不等式：

$$\sum_{j=0}^{t}\binom{n}{j}3^j 2^k \leqslant 2^n \tag{5.17}$$

这个定理不依赖于量子纠错编码的构成方法，无论什么样的量子编码体系，这个不等式都成立。但是请注意，即使满足式(5.17)的 n、k、t 组存在，也未必能够构成具有这些参数的编码体系。

例题 5.12 有关前面讲到的[[7, 1]]量子编码体系，有下列等式：

$$1-2H\left(\frac{2t}{n}\right)=1-2\times\left\{-\left(\frac{2}{7}\right)\log\left(\frac{2}{7}\right)-\left(\frac{5}{7}\right)\log\left(\frac{5}{7}\right)\right\}=-0.72624$$

因为 $\frac{k}{n}=\frac{1}{7}$，因此满足 Gilbert-Varshamov 界限。

另一方面，因为

$$\binom{7}{0}3^0 2^1+\binom{7}{1}3^1 2^1=2+42=44<2^7$$

[[7, 1]]量子编码体系同样也满足 Hamming 界限。

第 6 章　量子纠缠状态的纯化协议及其应用

本章节中我们着重介绍量子纠错编码与双对概念导入的量子纠缠状态纯化协议及其应用。量子纠缠状态纯化协议又称为 EPP(Entanglement Purification Protocol)协议。

6.1　EPP 的原理

再一次考虑贝尔状态：

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

正如第 3 章所述，这 4 个状态组成两位 qubit 列向量空间的正规直交基底。

在利用量子高密度编码或量子瞬间传递(Teleportation 离物传态)之前，送收信者双方必须共同拥有纠缠状态(更准确地说是贝尔状态)中的某个 qubit 对。但是，实际上在共同拥有贝尔状态的过程中，一是由于 qubit 在量子信道的传送过程中状态受噪声的干扰，或是由于 qubit 的保存时间持续其状态将会发生变化。因此，在实际利用贝尔状态进行通信时必须考虑这些 qubit 状态的抗干扰对策。这些抗干扰对策方法中的一个就是利用量子纠错编码体系，也就是说利用纠错编码体系，达到订正 qubit 在量子信道的传送过程中或在保存时间的持续中其状态发生变化产生的错误。另一个方法就是现在要讲述的“纠缠状态纯化协议(EPP)”。

以下首先假设在备制中心 C 备制出贝尔状态$|\beta_{00}\rangle$，且通过量子信道把纠缠

对中一个 qubit 传送给用户 A，把另一个 qubit 传送给用户 B。此时用户 A 和 B 双方除了自己拥有的 qubit 以外，对其他任意的 qubit 都不能进行演算和测定；再假定用户 A 和 B 双方可把测定的结果通过无噪声经典信道相互通知。如此状况与条件下纠缠状态纯化协议 EPP 的另一种说法是：以任意接近 1 的概率使 A、B 双方共同拥有贝尔状态$|\beta_{00}\rangle$的协议。

为了说明简单，我们可以考虑在中心和用户之间采用在 4.2 节里讲述的 bit 反转信道作为量子信道。也就是说：假设以概率 p 在输入状态上实施 bit 反转演算(量子逻辑非门，X-Gate)，以概率 $1-p$ 让输入状态按原样输出。此时无须花费什么精力，只要备制中心 C 将备制出的贝尔状态$|\beta_{00}\rangle$分别传送给用户 A 和用户 B，用户 A 和用户 B 的状态就变成

$$\text{以概率 } (1-p)^2 \text{ 为} \quad \frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

$$\text{以概率 } p(1-p) \text{ 为} \quad \frac{(X|0\rangle)|0\rangle+(X|1\rangle)|1\rangle}{\sqrt{2}}=\frac{|10\rangle+|01\rangle}{\sqrt{2}}$$

$$\text{以概率 } (1-p)p \text{ 为} \quad \frac{|0\rangle(X|0\rangle)+|1\rangle(X|1\rangle)}{\sqrt{2}}=\frac{|01\rangle+|10\rangle}{\sqrt{2}}$$

$$\text{以概率 } p^2 \text{ 为} \quad \frac{(X|0\rangle)(X|0\rangle)+(X|1\rangle)(X|1\rangle)}{\sqrt{2}}=\frac{|11\rangle+|00\rangle}{\sqrt{2}}$$

由此可见当备制中心 C 将一对纠缠的量子比特通过 bit 反转信道分别发送给 A 和 B 时，只有在其中一个 qubit 发生 bit 反转时，纠缠状态才会出现与备制中心传送的初始状态不同而出现错误。现在假设

$$q=1-(1-p)^2-p^2$$

我们知道用户 A 和用户 B 以概率 $1-q$ 共同拥有贝尔状态$|\beta_{00}\rangle$成功，以概率 q 共同拥有贝尔状态$|\beta_{00}\rangle$失败。也就是说：用户 A 和用户 B 共同拥有 qubit 对状态的概率为

$$\text{以概率 } 1-q \text{ 为} \quad \frac{|00\rangle+|11\rangle}{\sqrt{2}}=|\beta_{00}\rangle$$

$$\text{以概率 } q \text{ 为} \quad \frac{|01\rangle+|10\rangle}{\sqrt{2}}=|\beta_{01}\rangle$$

以下假设 q 满足不等式 $0<q<\frac{1}{2}$。假设备制中心 C 备制出 2 个贝尔状态

$|\beta_{00}\rangle$，并将 2 个贝尔状态$|\beta_{00}\rangle$中的第 1 个 qubit 发送给用户 A、第 2 个 qubit 发送给用户 B，此时因为 A 和 B 共同拥有 2 个 qubit 对，因此共同拥有贝尔状态$|\beta_{00}\rangle$的概率将大于 $1-q$ 的方法称为 EPP。首先 A 和 B 的 2 个 qubit 对的状态如下：

以概率 $(1-q)^2$ 为　　$|\beta_{00}\rangle|\beta_{00}\rangle$

以概率 $(1-q)q$ 为　　$|\beta_{00}\rangle|\beta_{01}\rangle$

以概率 $q(1-q)$ 为　　$|\beta_{01}\rangle|\beta_{00}\rangle$

以概率 q^2 为　　$|\beta_{01}\rangle|\beta_{01}\rangle$

使用 EPP 方法，用以下的操作能够以更高的概率共同拥有贝尔状态$|\beta_{00}\rangle$(参阅图6－1)。

假设用户 A 和 B 将自己所拥有的 2 个 qubit 输入到控制非门(Controlled-NOT-Gate)，其结果，如果 2 个 qubit 对的状态是

$$|\beta_{00}\rangle|\beta_{00}\rangle=\frac{(|00\rangle+|11\rangle)(|00\rangle+|11\rangle)}{2}$$

$$=\frac{(|0000\rangle+|0011\rangle)(|1100\rangle+|1111\rangle)}{2}$$

注意到 A 所拥有的 qubit 是 qubit 列中的第 1 位和第 3 位 bit、B 所拥有的 qubit 是 qubit 列中的第 2 位和第 4 位 bit。让它们分别通过 Controlled-NOT-Gate，便得到下式表示的状态：

$$\frac{(|0000\rangle+|0011\rangle)(|1111\rangle+|1100\rangle)}{2}=|\beta_{00}\rangle|\beta_{00}\rangle \tag{6.1}$$

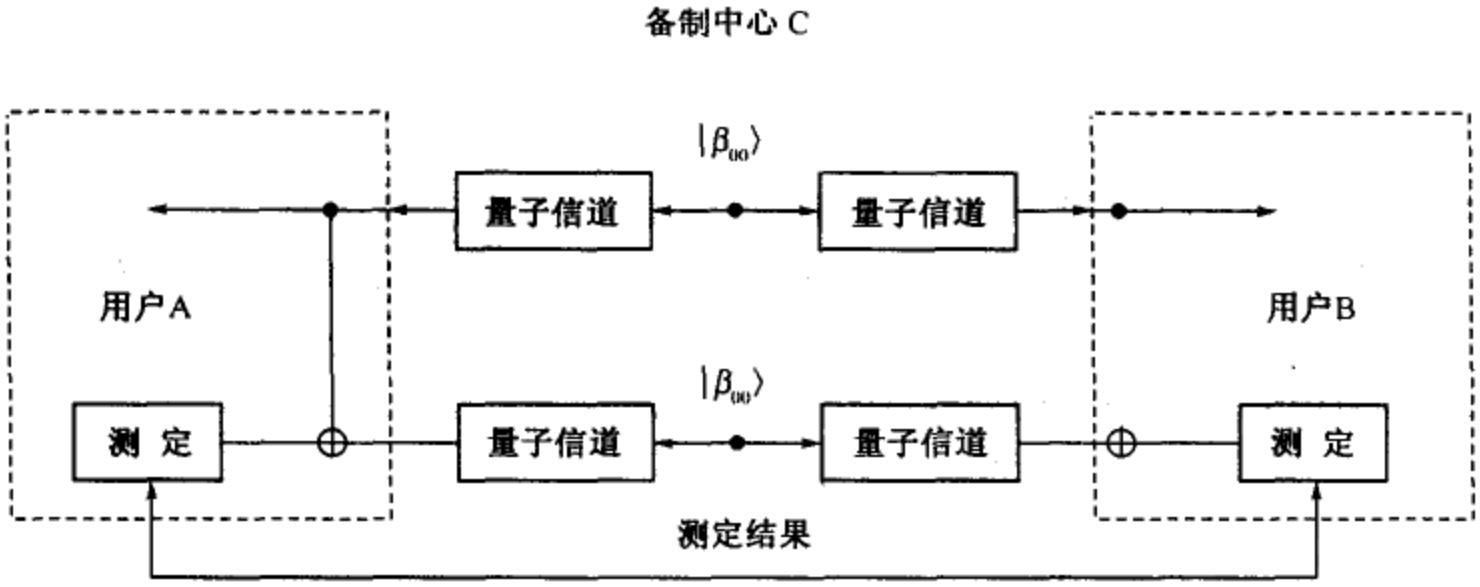


图 6－1　EPP

用同样的方法让其他的状态也通过 Controlled-NOT-Gate，可以得到以下的结果：

$$|\beta_{00}\rangle|\beta_{00}\rangle \rightarrow |\beta_{00}\rangle|\beta_{00}\rangle$$

$$|\beta_{00}\rangle|\beta_{01}\rangle \rightarrow |\beta_{00}\rangle|\beta_{01}\rangle$$

$$|\beta_{01}\rangle|\beta_{00}\rangle \rightarrow |\beta_{01}\rangle|\beta_{01}\rangle$$

$$|\beta_{01}\rangle|\beta_{01}\rangle \rightarrow |\beta_{01}\rangle|\beta_{00}\rangle$$

进一步，让用户 A 和 B 以$|0\rangle$和$|1\rangle$为基底共同测定自己拥有的第 2 位 qubit，测定的结果通过经典信道相互通知对方。如果两者测定的结果一致，则保存剩余的 qubit；如果结果不一致的话就放弃剩余的 qubit。在保存 qubit 的情况下，由第 3 位和第 4 位组成的 qubit 对的状态是

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

即状态$|\beta_{00}\rangle$出现的情况下，可以判定从备制中心 C 接收到的状态只能是$|\beta_{00}\rangle|\beta_{00}\rangle$或$|\beta_{01}\rangle|\beta_{01}\rangle$，且该状态出现的概率是$(1-q)^2+q^2$。再进一步，当 qubit 被保存时，剩余的qubit对的状态以及出现的概率如下：

以概率$\frac{(1-q)^2}{(1-q)^2+q^2}$为　　$|\beta_{00}\rangle$

以概率$\frac{q^2}{(1-q)^2+q^2}$为　　$|\beta_{01}\rangle$

这里因为 q 满足不等式 $0<q<\frac{1}{2}$，所以下列不等式成立：

$$\frac{(1-q)^2}{(1-q)^2+q^2} > 1-q$$

结论告诉我们：利用 EPP 的方法，拥有状态$|\beta_{00}\rangle$的概率是增加的。

例题 6.1　假设利用出错率为 $p=0.1$ 的 bit 反转信道将备制中心 C 备制的贝尔状态配置给用户 A 和 B 共同拥有，此时若使用 2 个贝尔状态并利用 EPP 方法，使用户 A 和 B 共同拥有贝尔状态$|\beta_{00}\rangle$的概率可计算如下：

$$q = 1-(1-0.1)^2-0.1^2 = 0.18$$

$$\frac{(1-0.18)^2}{(1-0.18)^2+0.18^2} = 0.954$$

这个结果比不利用 EPP 方法使用户 A 和 B 共同拥有贝尔状态$|\beta_{00}\rangle$的概率 0.82 要大。然而，利用 EPP 方法被破弃的 qubit 概率变为

$$1-\{(1-0.18)^2+0.18^2\}=0.2952$$

再进一步，使用 4 个贝尔状态，每两个贝尔状态上利用 EPP 方法获得 2 个 qubit 对后，再一次利用 EPP 方法，此时用户 A 和 B 共同拥有贝尔状态$|\beta_{00}\rangle$的概率将进一步增大到

$$\frac{(1-0.046)^2}{(1-0.046)^2+0.046^2}=0.998$$

这时，利用 EPP 方法的若干次过程中被破弃的全部 qubit 的概率也将增至到 0.678。

6.2　Quantum Privacy Amplification 协议

上一节讲述的基本 EPP 方法对量子信道是有限制的(即 bit 反转信道)。这一节讲解由 Deutsch 等人提出的，针对一般的量子信道能够利用的 EPP 方法，即 Quantum Privacy Amplification(QAP)协议。QAP 协议是在量子密钥分配的基础之上，利用共有纠缠状态的物理事实，为了减少量子信道本身的错误或避免第三者的恶意篡改对量子信息的影响而提出的协议。

再一次考虑这样的情况，为了使用户 A 和 B 共同拥有贝尔状态$|\beta_{00}\rangle$，备制中心 C 备制了 2 个贝尔状态$|\beta_{00}\rangle$，并通过量子信道配送给用户 A 和 B 各自 qubit 对中的对应部分。与上一节讲述的一样，用户 A 和 B 各自对自己拥有的 qubit 实施演算测试，希望增加贝尔状态$|\beta_{00}\rangle$共同拥有的概率。

QAP 协议里，用户 A 使用下面的酉演算子U_A对备制中心 C 传送来的 2 个 qubit 实施演算：

$$U_A=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -i\\ -i & 1\end{bmatrix}$$

则$U_A|0\rangle$和$U_A|1\rangle$分别为

$$U_A|0\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -i\\ -i & 1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}=\frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\0\end{bmatrix}+(-i)\begin{bmatrix}0\\1\end{bmatrix}\right)$$

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

$$U_A \mid 1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -i \\ -i & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} -i \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\left((-i)\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)$$

$$= \frac{1}{\sqrt{2}}((-i) \mid 0\rangle + \mid 1\rangle)$$

同样用户 B 使用下面的酉演算子 U_B 也对备制中心 C 传送来的 2 个 qubit 实施演算：

$$U_B = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$$

则 $U_B|0\rangle$ 和 $U_B|1\rangle$ 分别为

$$U_B \mid 0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ i \end{bmatrix} = \frac{1}{\sqrt{2}}\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} + i\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)$$

$$= \frac{1}{\sqrt{2}}(\mid 0\rangle + i \mid 1\rangle)$$

$$U_B \mid 1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} i \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\left(i\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)$$

$$= \frac{1}{\sqrt{2}}(i \mid 0\rangle + \mid 1\rangle)$$

然后，用户 A 和 B 各自将自己拥有的 2 个 qubit 通过控制非门(Controlled-NOT-Gate)，并以{|0⟩，|1⟩}为基底测定各自拥有的 qubit，并将测定的结果通过经典信道相互通知对方。如果两者测定的结果一致，则剩余的 1 个 qubit 以更高的概率被认定是状态$|\beta_{00}\rangle$并加以保存，另一方面若结果不一致的话就要破弃剩余的 1 个 qubit。QAP 协议的操作顺序如图 6－2 所示。

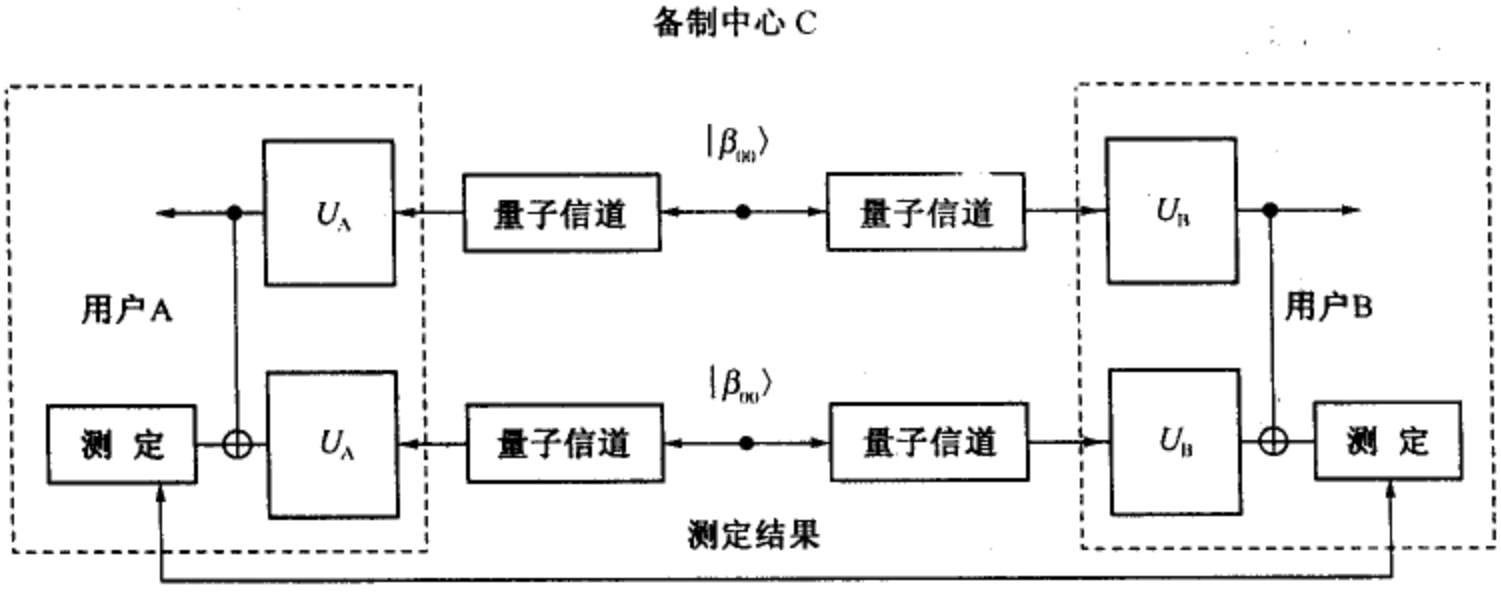


图 6－2 QAP 协议

现借助例题来说明 QAP 协议的效果。为了简单起见，假设备制中心和用户之间的量子信道是位相翻转信道，发送的信号能够以 $1-p$ 的概率正确地接收到，以 p 的概率接收到的信号是发送信号上实施的位相翻转演算(Z-Gate)的 qubit。设 $q=1-(1-p)^2-p^2$，此时用户 A 和 B 的可能状态如下：

以概率 $(1-q)^2$ 为　　$|\beta_{00}\rangle|\beta_{00}\rangle$

以概率 $(1-q)q$ 为　　$|\beta_{00}\rangle|\beta_{10}\rangle$

以概率 $q(1-q)$ 为　　$|\beta_{10}\rangle|\beta_{00}\rangle$

以概率 q^2 为　　$|\beta_{10}\rangle|\beta_{10}\rangle$

这时用户 A 对自己拥有的两个 qubit(第 1 位和第 3 位)实施 U_A 演算，用户 B 也对自己拥有的两个 qubit(第 2 位和第 4 位)实施 U_B 演算。如果用户 A 和 B 共同拥有的状态是$|\beta_{00}\rangle$，则通过演算我们能够得到以下状态：

$$|\beta_{00}\rangle \xrightarrow{U_A,U_B} \frac{(U_A|0\rangle)(U_B|0\rangle)+(U_A|1\rangle)(U_B|1\rangle)}{\sqrt{2}}$$

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

$$=\frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

$$=|\beta_{00}\rangle$$

用同样的方法针对其他的贝尔状态演算

$$|\beta_{01}\rangle \xrightarrow{U_A,U_B} \frac{(U_A|0\rangle)(U_B|1\rangle)+(U_A|1\rangle)(U_B|0\rangle)}{\sqrt{2}}$$

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

$$=\frac{|01\rangle+|10\rangle}{\sqrt{2}}$$

$$=|\beta_{01}\rangle$$

$$|\beta_{10}\rangle \xrightarrow{U_A,U_B} \frac{(U_A|0\rangle)(U_B|0\rangle)-(U_A|1\rangle)(U_B|1\rangle)}{\sqrt{2}}$$

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

$$=\frac{|01\rangle-|10\rangle}{\sqrt{2}}i$$

$$= |\beta_{11}\rangle$$

$$|\beta_{11}\rangle \xrightarrow{U_A, U_B} \frac{(U_A|0\rangle)(U_B|1\rangle) - (U_A|1\rangle)(U_B|0\rangle)}{\sqrt{2}}$$

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

$$= \frac{|00\rangle - |11\rangle}{\sqrt{2}} i$$

$$= |\beta_{10}\rangle$$

效果如下：

$$|\beta_{00}\rangle \rightarrow |\beta_{00}\rangle$$

$$|\beta_{01}\rangle \rightarrow |\beta_{01}\rangle$$

$$|\beta_{10}\rangle \rightarrow |\beta_{11}\rangle$$

$$|\beta_{11}\rangle \rightarrow |\beta_{10}\rangle$$

这里将对用户 A 和 B 的接收信号状态的不同分别进行讨论。

(1) 用户 A 和 B 的状态是$|\beta_{00}\rangle|\beta_{00}\rangle$场合

A 和 B 各自对自己拥有的 qubit 分别同时实施 U_A 演算或 U_B 演算：

$$|\beta_{00}\rangle |\beta_{00}\rangle \xrightarrow{U_A, U_B}$$

$$\frac{(U_A|0\rangle)(U_B|0\rangle) + (U_A|1\rangle)(U_B|1\rangle)}{\sqrt{2}} *$$

$$\frac{(U_A|0\rangle)(U_B|0\rangle) + (U_A|1\rangle)(U_B|1\rangle)}{\sqrt{2}}$$

$$= \frac{|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle}{2}$$

$$= |\beta_{00}\rangle |\beta_{00}\rangle$$

通过 Controlled-NOT-Gate 后的状态为

$$\xrightarrow{\text{Controlled-NOT-Gate}} \frac{|0000\rangle + |0011\rangle + |1111\rangle + |1100\rangle}{2}$$

$$= \frac{|00\rangle(|00\rangle + |11\rangle) + |11\rangle(|00\rangle + |11\rangle)}{2}$$

$$= \frac{|00\rangle + |11\rangle}{\sqrt{2}} \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$=|\beta_{00}\rangle\,|\beta_{00}\rangle$$

然后 A 和 B 测定各自第 2 位的 qubit，其结果一致的概率为 1。因此，双方共同拥有贝尔状态$|\beta 00\rangle$。

(2) 用户 A 和 B 的状态是$|\beta_{00}\rangle|\beta_{10}\rangle$场合

A 和 B 各自对自己拥有的 qubit 分别同时实施 U_A 演算或 U_B 演算：

$$|\beta_{00}\rangle\,|\beta_{10}\rangle \xrightarrow{U_A,\,U_B} \frac{(U_A|0\rangle)(U_B|0\rangle)+(U_A|1\rangle)(U_B|1\rangle)}{\sqrt{2}} * \frac{(U_A|0\rangle)(U_B|0\rangle)-(U_A|1\rangle)(U_B|1\rangle)}{\sqrt{2}}$$

$$=\frac{|0001\rangle-|0010\rangle+|1101\rangle-|1110\rangle}{2}$$

$$=|\beta_{00}\rangle\,|\beta_{11}\rangle$$

通过 Controlled-NOT-Gate 后的状态为

$$\xrightarrow{\text{Controlled-NOT-Gate}} \frac{|0001\rangle-|0010\rangle+|1110\rangle-|1101\rangle}{2}$$

$$=\frac{|00\rangle(|01\rangle-|10\rangle)-|11\rangle(|01\rangle+|10\rangle)}{2}$$

$$=\frac{|00\rangle-|11\rangle}{\sqrt{2}}\,\frac{|01\rangle-|10\rangle}{\sqrt{2}}$$

$$=|\beta_{10}\rangle\,|\beta_{11}\rangle$$

此时因为 A 和 B 测定各自第 2 位的 qubit，其结果不一致的概率为 1，所以破弃剩余的 qubit。

(3) 用户 A 和 B 的状态是$|\beta_{10}\rangle|\beta_{00}\rangle$场合

A 和 B 各自对自己拥有的 qubit 分别同时实施 U_A 演算或 U_B 演算：

$$|\beta_{10}\rangle\,|\beta_{00}\rangle \xrightarrow{U_A,\,U_B} \frac{(U_A|0\rangle)(U_B|0\rangle)-(U_A|1\rangle)(U_B|1\rangle)}{\sqrt{2}} * \frac{(U_A|0\rangle)(U_B|0\rangle)+(U_A|1\rangle)(U_B|1\rangle)}{\sqrt{2}}$$

$$=\frac{|0100\rangle+|0111\rangle-|1000\rangle-|1011\rangle}{2}$$

$$= |\beta_{11}\rangle\,|\beta_{00}\rangle$$

通过 Controlled-NOT-Gate 后的状态为

$$\xrightarrow{\text{Controlled-NOT-Gate}} \frac{|0101\rangle+|0110\rangle-|1010\rangle-|1001\rangle}{2}$$

$$= \frac{|01\rangle(|01\rangle+|10\rangle)-|10\rangle(|01\rangle+|10\rangle)}{2}$$

$$= \frac{|01\rangle-|10\rangle}{\sqrt{2}}\,\frac{|01\rangle+|10\rangle}{\sqrt{2}}$$

$$= |\beta_{11}\rangle\,|\beta_{01}\rangle$$

因为 A 和 B 测定各自第 2 位的 qubit，其结果不一致的概率为 1，所以破弃剩余的 qubit。

(4) 用户 A 和 B 的状态是$|\beta_{10}\rangle|\beta_{10}\rangle$场合

A 和 B 各自对自己拥有的 qubit 分别同时实施 U_A 演算或 U_B 演算：

$$|\beta_{10}\rangle\,|\beta_{10}\rangle \xrightarrow{U_A,\,U_B} \frac{(U_A|0\rangle)(U_B|0\rangle)-(U_A|1\rangle)(U_B|1\rangle)}{\sqrt{2}} *$$

$$\frac{(U_A|0\rangle)(U_B|0\rangle)-(U_A|1\rangle)(U_B|1\rangle)}{\sqrt{2}}$$

$$= \frac{|0101\rangle-|0110\rangle-|1001\rangle+|1010\rangle}{2}$$

$$= |\beta_{11}\rangle\,|\beta_{11}\rangle$$

通过 Controlled-NOT-Gate 后的状态为

$$\xrightarrow{\text{Controlled-NOT-Gate}} \frac{|0100\rangle+|0111\rangle-|1011\rangle-|1000\rangle}{2}$$

$$= \frac{|01\rangle(|00\rangle+|11\rangle)-|10\rangle(|00\rangle+|11\rangle)}{2}$$

$$= \frac{|01\rangle-|10\rangle}{\sqrt{2}}\,\frac{|00\rangle-|11\rangle}{\sqrt{2}}$$

$$= |\beta_{11}\rangle\,|\beta_{00}\rangle$$

因为 A 和 B 测定各自第 2 位的 qubit，其结果一致的概率为 1，但用户 A 和 B 共同拥有的却并非是所希望的状态$|\beta_{11}\rangle$。

无论如何，通过 QPA 协议配送后，A 和 B 拥有共同状态的概率：当 A 和 B 的接收状态是$|\beta_{00}\rangle|\beta_{00}\rangle$或$|\beta_{10}\rangle|\beta_{10}\rangle$时，其发生的概率为

$$(1-q)^2+q^2$$

另一方面，通过 QPA 协议配送后，在没有破弃 qubit 的情况下，A 和 B 共同拥有正确贝尔状态$|\beta_{00}\rangle$的概率为

$$\frac{(1-q)^2}{(1-q)^2+q^2}$$

从以上结果可知，与上一节讲述的 EPP 的基本协议一样，在 $0<q<\frac{1}{2}$ 范围内，通过 QPA 协议，A 和 B 双方能够共同拥有贝尔状态$|\beta_{00}\rangle$的概率比不作任何改进的 EPP 的基本协议要高。

例题 6.2　考虑从备制中心 C 到用户 A 和用户 B 的量子信道同是 bit 反转信道的情况。此时 A 和 B 的状态是状态集$\{|\beta_{00}\rangle|\beta_{00}\rangle, |\beta_{00}\rangle|\beta_{01}\rangle, |\beta_{01}\rangle|\beta_{00}\rangle, |\beta_{01}\rangle|\beta_{01}\rangle\}$中的某一个。如果用户 A 和 B 接收信息的状态是$|\beta_{00}\rangle|\beta_{00}\rangle$，那么情况与上述(1)的场合一样，双方共同拥有贝尔状态$|\beta_{00}\rangle$。

其次考虑用户 A 和 B 接收信息的状态是$|\beta_{00}\rangle|\beta_{01}\rangle$的情况，此时对状态作用 QPA 协议方法，在实施 U_A 演算或 U_B 演算后状态变化成

$$\begin{aligned}
|\beta_{00}\rangle|\beta_{01}\rangle &\xrightarrow{U_A,U_B} \\
&\frac{(U_A|0\rangle)(U_B|0\rangle)+(U_A|1\rangle)(U_B|1\rangle)}{\sqrt{2}}* \\
&\frac{(U_A|0\rangle)(U_B|1\rangle)+(U_A|1\rangle)(U_B|0\rangle)}{\sqrt{2}} \\
&=\frac{|0001\rangle+|0010\rangle+|1101\rangle+|1110\rangle}{2} \\
&=|\beta_{00}\rangle|\beta_{01}\rangle
\end{aligned}$$

再通过 Controlled-NOT-Gate 后的状态为

$$\begin{aligned}
&\xrightarrow{\text{Controlled-NOT-Gate}} \frac{|0001\rangle+|0010\rangle+|1110\rangle+|1101\rangle}{2} \\
&=\frac{|00\rangle(|01\rangle+|10\rangle)+|11\rangle(|01\rangle+|10\rangle)}{2} \\
&=|\beta_{00}\rangle|\beta_{01}\rangle
\end{aligned}$$

测定的结果不一致的概率为 1，因此破弃剩余的 qubit。同样，如果用户 A 和 B 接收信息的状态是$|\beta_{01}\rangle|\beta_{00}\rangle$时，也可以通过 QPA 协议确认破弃剩余的 qubit。

另一方面，如果用户 A 和 B 接收信息的状态是$|\beta_{01}\rangle|\beta_{01}\rangle$时，实施 U_A 演算或 U_B 演算后

$$|\beta_{01}\rangle|\beta_{01}\rangle \xrightarrow{U_A, U_B} \frac{(U_A|0\rangle)(U_B|1\rangle)+(U_A|1\rangle)(U_B|0\rangle)}{\sqrt{2}} * \frac{(U_A|0\rangle)(U_B|1\rangle)+(U_A|1\rangle)(U_B|0\rangle)}{\sqrt{2}}$$

$$= \frac{|0101\rangle+|0110\rangle+|1001\rangle+|1010\rangle}{2}$$

$$= |\beta_{01}\rangle|\beta_{01}\rangle$$

再通过 Controlled-NOT-Gate 其状态变为

$$\xrightarrow{\text{Controlled-NOT-Gate}} \frac{|0100\rangle+|0111\rangle+|1011\rangle+|1000\rangle}{2}$$

$$= \frac{|01\rangle(|00\rangle+|11\rangle)+|10\rangle(|00\rangle+|11\rangle)}{2}$$

$$= |\beta_{01}\rangle|\beta_{00}\rangle$$

测定结果一致的概率为 1。因此这种情况下双方共同拥有状态$|\beta_{01}\rangle$。从以上的结果可以看出对于 bit 反转信道在 QPA 协议适用的情况下，其效果与前一节讨论的基本 EPP 的效果是同样的。

6.3 EPP 的高效率化

以上讲述了使 A 和 B 双方共同拥有 1 个贝尔状态$|\beta_{00}\rangle$的最基本的方法 EPP。但是，利用 EPP 方法只能从 2 个 qubit 对中共同拥有 1 个贝尔状态，同时还可能伴随 qubit 对被破弃的情况，因此这些方法效率不高。本节讨论利用经典纠错编码的理论，从复数个纠缠状态中以高概率的方式使 A 和 B 双方共同拥有复数个$|\beta_{00}\rangle$状态的高效 EPP 的实现方法。

在以下的叙述中，为了简单起见，假设考虑从备制中心 C 到用户 A 以及到用户 B 之间的量子信道是可能以概率 p 发生 bit 反转的信道，并且用户 A 和 B 预计能够以较高概率共同拥有若干个贝尔状态$|\beta_{00}\rangle$。关于这个问题，对预计的若干个纠缠状态执行 QPA 协议就可以获得预期结果。

现在假设 A 和 B 的第 1 个 qubit 对来自于备制中心 C，第 2 个 qubit 对是备制好了的贝尔状态$|\beta_{00}\rangle$，因此 A 和 B 的 2 个 qubit 对的状态如下：

以概率 $(1-q)$ 为　　$|\beta_{00}\rangle|\beta_{00}\rangle$

以概率 q 为　　$|\beta_{01}\rangle|\beta_{00}\rangle$

A 和 B 再各自将自己拥有的 qubit 通过 Controlled-NOT-Gate，则得到的状态为

输入状态		输出状态
$\|\beta_{00}\rangle\|\beta_{00}\rangle$	→	$\|\beta_{00}\rangle\|\beta_{00}\rangle$
$\|\beta_{01}\rangle\|\beta_{00}\rangle$	→	$\|\beta_{01}\rangle\|\beta_{01}\rangle$
$\|\beta_{00}\rangle\|\beta_{01}\rangle$	→	$\|\beta_{00}\rangle\|\beta_{01}\rangle$
$\|\beta_{01}\rangle\|\beta_{01}\rangle$	→	$\|\beta_{01}\rangle\|\beta_{00}\rangle$

此后通过 Controlled-NOT-Gate 输出的状态仅有$|\beta_{00}\rangle$和$|\beta_0 1\rangle$两个，且从结果里可以看到只有当输入状态的第 1 个 qubit 对是$|\beta_{01}\rangle$时，第 2 个 qubit 对的状态才发生变化。

再进一步，如果输入状态是$|\beta_{00}\rangle|\beta_{00}\rangle$和$|\beta_{01}\rangle|\beta_{00}\rangle$其中之一时，若用户 A 和 B 的测定结果相等，则双方必定共同拥有贝尔状态$|\beta_{00}\rangle$；即使测定结果不相等，只要用户 A 和 B 双方中的某一方对自己拥有的 qubit 实施 bit 反转演算 X-Gate，双方就能够共同拥有贝尔状态$|\beta_{00}\rangle$。

为了讨论测定问题，首先假设用户 A 和 B 已共同拥有 3 个贝尔状态$|\beta_{00}\rangle$，再假设从备制中心 C 配送到用户 A 和 B 的 7 个贝尔状态中至多有 1 个贝尔状态发生 bit 反转（即实施了 bit 反转演算 X-Gate）。例如，假设 7 个贝尔状态$|\beta_{00}\rangle$中的第 2 个贝尔状态发生反转变化成为$|\beta_{01}\rangle$，此时 A 和 B 的共有状态为

$$|\beta_{00}\rangle|\beta_{01}\rangle|\beta_{00}\rangle|\beta_{00}\rangle|\beta_{00}\rangle|\beta_{00}\rangle|\beta_{00}\rangle \tag{6.2}$$

在这样的状态下，我们介绍使用 3 回测定或者说使用 3 个贝尔状态，获取 7 个贝尔状态$|\beta_{00}\rangle$的新方法。

首先着眼[7，4]Hamming 编码集合的同等校验矩阵

$$H=\begin{bmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{bmatrix}$$

在以上的假设条件下，用图 6.3 表示的方式对备制中心 C 配送来的 qubit 进行校验。因为同等校验矩阵 H 的第 1 行上值为 1 的位置是 4、5、6、7 列，就让从备制中心 C 配送过来的第 4、第 5、第 6 和第 7 位的 qubit 和纯粹的贝尔状态$|\beta_{00}\rangle$一方的 qubit（图 6.3 中从下往上数第 3 位 qubit）顺序地通过 Controlled-NOT-Gate。然后 A 和 B 以$\{|0\rangle，|1\rangle\}$为基底测定从下往上数第 3 位 qubit。此

时因为测定之前的状态是$|\beta_{00}\rangle$，所以 A 和 B 的测定结果完全一致的概率是 1。这个结果显示，与从备制中心 C 接收到的 qubit 列中至多仅有 1 个发生 bit 反转错误的假设里，显然可以知道从第 4 位到第 7 位的 qubit 对的状态全部都是$|\beta_{00}\rangle$。

又因为同等校验矩阵 H 的第 2 行上值为 1 的位置是 2、3、6、7 列，让从备制中心 C 送过来的第 2 位、第 3 位、第 6 位和第 7 位的 qubit 和纯粹的贝尔状态$|\beta_{00}\rangle$一方的 qubit（图6－3 中从下往上第 2 位 qubit）顺序地通过 Controlled-NOT-Gate。然后 A 和 B 再以$\{|0\rangle, |1\rangle\}$为基底测定从下往上数的第 2 位 qubit，此时因为测定之前的状态是$|\beta_{01}\rangle$，所以 A 和 B 的测定结果完全不一致的概率是 1。这个结果，与从备制中心 C 接收到的 qubit 列中至多仅有 1 个发生 bit 反转错误的假设比较中，可以知道接收到的信息中的第 2 位、第 3 位、第 6 位和第 7 位的 qubit 对中，其中有一个状态是$|\beta_{01}\rangle$，其余的都是状态$|\beta_{00}\rangle$。

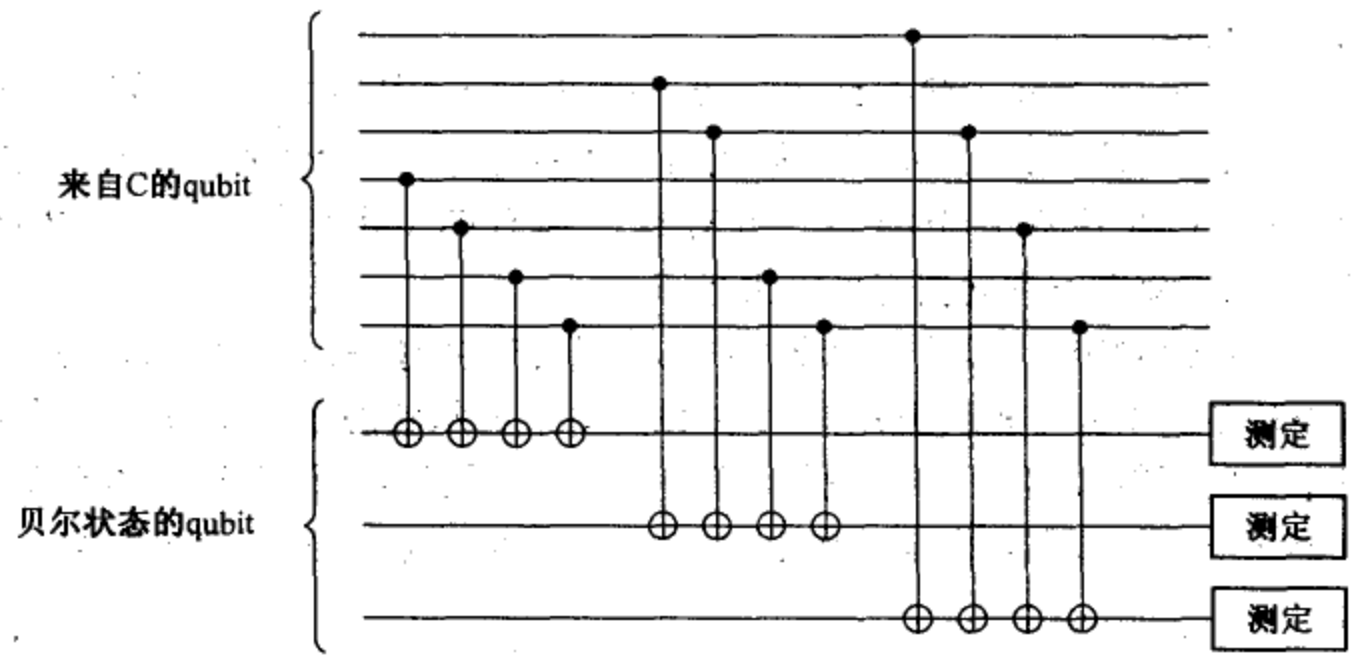


图 6－3　用户 A 以及 B 的操作

最后同等校验矩阵 H 的第 3 行上值为 1 的位置是 1、3、5、7 列，让从备制中心 C 送过来的第 1 位、第 3 位、第 5 位和第 7 位的 qubit 和纯粹的贝尔状态$|\beta_{00}\rangle$一方的 qubit（图 6.3 中的最下一位 qubit）顺序地通过 Controlled-NOT-Gate。然后 A 和 B 再以$\{|0\rangle, |1\rangle\}$为基底测定最下一位 qubit，此时因为测定之前的状态是$|\beta_{00}\rangle$，所以 A 和 B 的测定结果完全一致的概率是 1。这个结果意味着第 1 位、第 3 位、第 5 位和第 7 位的 qubit 对的状态全部是$|\beta_{00}\rangle$。从以上的讨论可以看到，在接收到的 qubit 列中仅有第 2 位 qubit 对的状态是$|\beta_{01}\rangle$，其他的 qubit 对的状态都是$|\beta_{00}\rangle$。因此，如果 A 对第 2 位 qubit 对实施 bit 反转演算 X-Gate，则 7 个 qubit 对就全部成为贝尔状态$|\beta_{00}\rangle$。

利用纠错编码校验出错 qubit 对的方法，能够与纠错编码的解码方法连接起来。例如，假设将 A 和 B 的测定结果一致与否用数值 1 和 0 表示：不一致时

设为 1，一致时设为 0。以上例为例，将得到矢量(010)。这个结果与第 2 位 qubit 发生错误时 Hamming 编码的伴随式相同，与发生错误的 qubit 对的位置是一致的。因此，把从测定结果得到的矢量看成是伴随式，即可判断出与出错位置对应的 qubit 对是$|\beta_{01}\rangle$。

使用这个协议，能够在至多一个 qubit 对发生错误的情况下，共有 7 个贝尔状态$|\beta_{00}\rangle$，假设量子信道上的出错率为 $p = 0.1$，则让 A 与 B 共同拥有 7 个贝尔状态$|\beta_{00}\rangle$的概率是

$$0.9^7 + 7 \times 0.1 \times 0.9^8 = 0.8503$$

这个协议还可以更加一般化。因为这里仅使用了能够订正一个错误的 Hamming 编码。如果使用更长的编码，使用能够订正更多错误的编码体系，就有可能实现更高效率的 EPP。另外，在复数个错误发生的情况下也可将对应测定结果的矢量看成是伴随式，并注意到利用这种方法可检查出出错的 qubit 对。

第 7 章 量子信道与量子信道容量

我们研究信道的目的是要讨论信道中平均每个符号所能传送的信息量，即信道的信息传输率 R。经典信息论中的平均互信息 $I(X;Y)$就是表示接收到符号 Y 后平均每个符号获得的关于 X 的信息量。因此信道的信息传输率就是平均互信息，即

$$R = I(X;Y) = H(X) - H(X \mid Y) \quad \text{(bit/符号)}$$

有时我们所关心的是信道在单位时间内平均传输的信息量。若平均传输一个符号需要 t 秒钟，则信道每秒钟平均传输的信息量为

$$R_t = \frac{1}{t} I(X;Y) = \frac{1}{t} H(X) - \frac{1}{t} H(X \mid Y) \quad \text{(bit/s)}$$

一般称此为信息传输速率。

我们知道，在经典信息论中，$I(X;Y)$是输入随机变量 X 的概率分布 $p(x)$的凸函数。因此，对于一个固定的信道，总存在一种信源(某种概率分布 $p(x)$)，使传输每个符号平均获得的信息量最大，也就是每个固定信道都有一个最大的信息传输率。定义这个最大的信息传输率为信道容量 C，即

$$C = \max_{p(x)} \{I(X;Y)\}$$

其单位是比特/符号或奈特/符号，而相应的输入概率分布称为最佳输入分布。若平均传输一个符号需要 t 秒钟，则信道单位时间内平均传输的最大信息量为

$$C_t = \frac{1}{t} \max_{p(x)} \{I(X;Y)\} \quad \text{(bit/s)}$$

一般仍称 C_t 为信道容量，增加一个下标 t 以示区别。

信道容量 C 与已输入信源的概率分布无关，它只是信道传输概率的函数，只与信道的统计特性有关。所以，信道容量是完全描述信道特性的参量，是信道能够传输的最大信息量。对于一般信道，信道容量的计算相当复杂。从数学上来说，就是对互信息 $I(X;Y)$求极大值的问题。下面从经典信息论有关信道容量的一些结论出发探讨量子信道与量子信道容量的一些问题，并给出相应的

结果。

7.1　从量子比特到经典比特

第一章到第六章讲述了量子信息与量子计算的诸多概念，例如量子信道的 qubit 传送方式、量子高密度编码的方法、量子信息的瞬间传送（Teleportation 离物传态）、量子纠错编码的原理与构造等内容。现在让我们回过头来再看一看这些概念，如今人们走进了信息化的时代，人们生活、娱乐、工作空间的每一个角落无处不存在着垂手可得的信息，这些信息的表示、存储、处理和传送都是基于经典信息理论的基础之上，表述信息字符量（不是信息量）的大小至今为止依然基于 bit 度量，用 bit 表示，因为我们还没有建立起使用 qubit 表示信息量的完整体系。另一方面，利用 qubit 表示的具有代表性的量子信息是为了量子计算机的演算，是我们无法直接操作的信息，因此通过量子信道传送的信息，在量子计算机还没有实用化之前的一段时间内，依然是用 qubit 表示的经典信息 bit 而非真正的量子信息 qubit。

从上述的观点看，到目前为止讲述的量子信道传输方式中究竟哪些东西是有用的？首先让经典比特 0 对应状态 $|0\rangle$、1 对应状态 $|1\rangle$，因此 1 个 qubit 至少能够表示 1 个 bit 的信息，也至少能够传送 1 个 bit 的信息。另外，在第三章中讲述了利用 1 个 qubit 仅能够传送 1 个 bit 的信息的信息量；而在 3.4 的量子瞬间传递（Teleportation 离物传态）中，讲述了利用量子瞬间传递技术传送 1 个 qubit 的协议，因此利用量子瞬间传递能够传送 1 个 bit。但根据量子瞬间传递协议，借助经典信道实现传送 1 个量子 qubit 信息，每一次都要通过传送 2 个经典 bit 信息来完成。也就是说即使是传送 1 个 bit 信息也要发送 2 个 bit 的信号，显然对于 bit 的传送来说该协议效率是极低的。

其次再考虑量子纠错编码。第五章中讲述的 CSS 编码方法，是将 1 个 qubit 源码转换成 7 个 qubit 的编码。若将该方法应用于经典 bit 的传送，那么 1 个 bit 就要转换成 7 个qubit。但是如果将有关量子信道的通信实体仅限于 bit 的传送，则与此比较显然还存在着更高效且更单纯的编码方法。利用第四章介绍的重复码，例如将 1 个 bit 转换成 3 个qubit的编码方式。考虑下式的编码方法：

送信 bit 源码		编码
0	→	$\|000\rangle$
1	→	$\|111\rangle$

(7.1)

对应的解码方法是以

$$\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$$

为基底测定接收到的 3 位 qubit，根据测定结果中包含的 0 和 1 个数的多少推定发送的信息。也就是说解码方法由下列约定决定：

接收的代码　　发送的信息

$$\left.\begin{array}{l}|000\rangle\\|001\rangle\\|010\rangle\\|100\rangle\end{array}\right\} \rightarrow \quad 0$$

$$\left.\begin{array}{l}|011\rangle\\|101\rangle\\|110\rangle\\|111\rangle\end{array}\right\} \rightarrow \quad 1$$

根据该解码方法，如果测定的结果是$|011\rangle$的话，则判断发送的信息是 bit 值 1。

在执行这样编码的情况下，我们可以很容易地确认该编码能够同时订正由于量子信道引发的 1 个以下的 bit 反转错误和 3 个以下的位相翻转错误。因此，与第四章讲述的 CSS 编码方法比较，显然它能够订正更多的错误，并且 1 个 bit 仅用 3 个 qubit 表示的编码也有较高效率。

例题 7.1　把 bit 1 用式(7.1)编码，将$|111\rangle$送入量子信道。在信道中假设第一个 qubit 上发生 bit 反转，第 2 位和第 3 位 qubit 上发生位相翻转错误。此时接收的信息状态是

$$(X|1\rangle)(Z|1\rangle)(Z|1\rangle) = (|0\rangle)(-|1\rangle)(-|1\rangle) = |011\rangle$$

测定接收到的信息状态是$|011\rangle$，因此解码器推定发送的信息是 1。

假设在量子信道上传送经典 bit 信息，并假设出错率任意小，此时能够以什么样的方式用 bit 和 qubit 之比决定信道的传送速率呢？再者，此任意小的出错率能够达到的传送速率的界限又是多少？本章以下部分将考察这些基本问题。

7.2　经典信道与信道编码定理

经典无记忆单符号离散信道 W，当给定输入变量为 X 取值有限字母集合 $\{a_1, \cdots, a_r\}$、输出变量为 Y 取值有限字母集合 $\{b_1, \cdots, b_s\}$ 时，从 X 到 Y 的概率迁移(传递概率)由下式

$$P(y|x)=P(y=b_j|x=a_i)=P(b_j|a_i)\quad (i=1,\cdots,r;\ j=1,\cdots,s)$$

完全决定。很显然，对于任意的 $a_i\in X$ 以及 $b_j\in Y$，以下不等式成立：

$$0\leqslant P(b_j\mid a_i)\leqslant 1\quad (i=1,\cdots,r;\ j=1,\cdots,s)$$

因为信道中有干扰(噪声)存在，若信道输入为 $x=a_i$ 时输出是哪一个符号 y 事先无法确定，但信道输出一定是 b_1，b_2，…，b_s 中的一个，即对任意 $a_i\in X$，以下的等式显然成立：

$$\sum_{j=1}^{s}P(b_j\mid a_i)=1\quad (i=1,\cdots,r)$$

由于信道的干扰使输入符号 x 在传输中发生错误，所以可以用传递概率 $P(b_j|a_i)$ $(i=1,\cdots,r;\ j=1,\cdots,s)$来描述干扰影响的大小。因此，一般简单的单符号离散信道的数学模型可以用概率空间$[X,\ P(y|x),\ Y]$加以描述。

例题 7.2　设输入与输出的字母集合同是$\{0,\ 1\}$，由以下迁移概率

$$P(0\mid 0)=P(1\mid 1)=1-\varepsilon$$

$$P(1\mid 0)=P(0\mid 1)=\varepsilon$$

决定的无记忆单符号离散信道称作为二元对称信道(图 7-1)。

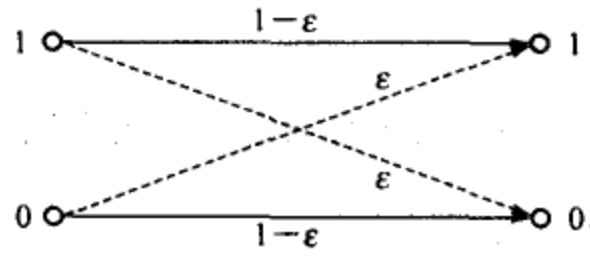


图 7-1　二元对称信道

以下就经典信息论中与信道容量有关的概念作一简单介绍。

无记忆信道定义为：当将一长度为 n 的输入列送入信道

$$X=x_1x_2\cdots x_n\in X^n$$

即发送信息 X 时，信道的输出序列

$$Y=y_1y_2\cdots y_n\in Y^n$$

由以下概率给出：

$$P^n(Y\mid X)=\prod_{i=1}^{n}P(y_i\mid x_i)$$

也就是说在某一时刻 i 输出的 y_i 仅依赖于输入 x_i 并由此决定，与时刻 i 之前以

及之后的输入 x_i 以及输出 $y_j(j \neq i)$ 均无关。

信息的编码定义为:将包含 M 种类信息集合 $M=\{1, 2, \cdots, M\}$ 中的每一个信息 m 都映射成信道输入字母集合 $X=\{a_1, \cdots, a_r\}$ 上的一个长度为 n 的序列,即信息编码由映射 ϕ 定义

$$\phi: M \to X^n$$

此时称 $\phi(m)$为信息 $m(\in M)$的编码。称

$$R=\frac{1}{n}\log M$$

为信息的编码率(rate)或称为传送速率。

另一方面,当某一个信息编码通过信道发送时,基于信道输出的长度为 n 的信息序列状态推断出发送的信息是属于 M 中的哪个信息的过程称为解码。一般性的解码由映射 φ 定义

$$\varphi: Y^n \to M$$

通常称编码与解码对(ϕ, φ)为代码。

在这里,把与信息 m 的编码以及送入信道行为无关的仅由信道产生的错误,经过解码得到的结果却有别于 m 信息的概率

$$P_r\{\varphi(\phi(m)) \neq m\}$$

称为对信息 m 的错误率。特别当所有的信息等概率发生时,错误率的均值

$$P_e=\frac{1}{M}\sum_{m\in M}P_r\{\varphi(\phi(m)) \neq m\}$$

被称为解码错误率。

有关信道编码的问题可以解说为,在编码长度 n 足够大,解码错误率任意小的条件下传送速率 R,即平均每个符号携带的信息量究竟能够有多大,给出传送速率 R 的界限就解决了信道编码问题。为了讲解有关这个问题最基本的成果,下面首先讲解信道的信道容量。

假设给定具有迁移概率 $P(b|a)(a\in X, b\in Y)$的信道 W,并假设输入字母集合 X 的符号 a 以概率 $\pi(a)$出现。此时互信息量 $I(\pi; W)$由下式决定:

$$I(\pi; W)=\sum_{a\in X}\sum_{b\in Y}\pi(a)P(b\mid a)\log\frac{P(b\mid a)}{\sum_{a\in X}\pi(a)P(b\mid a)} \tag{7.2}$$

进一步,在 X 上取不同的概率分布 π 得到的互信息量的最大值定义为信道 W 的信道容量即信道传输率 $C(W)$。即

$$C(W) = \max_{\pi} I(\pi; W)$$

注意，这里信道容量 $C(W)$ 仅仅依赖于信道的迁移概率 $P(b|a)$，并由此决定。

定理 7.1（信道编码定理）　设离散无记忆信道 $[X, P(y|x), Y]$，$P(y|x)$ 为信道迁移概率，其信道容量为 $C(W)$，如果信息传送速率 R 满足下列不等式：

$$R < C(W)$$

当编码长度 n 足够大时，一定存在解码错误率 P_e 能够任意小的代码体系（总可以在输入 X^n 符号集中找到 $M(=2^{nR})$ 个码字组成的一组码 $(2^nR, n)$ 和相应的解码规则，使解码错误率 P_e 能够任意小）。反之，如果

$$R > C(W)$$

则无论采用什么样的编码，当编码长度 n 足够大时，解码错误率 P_e 渐近于 1。

信道编码定理指出，如果传送速率严格地小于信道容量，在增加代码长度的情况下能够以任意小的错误率传送信息。定理 7.1 告诉我们，如果实施编码，虽然编码将导致延迟或计算量的增加，但这非但没有降低传送速率还因此而获得高品质高信赖性的通信。该定理没能预测到它会对 20 世纪后半叶独树一帜的数字通信以及数字记录产生如此巨大的影响。

例题 7.3　求解例题 7.2 中讲述的二元对称信道 W 的信道容量。假设 $\pi(0) = p$，$\pi(1) = 1-p$，用式(7.2)计算互信息量 $I(\pi; W)$ 得到

$$\begin{aligned} I(\pi; W) = {} & p(1-\varepsilon)\log\frac{1-\varepsilon}{p(1-\varepsilon)+(1-p)\varepsilon} + \\ & (1-p)\varepsilon\log\frac{\varepsilon}{p(1-\varepsilon)+(1-p)\varepsilon} + \\ & p\varepsilon\log\frac{\varepsilon}{(1-\varepsilon)(1-p)+p\varepsilon} + \\ & (1-p)(1-\varepsilon)\log\frac{1-\varepsilon}{(1-\varepsilon)(1-p)+p\varepsilon} \\ = {} & -(p+\varepsilon+2p\varepsilon)\log(p+\varepsilon+2p\varepsilon) - \\ & (1-p-\varepsilon+2p\varepsilon)\log(1-p-\varepsilon+2p\varepsilon) + \\ & \varepsilon\log\varepsilon + (1-\varepsilon)\log(1-\varepsilon)。 \end{aligned}$$

对该式作关于 p 的微分，得到 $I(\pi; W)$ 在 $p = \frac{1}{2}$ 时取得最大值

$$1 + \varepsilon\log\varepsilon + (1-\varepsilon)\log(1-\varepsilon)$$

因此二元对称信道 W 的信道容量为

$$C(W) = \max_{\pi} I(\pi, W)$$
$$= 1 + \varepsilon\log\varepsilon + (1-\varepsilon)\log(1-\varepsilon)$$

7.3 量子信息源与冯·诺依曼熵(entropy)

在讲解量子信道之前,这一节作为准备知识我们先讲解量子信息源与冯·诺依曼熵的有关概念。

在上一节中定义了经典的二元无记忆信息源:即比特 0 和比特 1 各自以概率 p 和 $1-p$ 独立发生,且当前输出与过去无关的二元信息源。

与此对应定义二元量子无记忆信息源:让量子比特$|a\rangle$与量子比特$|b\rangle$替代比特 0 与比特 1,

$$|a\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}, \quad |b\rangle = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$$

且各自以概率 p 和 $1-p$ 独立发生,且当前输出与过去无关的量子信息源称为二元量子无记忆信息源。

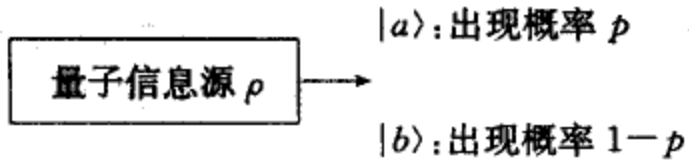


图 7-2 量子信息源

下面说明量子信息源的密度算子。

我们将量子比特$|a\rangle$与量子比特$|b\rangle$各自以概率 p 和 $1-p$ 发生的量子信息源用被称为密度算子的 2×2 矩阵表示

$$\rho = p\,|a\rangle\langle a| + (1-p)\,|b\rangle\langle b|$$

其中$\langle a|$是 $ket|a\rangle$(右矢)的共轭转置,被称为 bra(左矢)。即如果 $|a\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$,则$\langle a| = [a_1^* \quad a_2^*]$。

例题 7.4 量子信息源 S 的两个 qubit

$$|a\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |b\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

且各自以概率 p 和 $1-p$ 输出，此时的量子信息源 S 的密度算子为

$$\rho = p\begin{bmatrix}1\\0\end{bmatrix}[1 \quad 0]+(1-p)\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}\left[\frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{2}}\right]$$

$$= \begin{bmatrix}\frac{1+p}{2} & \frac{1-p}{2}\\ \frac{1-p}{2} & \frac{1-p}{2}\end{bmatrix}$$

以上考虑了输出 2 种 qubit 的二元量子信息源，用同样的方法我们能够考虑输出 r 种类 qubit 的 r 元量子信息源。一般情况下，在 r 元量子信息源的场合，我们把 qubit 考虑成 r 维的复数矢量，同时密度算子为 $r\times r$ 矩阵。

在量子信息源中与香农熵对应的概念是下面介绍的冯·诺依曼熵。

假设对应于 r 元量子信息源的密度算子为 ρ，ρ 的固有（本征）值为 λ_1，λ_2，…，λ_r（其中重复的固有值按重复的次数计数），则冯·诺依曼熵被定义为

$$H(\rho) = -\sum_{i=1}^{r}\lambda_i \log\lambda_i \tag{7.3}$$

例题 7.5　试求两个 qubit

$$|a\rangle = \begin{bmatrix}1\\0\end{bmatrix},\ |b\rangle = \begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}$$

等概率发生的量子信息源 S 的冯·诺依曼熵。这个信息源的密度算子 ρ 为

$$\rho = \frac{1}{2}\begin{bmatrix}1\\0\end{bmatrix}[1 \quad 0]+\frac{1}{2}\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}\left[\frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{2}}\right]$$

$$= \begin{bmatrix}\frac{3}{4} & \frac{1}{4}\\ \frac{1}{4} & \frac{1}{4}\end{bmatrix}$$

求解 ρ 的固有值。

我们从

$$\det\begin{bmatrix}\frac{3}{4}-\lambda & \frac{1}{4}\\ \frac{1}{4} & \frac{1}{4}-\lambda\end{bmatrix}=0$$

得到1个二次方程式

$$\lambda^2-\lambda+\frac{1}{8}=0$$

解方程得到 ρ 的两个固有值

$$\lambda_1=\frac{2-\sqrt{2}}{4},\ \lambda_2=\frac{2+\sqrt{2}}{4}$$

因此冯·诺依曼熵为

$$H(\rho)=-\frac{2-\sqrt{2}}{4}\log\left(\frac{2-\sqrt{2}}{4}\right)-\frac{2+\sqrt{2}}{4}\log\left(\frac{2+\sqrt{2}}{4}\right)\approx 0.6009$$

另外,0 和 1 等概率发生的经典信息源的香农熵为 1,由此得知冯·诺依曼熵小于香农熵。

例题 7.6 试求相互直交的两个 qubit

$$|a\rangle=\begin{bmatrix}1\\0\end{bmatrix},\ |b\rangle=\begin{bmatrix}0\\1\end{bmatrix}$$

各自以概率 p 和 $1-p$ 发生的量子信息源的冯·诺依曼熵。这个信息源的密度算子 ρ 为:

$$\rho=p\begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix}+(1-p)\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix}$$

$$=\begin{bmatrix}p & 0\\0 & 1-p\end{bmatrix}$$

很显然 ρ 的固有值为 p 和 $1-p$,因此冯·诺依曼熵为

$$H(\rho)=-p\log(p)-(1-p)\log(1-p)$$

这与 0 和 1 各自以概率 p 和 $1-p$ 发生的经典信息源的香农熵是一致的。

由以上的两个例题讨论我们可以推断出以下的结论,两个 qubit 各自以概率 p 和 $1-p$ 发生的量子信息源的冯·诺依曼熵,一般情况下小于等于香农熵,即有以下不等式成立:

$$H(\rho) \leqslant -p\log(p) - (1-p)\log(1-p)$$

7.4　量子信道与量子信道容量

本节先说明量子信道与量子信道容量，然后讲述量子信道编码定理。

量子信道有若干种类型(模型)。这里我们介绍一种最常利用的模型，该模型描述的是：依赖输入序列的输出序列、其分布是变化的量子信息源的量子信道。也就是说该模型拥有作为输入的字母集合是量子比特有限集合 X：

$$X = \{|a_1\rangle, |a_2\rangle, \cdots, |a_N\rangle\}$$

作为输出的字母集合是量子比特有限集合 Y：

$$Y = \{|b_1\rangle, |b_2\rangle, \cdots, |b_N\rangle\}$$

的(无记忆)量子信道 Q。Q 定义为：将 $|a\rangle \in X$ 送入信道，将信道的输出看成是由密度算子 $\rho(|a\rangle)$ 完全决定的量子信息源的输出，满足该条件的量子信道 Q 称为(无记忆)量子信道。

例题 7.7　假设输入输出的字母集合 X 与 Y 均为 $\{|a\rangle, |b\rangle\}$，由输出的密度算量子

$$\rho(|a\rangle) = |a\rangle\langle b| \text{ 以及 } \rho(|b\rangle) = |b\rangle\langle b|$$

决定的量子信道被称为无噪声信道。在这个信道上被输入的 qubit $|a\rangle$ 或者 qubit $|b\rangle$ 将按原样输出。

另外在第四章中介绍了 bit 反转信道，该信道在密度算子

$$\rho(|a\rangle) = (1-\varepsilon)|a\rangle\langle a| + \varepsilon|b\rangle\langle b|$$

$$\rho(|b\rangle) = (1-\varepsilon)|b\rangle\langle b| + \varepsilon|a\rangle\langle a|$$

决定下的一般化信道被称为是二元对称信道。该信道在 $|a\rangle = |0\rangle$，$|b\rangle = |1\rangle$ 时就是通常的 bit 反转信道。因为该信道中 qubit $|a\rangle$ 与 qubit $|b\rangle$ 以概率 $1-\varepsilon$ 正确输出、以概率 ε 错误输出，所以该信道能够看成是例题 7.2 的二元对称信道的量子版本。

量子信道 Q 的信道编码映射 ϕ 的定义：映射 ϕ 是从包含 M 种信息集合 $M = \{1, 2, \cdots, M\}$ 中的信息 m 到 X 上长度为 n 的 qubit 序列上的映射。与经典信道编码同样的道理，这个编码的传送速率由

$$R = \frac{1}{n}\log M$$

决定。在解码上也与经典信道解码体系相同，映射 φ 将由基于信道输出长度为 n 的 qubit 密度算子到属于 M 信息上的映射决定。我们称这样的编码与解码对 (ϕ, φ) 为代码体系。解码的出错率由

$$p_e = \frac{1}{M}\sum_{m\in M} p_r\{\varphi(\rho^n(\phi(m))) \neq m\}$$

决定。其中 $\rho^n(\phi(m))$ 表示长度为 n 的信道输入序列 $\phi(m)$ 与输出序列的密度算子。

下面来定义量子信道 Q 的信道容量。假设信道 Q 的输入字母集合 X 为

$$X = \{|a_1\rangle, |a_2\rangle, \cdots, |a_N\rangle\}$$

对应 $|a_i\rangle$ 输入将其信道的输出视为信息源的输出，其密度算子用 ρ_i 表示。此时如果利用 X 上的概率分布 $\pi(i)$ 求出 ρ_i 的平均值，则均值为

$$\bar{\rho} = \sum_{i=1}^{N}\pi(i)\rho_i$$

这个结果与以概率 $\pi(i)$ 将 $|a_i\rangle$ 输入信道，把信道的输出看成是由密度算子 $\rho(|a\rangle)$ 完全决定的量子信息源输出的均值 $\bar{\rho}$ 相等。与经典信息论中的互信息量的对应关系由下列等式给出：

$$\Delta H(\pi, Q) = H(\bar{\rho}) - \sum_i \pi(i)H(\rho_i)$$

其中 $H(\cdot)$ 表示冯·诺依曼熵。量子信道容量 C 被定义为取对应于 $\Delta H(\pi, Q)$ 的输入字母集合上的概率分布最大值，即

$$C(Q) = \max_{\pi}\Delta H(\pi, Q)$$

下面的定理是量子信息理论中最基本的内容。

定理 7.2 （量子信道编码定理）设离散无记忆量子信道 $[X, \rho(|a\rangle), Y]$ 的输出由密度算子 $\rho(|a\rangle)$ 完全决定，信道容量为 $C(Q)$。如果传送速率满足不等式：

$$R < C(Q)$$

当编码长度 n 足够大时，一定存在解码错误率 p_e 能够任意小的代码体系。反之，如果

$$R > C(Q)$$

则无论采用什么样的编码，当编码长度 n 足够大时，解码错误率 p_e 渐近于 1。

例题 7.8　考虑给定输入输出的字母集合为 $X = Y = \{|a\rangle, |b\rangle\}$ 的无噪声信道。此时，因为输入的状态能够原样地输出，所以密度算子一定为

$$\rho(|a\rangle) = |a\rangle\langle a|, \rho(|b\rangle) = |b\rangle\langle b|$$

假设输入字母集合上的概率分布为 $\pi(a) = p$，$\pi(b) = 1-p$，则密度算子的均值为

$$\bar{\rho} = p|a\rangle\langle a| + (1-p)|b\rangle\langle b|$$

这个结果与 qubit$|a\rangle$和 qubit$|b\rangle$各自以概率 p 和 $1-p$ 输出的量子信息源的密度算子是一致的。

再者，因为 ρ_a 与 ρ_b 的固有值同是 0 和 1，所以

$$H(\rho_a) = H(\rho_b) = 0$$

成立。如果注意到这一点，即上面等式成立的同时就能得到下面等式也成立：

$$\Delta H(\pi, Q) = H(\bar{\rho})$$

因此下面的等式自然也成立：

$$C(Q) = \max_{\pi} H(\bar{\rho}) = \max_{0 \leqslant p \leqslant 1} H(\bar{\rho})$$

此时该量子信道的信道容量与输出 qubit$|a\rangle$和 qubit$|b\rangle$在信息源上可达到的最大冯·诺依曼熵值相等。在以上假设条件成立的情况下，有关经典无噪声信道 W 的 $H(Y|X) = 0$，这与下列等式的成立是对应的：

$$C(W) = \max H(X)$$

特别当 $|a\rangle = |0\rangle$、$|b\rangle = |1\rangle$，均值为

$$\bar{\rho} = \begin{bmatrix} p & 0 \\ 0 & 1-p \end{bmatrix}$$

时，有

$$C(Q) = \max_{0 \leqslant p \leqslant 1} (-p\log p - (1-p)\log(1-p)) = 1$$

因此能够无错误传送的最高传送速率将是 1bit/qubit。

例题 7.9　考虑给定输入与输出的字母集合同时为 $X = Y = \{|0\rangle, |1\rangle\}$ 的 bit 反转信道。该信道上$|0\rangle$输入时其输出的密度算子为 ρ_0：

$$\rho_0 = (1-\varepsilon)|0\rangle\langle 0| + \varepsilon|1\rangle\langle 1|$$

$$= \begin{bmatrix} 1-\varepsilon & 0 \\ 0 & \varepsilon \end{bmatrix}$$

同样$|1\rangle$输入时其输出的密度算子为ρ_1：

$$\begin{aligned} \rho_1 &= \varepsilon |0\rangle\langle 0| + (1-\varepsilon)|1\rangle\langle 1| \\ &= \begin{bmatrix} \varepsilon & 0 \\ 0 & 1-\varepsilon \end{bmatrix} \end{aligned}$$

假设输入集合上的概率分布为$\pi(0) = p$，$\pi(1) = 1-p$，则得到的密度均值为

$$\begin{aligned} \bar{\rho} &= p\rho_0 + (1-p)\rho_1 \\ &= (p+\varepsilon-2\varepsilon p)|0\rangle\langle 0| + (1-p-\varepsilon+2\varepsilon p)|1\rangle\langle 1| \\ &= \begin{bmatrix} p+\varepsilon-2\varepsilon p & 0 \\ 0 & 1-p-\varepsilon+2\varepsilon p \end{bmatrix} \end{aligned}$$

这个结果与$|0\rangle$和$|1\rangle$各自以概率$p+\varepsilon-2\varepsilon p$和$1-p-\varepsilon+2\varepsilon p$发生的量子信息源的密度算子是一致的。

再者通过简单的计算能够得到以下等式：

$$H(\rho_0) = H(\rho_1) = -\varepsilon\log\varepsilon - (1-\varepsilon)\log(1-\varepsilon)$$

以及

$$\begin{aligned} H(\bar{\rho}) = &-(p+\varepsilon-2\varepsilon p)\log(p+\varepsilon-2\varepsilon p) \\ &-(1-p-\varepsilon+2\varepsilon p)\log(1-p-\varepsilon+2\varepsilon p) \end{aligned}$$

的成立。根据定义计算得到

$$\begin{aligned} \Delta H(\pi, Q) = &-(p+\varepsilon-2\varepsilon p)\log(p+\varepsilon-2\varepsilon p) \\ &-(1-p-\varepsilon+2\varepsilon p)\log(1-p-\varepsilon+2\varepsilon p) \\ &+\varepsilon\log\varepsilon + (1-\varepsilon)\log(1-\varepsilon) \end{aligned}$$

对$\Delta H(\pi, Q)$作关于p的微分得知$\Delta H(\pi, Q)$在$p=1/2$时取得最大值，所以量子信道容量为

$$\begin{aligned} C(Q) &= \max_{\pi} \Delta H(\pi, Q) \\ &= 1 + \varepsilon\log\varepsilon + (1-\varepsilon)\log(1-\varepsilon) \end{aligned}$$

这种情况下的量子信道与有误码率ε的二元对称经典信道的信道容量是一致的。但是在输入集合的二元状态非直交的情况下量子二元对称信道的信道容量与二元对称经典信道的信道容量是不一致的。

本章节在有关量子信道容量上，揭示了能够达到任意小错误率的传送速率界限为量子信道容量。但是，接近量子信道容量传送速率的、达到任意小出错率的具体的编码方法仍然是未知的，还有待今后的研究。

参 考 文 献

[1] A. K. Ekert. Quantum cryptography based on Bell's theorem. Physical Review Letters, vol. 67, pp. 661～663, 1991

[2] A. K. Ekert, C. Macchiavello. Error correction in quantum communication. Physical Review Letters, vol. 77, pp. 2585～2588, 1996

[3] A. M. Steane. Error correcting codes in quantum theory. Physical Review Letters, vol. 77, pp. 793～797, 1996

[4] A. Peres. Quantum Theory: Concepts and Methods. Kluwer Academic publisher, 1995

[5] A. R. Calderbank, P. W. Shor. Good quantum error-correcting codes exist. Physical Review A, vol. 54, no. 2, pp. 1098～1105, Aug. 1996

[6] A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane. Quantum error correction and orthogonal geomrtry. Physical Review Letters, vol. 78, pp. 405～408, 1997

[7] A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane, Quantum error correction via codes over GF(4). IEEE. Trans. IT, vol. 44, no. 4, pp. 1369～1387, 1998

[8] A. S. Holevo. Statistical problems in quantum physics. Proceedings of the second Japan-USSR Symposium on probability theory. Lecture Notes in Mathematics, vol. 330, pp. 104～119, Springer-Verlag, 1973

[9] A. S. Holevo. Capacity of a quantum communications channel. Problems of Information Transmission, vol. 5, no. 4, pp. 247～253, 1979

[10] A. S. Holevo, The capacity of the quantum channel with general states. IEEE. Trans. IT, vol. 44, no. 1, pp. 269～273, 1998

[11] A. S. Holevo. Reliability function of general classical-quantum channel. IEEE. Trans. IT, vol. 46, pp. 2256～2261, 2000

[12] A. Winter. Coding Theorems of Quantum Information Theory. Ph. D. thesis. University of Bielefeld, Germany, 1999

[13] B. Schumacher. Quantum coding. Physical Review A, vol. 51, no. 4, pp. 2738～2747, 1995

[14] B. Schumacher, M. D. Westmoreland. Sending classical information via noisy quantum channels. Physical Review A, vol. 56, no. 1, pp. 131～138, 1997

[15] C. E. Shannon. A mathematical theory of communications. The Bell System Technical Journal, vol. 27, pp. 379～423, pp. 623～656, 1948

[16] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin. Capacities of quantum erasure channels. Physical Review Letters, vol. 78, pp. 3217～3220, 1997

[17] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wootters. Mixed state entanglment and quantum error correction. Physical Review A, vol. 54, pp. 3824～3851, 1996

[18] C. H. Bennett, D. P. DiVincenzo. Quantum information and computation. Nature, vol. 404, pp. 247～255, 2000

[19] C. H. Bennett, G. Brassard. Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Singnal Processing, pp. 175～179, Bangralore, India, 1984

[20] C. H. Bennett, P. W. Shor, Quantum Information Theory. IEEE. Trans. IT, vol. 44, no. 6, pp. 2724～2742, Oct. 1998

[21] C. H. Bennett, S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Physical Review Letters, vol. 69, pp. 2881～2884, 1992

[22] D. Bouwmeester, A. Ekert, A. Zeilinger (Eds). The Physics of Quantum Information. Springer, 2000

[23] D. Bouwmeester, J. M. Pan, K. Mattle, M. Eible, H. Weinfurter, A. Zeilinger. Experimental quantum teleportation. Nature, vol. 390, pp. 575～579, 1997

[24] D. Boschi, S. Branca, F. De. Martini, L. Hardy, S. Popescu. Experimental realization of teleporting an unknown pyre quantum state via dual classical and Einstein-Podolsky-rosen channels. Physical Review Letters, vol. 80, pp. 1121～1125, 1998

[25] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. San-

pera. Quantum privacy amplification and the security of quantum sryptography over noisy channels. Physical Review Letters, vol. 76, pp. 2818～2821, 1996

[26] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. Physical Review A, vol. 54, pp. 1862～1864, 1996

[27] E. Knill, R. Laflamme. A theory of quantum error-correcting codes. Physical Review A, vol. 55, pp. 900, 1997

[28] E. Bernstein, U. Vazirani. Quantum complexity theory. SIAM Journal on Computing, vol. 26, no. 5, pp. 3457～3467, 1997

[29] H. -K. Lo, S. Popescu, T. Spiller(Eds.). Introduction to Quantum Computation and Information. World Scientific, 1998

[30] J. Preskill. Physical 229: Advanced Mathematical Methods of Physics Quantum Computation and Information, Chapter 7. California Institute of Technology, 1998
URL:http://www.theory.caltech.edu/people/preskill/ph229

[31] K. Mattle, H. Weinfurter, P. G. Kwiat, A. Zeilinger. Dense coding in experimental quantum communication. Physical Review Letters, vol. 76, pp. 4656～4659, 1996

[32] L. K. Grover. A fast quantum mechanical algorithm for database search. Proceedings of the 28th ACM Symposium on Theory of Computing, pp. 212～219, 1996

[33] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information. Cambridge Univ. Press, 2000

[34] M. A. Nielsen. Quantum Information Thory. Ph. D. thesis, University of New mexico, USA., 1998

[35] M. V. Burnashev, A. S. Holevo. On reliability function of quantum communication channel. quant-ph/9703013

[36] M. Zukowskim, A. Zeilinger, M. A. Horne, A. K. Ekert. "Event-ready-detectors" Bell experiment via entanglement swapping. Physical Review Letters, vol. 71, no. 26, pp. 4287～4290, 1993

[37] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, W. K. Wootters. Classical information capacity of a quantum channel. Physical Review A, vol. 54, pp. 1869, 1996

[38] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of 35th Annual Symposium on Foundations of Computer Science, Los Alamitos, CA, 1994

[39] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. Physical Review A, vol. 52, pp. 2494, 1995

[40] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, vol. 25, no. 5, pp. 1484～1509, 1997

[41] R. Matsumoto. Fidelity of a t-error-correcting quantum code with more than terrors,. Physical Review A, vol. 64, 022314, 2001

[42] R. Matsumoto, T. Uyematsu, Lower Bound for the Quantum Capacity of a Discrte Memoryless Quantum channel. LANL E-print, quantph/0105151, 2001

[43] R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, M. Schauer. Quantum cryptography. Contemp. Phys. vol. 36, no. 3, pp. 149～163, 1995. LANL E-print quant-ph/9504002

[44] R. Cleve, W. van Dam, M. A. Nielsen, A. Tapp. Quantum entanglement and the communication complexity of the inner product function. LANL E-print quant-ph/9708019, 1997

[45] S. Lloyd. Almost any quantum logic gate is universal. Physical Review Letters, vol. 75, pp. 346～349, 1995

[46] T. M. Cover, J. A. Thomas. Elements of Information Theory. John Wiley and Sons, 1991

[47] T. Uyematsu. Introduction of quantum information theory. 2000 URL: http://www. it. ss. titech. ac. jp/uematsu/uematsu. html

[48] W. W. Peterson, E. J. Weldon. Error-Correcting Codes. Second Edition, MIT Press, 1972

[49] A. Ashikhim and E. knill, Non-binary quantum stabilizer codes, IEEE Trans. Inform. Theory, vol. 47, pp. 3065～3072, Nov. 2001

[50] R. Matsumoto, T. Uyematsu, Constructing quantum error-correcting codes for p^m-state systems from classical error-correcting codes, quant-ph/9911011, 1999

[51] E. M. Rains, Nonbinary quantum coeds, IEEE Trans. Inform. Theory, vol. 45, pp. 1827～1832, Sept. 1999

[52] D. Schlingemann and R. F. Werner, Quantum error-correcting codes associated with graphs, Physical Review A, vol. 65, no. 012308, 2001. quant-ph/0012111

[53] A. M. Steane. Multiple particle interference and quantum error correction, Proc. Roy. London A, vol. 452, pp. 2551～2557, 1996

[54] K. Feng, Quantum Error-Correcting Codes, Coding Theory and Cryptography, Lecture Notes Series 1, Institute for Mathematical Sciences, National University of Singapore, edited by H. Niederreiter, World Scientific, 2002, pp. 91～142

[55] K. Feng and Z. Ma, Finite quantum Gilbert-Varshamov bound. To appear in IEEE Trans. Information Theory, 2005

[56] K. Feng, A New description of quantum error-correcting codes, preprint, 2004

[57] K. Feng and C. Xing, A New construction on quantum error-correcting codes, preprint, 2004

[General Information]
书名=电子信息与最子计算简明教程
作者=陈汉武编
页数=188
出版社=东南大学出版社
出版日期=2006年06月第1版
SS号=11631692
DX号=
URL=http://book2.duxiu.com/bookDetail.jsp?dxNumber=&d=20401835 0E153ABB9B73FEBC82B56715