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.①TP387②O413.1

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 江苏兴化印刷厂印刷
开本：700 mm×1000 mm 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。

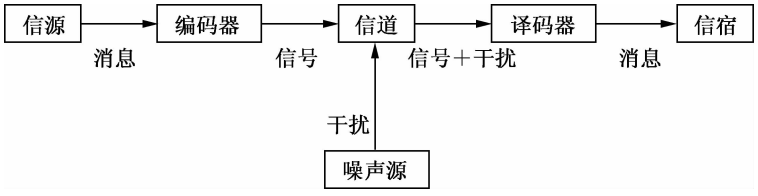

图 1　通信系统的理论模型

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。

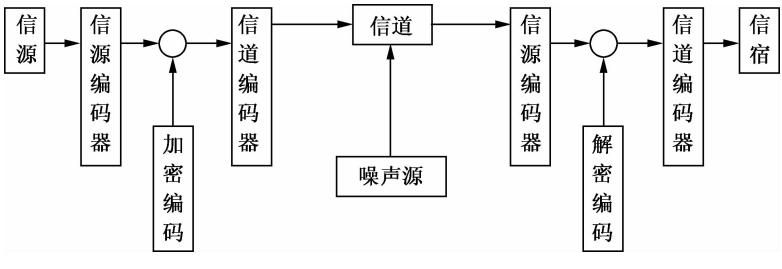

图 2 带有信息安全保密的通信系统的理论模型

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。

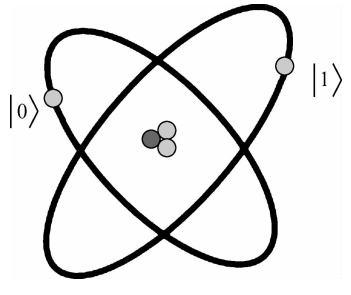

图 1－1 具有两个电子层面的原子可以表示量子信息

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。

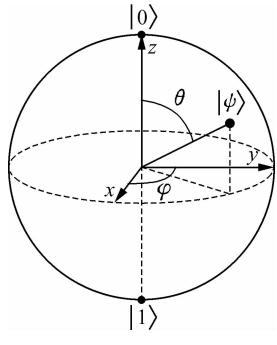

图1-2 一个量子比特的布洛赫球表示法

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。