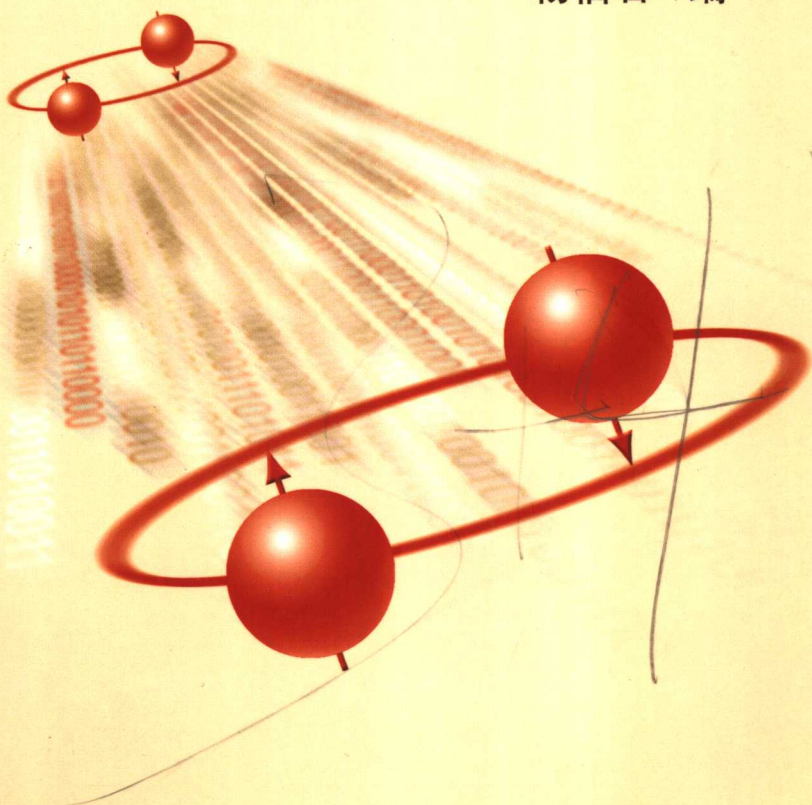


# 量子通信基础

杨伯君 编

Foundation  
of Quantum  
Communication



北京邮电大学出版社  
[www.buptpress.com](http://www.buptpress.com)

TN929.1/11

2007

# 量子通信基础

杨伯君 编

北京邮电大学出版社

·北京·

## 内 容 简 介

量子通信是近 20 年发展起来的新型交叉学科,是量子论和信息论相结合的新的研究领域。目前量子通信主要涉及量子密码通信、量子远程传态和量子密集编码等。近来这门学科已逐渐从理论走向实验,并向实用化方向发展。

本书主要介绍量子通信的物理基础和研究的进展,绪论中简要介绍了量子通信研究的历史。全书分 4 章。第 1 章介绍与量子通信有关的量子力学的基础知识,讲述微观粒子的特性,包括测不准关系、不可克隆定理和纠缠的非定域性等,这些特性是量子通信的物理基础。第 2 章介绍量子信息论基础,书中采用了经典信息论与量子信息论并行介绍的方法,其中最主要的是引入信息熵的概念,讨论信息熵的性质和计算方法。第 3、4 章分别介绍基于单光子和连续变量量子通信的各种方案和近期实验结果。

本书可以作为电子、信息和通信类专业开设量子通信课程的参考教材,也可供对量子通信感兴趣的各类人员参考。

### 图书在版编目(CIP)数据

量子通信基础/杨伯君编. —北京:北京邮电大学出版社,2007

ISBN 978-7-5635-1552-3

I. 量… II. 杨… III. 量子力学—光通信 IV. TN929.1

中国版本图书馆 CIP 数据核字(2007)第 153740 号

---

书 名: 量子通信基础

作 者: 杨伯君

责任编辑: 黄建清

出版发行: 北京邮电大学出版社

社 址: 北京市海淀区西土城路 10 号(邮编:100876)

北方营销中心: 电话: 010-62282185 传真: 010-62283578

南方营销中心: 电话: 010-62282902 传真: 010-62282735

E-mail: publish@bupt.edu.cn

经 销: 各地新华书店

印 刷: 北京源海印刷有限责任公司

开 本: 787 mm×960 mm 1/16

印 张: 7

字 数: 151 千字

印 数: 1—3 000 册

版 次: 2007 年 12 月第 1 版 2007 年 12 月第 1 次印刷

---

ISBN 978-7-5635-1552-3

定 价: 15.00 元

· 如有印装质量问题,请与北京邮电大学出版社营销中心联系 ·

# 前 言

量子通信是最近 20 年才发展起来的新型交叉学科,是量子论和信息论相结合的新的研究领域,是通信和信息领域研究的前沿。

目前,量子通信主要涉及量子密码通信、量子远程传态和量子密集编码等学科内容。近 20 年来,这个学科已逐步从理论走向实验,并向实用化方向发展,引起了越来越多部门和科学工作者的关注。目前,在这一领域工作的主要是物理学家和部分应用数学家,但也逐渐引起了从事计算机和通信领域工作人员的关注<sup>[2]</sup>。

在 1998 年之前,有关量子通信的文章大多发表在英国的 Nature 和美国的 Science 等探索性期刊上。从 1998 年下半年开始,在世界著名的物理学期刊 Physics Review A 上专门开了一栏“Quantum Information(量子信息,包括量子通信和量子计算)”,比较集中地报道这方面的研究成果,相应研究论文逐年增加。

我国在量子通信与量子计算方面已投入不少力量,量子通信和量子计算已列入国家 973 项目和国家自然科学基金重点项目,在科学院和各高校也已有数十个单位成立了量子信息研究室或研究组。我校作为全国通信研究的重点院校,也应在量子通信与量子信息研究方面占有一席之地。

本书主要介绍量子通信的物理基础和研究的进展,绪论中简要介绍了量子通信研究的历史。全书分 4 章。

第 1 章介绍与量子通信有关的量子力学的基础知识,讲述微观粒子的特性,包括测不准关系、不可克隆定理和纠缠的非定域性等,这些特性是量子通信的物理基础。

第 2 章介绍量子信息论基础,书中采用经典信息论与量子信息论并行介绍的方法,其中最主要的是引入信息熵的概念,讨论信息熵的性质和计算方法。

第 3,4 章分别介绍基于单光子和连续变量量子通信的各种方案和近期实

验结果。

本书是作者在北京邮电大学为研究生讲述“量子通信基础”的讲稿的基础上,适当修改而成的。本书可以作为电子、信息和通信类专业开设量子通信课程的参考教材,也可供对量子通信感兴趣的人员参考。

本书是国家自然科学基金项目(60578043)的一个成果,感谢基金给予的支持。在本书的出版过程中,北京邮电大学出版社给予了大力的支持,研究生王秋国、张虎、逯志钦和戴娟给予了有力的帮助,在此也一并表示衷心的感谢。

由于编者水平有限,不妥与错误之处在所难免,欢迎读者批评指正。

作 者

# 目 录

|                     |     |
|---------------------|-----|
| 绪 论                 | 1   |
| 第 1 章 量子力学的基本知识     |     |
| 1.1 量子力学的基本原理       | 3   |
| 1.2 量子力学的表述与模型      | 9   |
| 1.3 密度矩阵            | 15  |
| 1.4 EPR 佯谬与贝尔不等式    | 22  |
| 习题                  | 26  |
| 第 2 章 量子信息论基础       |     |
| 2.1 熵、量子信息的测度       | 28  |
| 2.2 可获取的最大信息        | 36  |
| 2.3 量子无噪声编码定理       | 39  |
| 2.4 带噪声量子信道上的信息     | 43  |
| 习题                  | 49  |
| 第 3 章 基于光子的量子通信     |     |
| 3.1 量子纠缠态的产生、性质与测量  | 51  |
| 3.2 双光子纠缠态在量子通信中的应用 | 58  |
| 3.3 基于单光子的量子密码术     | 64  |
| 习题                  | 73  |
| 第 4 章 基于连续变量的量子通信   |     |
| 4.1 量子光学中的连续变量      | 75  |
| 4.2 连续变量纠缠          | 80  |
| 4.3 利用连续变量的量子通信     | 88  |
| 习题                  | 101 |
| 部分习题答案              | 102 |
| 主要参考文献              | 103 |

# 绪 论

相对论、量子论和信息论是 20 世纪人类的三大发现。相对论就是爱因斯坦 (Einstein) 建立的狭义相对论和广义相对论<sup>[9]</sup>, 开始于 1905 年, 完成于 1916 年; 量子论开始于 1900 年, 在这一年普朗克 (Planck) 提出量子论假设, 到 1925 年狄拉克 (Dirac) 建立了矩阵力学<sup>[8]</sup>, 1926 年薛定谔 (Schrödinger) 建立了波动力学; 信息论则诞生于 20 世纪 40 年代, 公认的信息论的奠基人是美国数学家香农 (C. E. Shannon), 他在 1948 年发表了著名论文“通信的数学理论”<sup>[15]</sup>, 将概率论应用于信息领域, 引入信息熵, 给信息以定量的描述。

量子通信是量子论和信息论相结合的产物, 是通信和信息领域研究的前沿。量子通信主要涉及到量子密码通信、量子远程传态和量子密集编码等学科内容。早在 20 世纪 60 年代末, 威斯纳 (S. Wiesner) 就首次提出了量子密码的概念, 但不幸的是, 其文章没有被发表。量子通信研究的第一个成果是 1984 年 IBM 公司的班尼特 (Bennett) 和加拿大蒙特利尔大学的 Brassard 提出的第一个量子密钥分配 (QKD) 方案, 现称为 BB84 协议<sup>[14]</sup>。量子密钥分配的第一个实验由班尼特等人在 1989 年完成<sup>[16]</sup>, 当时传送距离只有十几米。近 20 年来, 量子密钥分配已取得很大发展, 理论上提出了数十种分配方案, 其中比较有名的有 1991 年英国牛津大学 Ekert 提出的基于纠缠态的 Ek91 方案和 1992 年班尼特提出的基于两态系统的 B92 方案。在实验方面, 1993 年英国国防研究部在光纤中用相位编码方式实现了 10 km 的 QKD, 1995 年传输距离达到 30 km; 1995 年日内瓦大学利用偏振编码实现了 23 km 的量子密钥分配, 为了克服光纤双折射对光子传输的影响, 他们提出了“即插即用”传输方案, 1999 年使量子密钥传输距离达到了 67 km; 2004 年 Gobby 等人实现了 122 km 的量子密钥传输; 同年日本 NEC 公司也进行了 150 km 的单光子的传送演示; 我国中国科学技术大学马晓繁等人也实现了北京到天津 125 km 的量子通信试验, 2003 年量子空间通信距离达到 23 km。由于现用的单光子源是利用微弱激光衰减而成的, 多光子态存在加上通信信道损失, 人们对量子通信的安全性提出了质疑。近期人们提出利用诱骗 (Decoy) 态可以增加 QKD 系统的安全性。诱骗态传输系统的传送距离已达 130 km<sup>[18]</sup>, 在自由空间利用诱骗态, 量子密钥分配传输距离已达 144 km<sup>[42]</sup>。量子密码通信除了量子密钥分配外, 还包括量子秘密共享和量子安全直接通信等。1999 年 Hillery 等人提出了第一个量子秘密共享方案, 现在已有十几种理论方案, 2001 年 Tittel 等人在实验上演示了三体量子秘密共享<sup>[43]</sup>, 2007 年 Gaertner 等人利用四光子纠缠态实现了四体量子秘密共享<sup>[44]</sup>。量子安全直接通信从 2002 年开始有一些理论性的探讨, 但由

于目前量子信号的码速率太低,还没法进行有关的实验。

量子远程传态(Teleportation)是班尼特等人<sup>[17]</sup>于1993年提出的,是一种用来传输未知量子态的技术。1997年奥地利 Zeilinger 等人利用晶体中Ⅱ型参量下转换产生光子的偏振纠缠态,成功地实现了一个光子偏振态的远程传送;1998年意大利 Boschi 等人利用参量放大和起偏器产生光子纠缠对,也实现了量子远程传态;2003年潘建伟等人在实验上完成了自由量子态的远程传态;2006年 Hinwelingen 等人利用三个贝尔(Bell)态分析器实现了三个贝尔态的远程传送<sup>[45]</sup>,同年 Hanmeres 等人还实现了光与原子之间的量子远程传态<sup>[46]</sup>。

利用单光子为载体进行量子通信,探测器必须工作在 Gaiger 模式,由于单光子产生的随机性和探测器的死时间限制,其信息码速率小于 1 Mbit/s。近几年,人们提出利用连续变量实现量子通信,信息载体是相干态或压缩态脉冲,其测量采用平衡零差和外差探测器,码速率可以明显地提高,而且可以中继放大而适合长距离传送。利用相干态进行量子密钥分配,其安全性讨论目前还是一个开放性的问题。由于目前还没有适用相位有关的参量放大器,理论上相干态传送距离只有 75 km,实验上利用相干态,量子密钥传输距离已超过 25 km<sup>[19]</sup>。

21 世纪是信息的时代,也是量子的时代,量子通信必将得到更大的发展。



# 第 1 章 量子力学的基本知识<sup>[7,8]</sup>

量子通信是用量子态为信息载体进行信号的发射、传输和处理,一切都满足量子力学的规律。因此,要学习量子通信必须掌握必要的量子力学的基本知识,包括量子力学的基本原理、量子力学的某些特征表示和模型等。此外,还需要了解与量子通信密切相关的密度矩阵、EPR 佯谬和贝尔不等式。本章分为以下几节:

- (1) 量子力学的基本原理,介绍量子力学的 5 个基本公设;
- (2) 量子力学的表述与模型;
- (3) 密度矩阵;
- (4) EPR 佯谬和贝尔不等式。

## 1.1 量子力学的基本原理<sup>[5]</sup>

物理学中各学科的基本理论都是建立在几个基本定律或假设的基础上的,如力学的基本理论是牛顿三定律;电磁学是麦克斯韦(Maxwell)方程组,它对应电磁场中 4 个基本定律,即法拉第(Faraday)电磁感应定律、安培(Ampere)环路定律和电场与磁场的高斯(Gauss)定理;热学有热力学三定律,其中热力学第二定律引入了熵的概念,熵的概念在信息论中起着重要作用。

作为描述物质微观运动的量子力学,其理论系统是建立在几个基本假设或称公设基础上的,这几个公设就是量子力学的基本原理,它们分别是量子状态公设、力学量公设、量子态运动方程公设、量子测量公设和全同性原理公设。下面就对这 5 个公设进行阐述。

### 1. 公设 1——量子状态公设

在量子力学建立初期,对粒子微观状态的描述有 2 种方法,即薛定谔的波动力学方法和狄拉克的矩阵力学方法。薛定谔的波动力学方法物理概念比较清楚,微观粒子波粒二象性表现也比较清楚,成为量子力学介绍的主流方法;狄拉克的矩阵力学方法表述比较简单,在量子力学的应用领域中得到广泛应用,特别是在量子通信的表述中用得较多。因此,本节同时介绍这两种表述方法。

按薛定谔的表述,量子力学第一条公设为:量子力学系统的状态用波函数  $\psi(\mathbf{r}, t)$  来描述,它来源于实验中显示的微观粒子(如电子、中子等)具有的波动特性。

1924 年,德布罗意(de-Broglie)给出自由粒子用平面波来描述的波函数

$$\psi(\mathbf{r}, t) = A e^{i(\mathbf{k} \cdot \mathbf{r} - \omega t)} = A e^{\frac{i}{\hbar}(\mathbf{p} \cdot \mathbf{r} - E t)} \quad (1-1)$$

从(1-1)式可以看出,粒子的动量、能量与相应波的波矢、频率的关系为

$$p = \hbar k, \quad E = \hbar \omega = h\nu \quad (1-2)$$

其中

$$\hbar = \frac{h}{2\pi}, \quad |k| = \frac{2\pi}{\lambda}$$

结论(1-2)也为光子实验所证实。在这条公设中,最重要的是如何正确理解波函数的物理意义,即如何理解波函数与它所描述的微观粒子之间的关系。目前认为正确的理解是:波函数在空间某处的强度 $|\psi|^2$ 和该处发现粒子的概率成正比,波函数描述的是概率波, $\psi$ 称为概率振幅。因为是概率波, $\psi$ 应满足归一化条件:

$$\int_{-\infty}^{\infty} |\psi|^2 dV = 1 \quad (1-3)$$

在物理上,还要求波函数满足单值、连续和有限的条件。

按狄拉克表述,量子力学第一条公设为:任一个孤立物理系统,将对应一个矢量空间,它是一个复空间,称为 Hilbert 空间,系统状态将由这空间中的一个单位矢量表示,符号为 $|\rangle$ ,称为右矢(ket),要标出特定状态可写为 $|\psi\rangle$ ,相应复共轭空间矢量为 $\langle|$ ,称为左矢(bra),矢量 $|\psi\rangle$ 与 $\langle\phi|$ 的内积为 $\langle\psi|\phi\rangle$ ,归一化表示为

$$\langle\psi|\psi\rangle = 1$$

对一个实际物理系统,即使要给出一个原子或分子的状态空间与态矢量都是不容易的,但对于量子计算与量子通信中的应用量子系统,一般比较简单。这里,我们关心的量子系统是量子比特,它对应一个二维的状态空间,这个空间的基矢为 $|0\rangle$ 和 $|1\rangle$ ,其中

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (1-4)$$

因此,任一个态矢量可以表示为

$$|\psi\rangle = a|0\rangle + b|1\rangle \quad (1-5)$$

实际系统可以是电子两自旋态、光子两偏振态,或原子两能态。(1-5)式中 $a, b$ 为复数,从 $|\psi\rangle$ 归一化条件得出 $|a|^2 + |b|^2 = 1$ 。两个状态 $|0\rangle$ 和 $|1\rangle$ 也可以形成一个经典比特。量子比特与经典比特不同之处是除状态 $|0\rangle$ 和 $|1\rangle$ 外,还存在 $a|0\rangle + b|1\rangle$ 的叠加态,因此量子比特带的信息量多于经典比特。

## 2. 公设 2——力学量公设

量子力学第二条基本原理就是力学量公设,表述为:量子力学中系统的力学量 $F$ 用线性厄米算符 $\hat{F}$ 表示。所谓算符就是一个运算符号,它可以是微商运算,也可以是一个矩阵,与态矢量的表述有关。

若对状态 $|\psi_1\rangle$ 和 $|\psi_2\rangle$ ,算符 $\hat{F}$ 满足

$$\hat{F}(c_1|\psi_1\rangle + c_2|\psi_2\rangle) = c_1\hat{F}|\psi_1\rangle + c_2\hat{F}|\psi_2\rangle \quad (1-6)$$

其中,  $c_1, c_2$  为常数, 则  $\hat{F}$  称为线性算符。

在狄拉克表述中, 状态用 Hilbert 空间矢量表示, 相应的算符是一个矩阵, 算符将满足矩阵的运算规则。

下面给出线性算符的性质及运算法则。

(a) 算符相等: 若  $\hat{A}|\psi\rangle = \hat{B}|\psi\rangle$ , 且  $|\psi\rangle$  是任意的, 则  $\hat{A} = \hat{B}$ 。

(b) 算符加减:

对任意态矢量  $|\psi\rangle$ , 有  $\hat{A}|\psi\rangle + \hat{B}|\psi\rangle = \hat{F}|\psi\rangle$ , 则  $\hat{F} = \hat{A} + \hat{B}$ ;

对任意态矢量  $|\psi\rangle$ , 有  $\hat{A}|\psi\rangle - \hat{B}|\psi\rangle = \hat{G}|\psi\rangle$ , 则  $\hat{G} = \hat{A} - \hat{B}$ 。

(c) 算符乘法一般不满足交换律, 即  $\hat{A}\hat{B}|\psi\rangle \neq \hat{B}\hat{A}|\psi\rangle$ 。

若两个算符满足  $\hat{A}\hat{B} = \hat{B}\hat{A}$ , 称  $\hat{A}$  与  $\hat{B}$  是对易的。

若算符作用在态矢量上等于一个常量与态矢量的乘积, 即

$$\hat{F}|\psi\rangle = \lambda|\psi\rangle \quad (1-7)$$

其中,  $\lambda$  为常数, 称为本征值;  $|\psi\rangle$  称为  $\hat{F}$  的本征态; (1-7) 式称为  $\hat{F}$  的本征值方程。

算符本征值是实数, 为此要求力学量算符是厄米 (Hermite) 的。

所谓算符的厄米性, 即要求对任意函数  $\psi$  与  $\varphi$ , 有

$$\int \psi^* \hat{F} \varphi dV = \int (\hat{F} \psi)^* \varphi dV \quad (1-8)$$

满足 (1-8) 式的算符称为厄米算符。特别地, 若  $\varphi = \psi$ , 则称为自厄算符。厄米算符对应的矩阵称为厄米矩阵。

记矩阵的厄米共轭为  $\mathbf{A}^\dagger = [\mathbf{A}^*]^\top$ , 其中  $*$  表示复共轭,  $\top$  表示转置运算, 如

$$\begin{bmatrix} 2+i & 3i \\ 1-i & 1-2i \end{bmatrix}^\dagger = \begin{bmatrix} 2-i & 1+i \\ -3i & 1+2i \end{bmatrix}$$

若算符  $\hat{A}$  的厄米共轭仍为  $\hat{A}$ , 即  $\hat{A}^\dagger = \hat{A}$ , 则称  $\hat{A}$  为厄米算符。

在量子通信中, 下列 4 个矩阵

$$\sigma_I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (1-9)$$

是非常有用的矩阵, 它们都是  $2 \times 2$  的厄米矩阵, 有时也分别写为  $\hat{I}, \hat{X}, \hat{Y}, \hat{Z}$ 。其中,  $\hat{I}$  为单位矩阵,  $\hat{X}, \hat{Y}$  和  $\hat{Z}$  为泡利 (Pauli) 矩阵。

### 3. 公设 3——量子态运动方程公设

按薛定谔的描述, 该公设为: 在非相对论量子力学中, 波函数  $\psi(r, t)$  满足的动力学方

程是薛定谔方程,表示为

$$i\hbar \frac{\partial}{\partial t} \psi(r, t) = \hat{H} \psi(r, t) \quad (1-10)$$

其中,  $\hat{H}$  是系统的哈密顿(Hamilton)算符,  $\hbar = h/(2\pi)$  为约化普朗克常数。

按狄拉克描述,该公设为:一个封闭量子系统的时间演化可以用一个幺正变换得到。若  $t_1$  时刻状态为  $|\psi_1\rangle$ ,  $t_2$  时刻状态为  $|\psi_2\rangle$ , 则有

$$|\psi_2\rangle = U |\psi_1\rangle \quad (1-11)$$

从薛定谔方程得

$$|\psi(t_2)\rangle = \exp\left[\frac{-i\hat{H}(t_2-t_1)}{\hbar}\right] |\psi(t_1)\rangle \quad (1-12)$$

则幺正变换算符用  $\hat{H}$  表示为

$$U(t_1, t_2) = \exp\left[\frac{-i\hat{H}(t_2-t_1)}{\hbar}\right] \quad (1-13)$$

对任意一个量子系统,如果能写出它的哈密顿量  $\hat{H}$ , 就可以解相应的薛定谔方程,从而给出它的状态的变化。对一般量子系统,要写出它的哈密顿量都不太容易,但对量子信息中量子比特来说,两态之间变化的哈密顿量是很简单的,为

$$\hat{H} = \hbar \omega \sigma_x \quad (1-14)$$

其中,  $\omega$  为一个参量,由实验确定,相应的本征态与  $\sigma_x$  相同,即为  $(|0\rangle + |1\rangle)/\sqrt{2}$  和  $(|0\rangle - |1\rangle)/\sqrt{2}$ ; 相应的本征能量为  $\hbar\omega$  与  $-\hbar\omega$ ; 基态为  $(|0\rangle - |1\rangle)/\sqrt{2}$ 。

#### 4. 公设 4——量子测量公设

前面提到对一个封闭量子系统,将按幺正算符演化。如果对系统进行测量,必须破坏其封闭性,为此引入量子测量公设。

对量子系统  $|\psi\rangle$  进行力学量  $M$  的测量,测到的是  $\hat{M}$  算符的某个本征值  $m_i$ , 系统将坍缩为  $\hat{M}$  的一个本征态  $|m_i\rangle$ , 将  $|\psi\rangle$  用  $|m_i\rangle$  展开

$$|\psi\rangle = \sum_i c_i |m_i\rangle \quad (1-15)$$

对大量测量,任一个本征值  $m_i$  出现的概率是展开系数的模的平方  $|c_i|^2$ , 相应力学量平均值(期望值)为

$$\langle M \rangle = \sum_i m_i |c_i|^2 = \langle \psi | \hat{M} | \psi \rangle \quad (1-16)$$

薛定谔描述为

$$\langle M \rangle = \int \psi^* \hat{M} \psi dV \quad (1-17)$$

测量最简单的例子是单量子比特在正交基下的测量,被测状态为

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

测量 $|0\rangle$ 态概率,相应力学量算符 $\hat{M}_0 = |0\rangle\langle 0|$ ,且

$$P(0) = \langle\psi|\hat{M}_0|\psi\rangle = \langle\psi|0\rangle\langle 0|\psi\rangle = |a|^2$$

测量后状态坍缩为

$$|0\rangle\langle 0|\psi\rangle/|a| = \frac{a}{|a|}|0\rangle$$

同样测量 $|1\rangle$ 态概率

$$P(1) = \langle\psi|\hat{M}_1|\psi\rangle = \langle\psi|1\rangle\langle 1|\psi\rangle = |b|^2$$

状态坍缩为

$$|1\rangle\langle 1|\psi\rangle/|b| = \frac{b}{|b|}|1\rangle$$

若量子力学系统是力学量 $M$ 的本征态 $|m_i\rangle$ ,则测量 $M$ 有

$$\hat{M}|m_i\rangle = m_i|m_i\rangle \quad (1-18)$$

$M$ 将有确定数值;若不是本征态,测量结果有意义的是平均值。测量的不确定性利用均方差根(也称标准偏差)表示

$$\Delta M = [\langle(\hat{M} - \langle\hat{M}\rangle)^2\rangle]^{\frac{1}{2}} \quad (1-19)$$

若两个算符 $\hat{A}$ 与 $\hat{B}$ 不对易,则在同一状态下,这两个力学量不能同时确定,其不确定量由海森堡(Heisenberg)测不准关系来确定。在量子力学中,可以证明两个物理量测不准关系为(后面证明)

$$\Delta A \Delta B \geq \frac{1}{2} |\langle\psi|[\hat{A}, \hat{B}]|\psi\rangle| \quad (1-20)$$

其中, $[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}$ 称为对易子。

### 5. 公设 5——全同性原理公设

描写全同粒子系统的态矢量,对于其中任意一对粒子,交换态矢量必须是对称的或反对称的。要求态矢量对称粒子为玻色子(Boson),要求反对称的粒子为费米子(Fermion)。

费米子系统满足泡利不相容原理;在每个量子态上最多只有一个费米子,费米子的自旋为 $\hbar$ 的半整数,电子、中子和质子为费米子;玻色子的自旋为 $\hbar$ 的整数,光子是玻色子。

对于多粒子系统,其量子行为比单粒子系统要复杂,量子纠缠就是多粒子系统表现出的一种不同于单粒子系统的特性。

考虑 $A, B$ 两粒子组成的系统,粒子 $A$ 用 Hilbert 空间 $H_A$ 的态矢量 $|\psi(t)\rangle_A$ 描述;粒子 $B$ 利用 Hilbert 空间中 $H_B$ 的态矢量 $|\psi(t)\rangle_B$ 描述; $A, B$ 组成两粒子系统,相应 Hilbert 空间 $H_{AB} = H_A \otimes H_B$ 。如果两粒子没有作用,其态矢量 $|\psi(t)\rangle_{AB} = |\psi(t)\rangle_A \otimes |\psi(t)\rangle_B$ ,这

乘积为张量积,这个态称为直积态。

下面给出张量积与直积态的分量表示:

若取  $|\psi\rangle = \begin{bmatrix} \psi_1 \\ \psi_2 \end{bmatrix}$ ,  $|\varphi\rangle = \begin{bmatrix} \varphi_1 \\ \varphi_2 \end{bmatrix}$ , 则

$$|\psi\rangle|\varphi\rangle = |\psi\rangle \otimes |\varphi\rangle = \begin{bmatrix} \psi_1|\varphi\rangle \\ \psi_2|\varphi\rangle \end{bmatrix} = \begin{bmatrix} \psi_1\varphi_1 \\ \psi_1\varphi_2 \\ \psi_2\varphi_1 \\ \psi_2\varphi_2 \end{bmatrix} \quad (1-21)$$

考虑量子比特两态,  $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ ,  $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ , 则

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

相应算符为矩阵张量积,若取

$$\mathbf{A} = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}$$

则

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} A_{11}\mathbf{B} & A_{12}\mathbf{B} \\ A_{21}\mathbf{B} & A_{22}\mathbf{B} \end{bmatrix} = \begin{bmatrix} A_{11}B_{11} & A_{11}B_{12} & A_{12}B_{11} & A_{12}B_{12} \\ A_{11}B_{21} & A_{11}B_{22} & A_{12}B_{21} & A_{12}B_{22} \\ A_{21}B_{11} & A_{21}B_{12} & A_{22}B_{11} & A_{22}B_{12} \\ A_{21}B_{21} & A_{21}B_{22} & A_{22}B_{21} & A_{22}B_{22} \end{bmatrix}$$

二阶张量的张量积为四阶张量。

考虑泡利矩阵张量积,由

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

则

$$\sigma_x \otimes \sigma_y = \begin{bmatrix} 0\sigma_y & 1\sigma_y \\ 1\sigma_y & 0\sigma_y \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{bmatrix}$$

若两粒子之间没有相互作用,  $t=t_0$  时状态为  $|\psi(t_0)\rangle_{AB}$ , 在  $t$  时刻状态为  $|\psi(t)\rangle_{AB}$ , 则两者关系为

$$|\psi(t)\rangle_{AB} = U_{AB}(t, t_0) |\psi(t_0)\rangle_{AB} \quad (1-22)$$

这时

$$\hat{H} = \hat{H}_A + \hat{H}_B, \quad U_{AB} = U_A \otimes U_B = e^{-\frac{i}{\hbar}(\hat{H}_A + \hat{H}_B)(t-t_0)} \quad (1-23)$$

若两系统之间有作用,则总的  $\hat{H} \neq \hat{H}_A + \hat{H}_B$ ,  $U_{AB} \neq U_A \otimes U_B$ , 这时系统状态不再是两子系统的直积态,而是处于纠缠态(Entangled State)。若两粒子分别对应两量子态  $|0\rangle$  和  $|1\rangle$ , 则对称与反对称的纠缠态分别为

$$|\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B) \quad (1-24)$$

$$|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B) \quad (1-25)$$

另 2 个纠缠态分别表示为

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B) \quad (1-26)$$

$$|\phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B) \quad (1-27)$$

这 4 个纠缠态在量子通信中有重要作用,称为 Bell 基态。处在 Bell 基态的两纠缠粒子称为 EPR(Einstein-Podolsky-Rosen)对。

## 6. 小结

到此我们已阐述完量子力学的 5 个公设,也是量子力学的 5 条基本原理。现在,从全局观点来小结一下这些公设。

公设 1 通过确定如何描述一个封闭量子系统的状态,设定了量子力学研究的对象;公设 2 给出了力学量在量子力学中的表述,它是一个线性厄米算符;公设 3 明确了封闭量子系统的动态由薛定谔方程,即一个幺正变换来描述;公设 4 告诉人们如何通过规定的测量来从量子系统中获取信息;公设 5 确定了一个复杂系统的量子力学状态应如何用单粒子状态去组合。

从经典观点看,量子力学独特之处是不能直接观测确定系统状态矢量,对一个状态矢量,其中力学量是不完全确定的。在测量状态时,状态会发生坍缩,坍缩为测量力学量的一个本征态。量子态的纠缠和量子态的隐含特性正是量子信息与量子通信独特性能的基础。

## 1.2 量子力学的表述与模型

本节介绍量子力学中的一些描述方法和有用的简单模型。

### 1. 量子力学中的表象

当量子力学利用薛定谔波动力学方式来描述时,其状态是用波函数来表示的。波函数的写法与自变量有关,通常波函数表示为  $\psi(r, t)$ , 自变量是坐标  $r$  与时间  $t$ , 称为坐标表象中波函数;若将波函数表示为  $\varphi(p, t)$ , 则称为动量表象中波函数。两类波函数之间

的关系是一个傅里叶(Fourier)变换

$$\varphi(\mathbf{p}, t) = \frac{1}{(2\pi\hbar)^{3/2}} \int \psi(\mathbf{r}, t) e^{-i\mathbf{p}\cdot\mathbf{r}/\hbar} dV \quad (1-28)$$

逆变换为

$$\psi(\mathbf{r}, t) = \frac{1}{(2\pi\hbar)^{3/2}} \int \varphi(\mathbf{p}, t) e^{i\mathbf{p}\cdot\mathbf{r}/\hbar} dV_p \quad (1-29)$$

其中,  $|\varphi(\mathbf{p}, t)|^2$  表示  $t$  时刻在动量空间  $\mathbf{p}$  附近出现的概率密度,  $dV_p$  为动量空间的体积元。

表示力学量的算符也与所用的自变量有关, 即与表象有关。在坐标表象中, 坐标算符为乘算符, 动量算符是微商算符, 即有

$$\hat{p}_x = \frac{\hbar}{i} \frac{\partial}{\partial x}, \quad \hat{p}_y = \frac{\hbar}{i} \frac{\partial}{\partial y}, \quad \hat{p}_z = \frac{\hbar}{i} \frac{\partial}{\partial z} \quad (1-30)$$

在动量表象中, 动量算符为乘算符  $\hat{p}_x, \hat{p}_y, \hat{p}_z$ , 而坐标算符为微商算符, 即有

$$\hat{x} = i\hbar \frac{\partial}{\partial p_x}, \quad \hat{y} = i\hbar \frac{\partial}{\partial p_y}, \quad \hat{z} = i\hbar \frac{\partial}{\partial p_z} \quad (1-31)$$

当量子力学利用狄拉克矩阵力学方式来描述时, 量子状态表示与表象无关。

## 2. 量子力学中的绘景

若系统处在状态  $|\psi\rangle$ , 系统某力学量的平均值(期望值)

$$\langle M \rangle = \langle \psi | \hat{M} | \psi \rangle \quad (1-32)$$

则当系统变化时,  $\langle M \rangle$  也将随时间变化。这变化可以来源于  $|\psi(t)\rangle$ , 也可以来源于  $\hat{M}(t)$ , 到底以谁的变化来实现而形成 3 个绘景(Picture), 分别称为薛定谔绘景、海森堡绘景和相互作用绘景。

### (1) 薛定谔绘景

在薛定谔绘景中, 力学量平均值变化来自于态矢量而与算符无关, 即算符不随时间变化

$$\langle M \rangle = \langle \psi_s(t) | \hat{M}_s | \psi_s(t) \rangle \quad (1-33)$$

其中,  $|\psi_s(t)\rangle$  的变化满足薛定谔方程。

### (2) 海森堡绘景

在海森堡绘景中, 力学量平均值变化来自于算符  $\hat{M}(t)$ , 而与态矢量  $|\psi\rangle$  无关

$$\langle M \rangle = \langle \psi_H | \hat{M}_H(t) | \psi_H \rangle \quad (1-34)$$

其中,  $\hat{M}_H(t)$  的变化满足海森堡方程, 即有

$$i\hbar \frac{\partial}{\partial t} \hat{M}_H(t) = \hat{M}_H(t) \hat{H}(t) - \hat{H}(t) \hat{M}_H(t) = [\hat{M}_H(t), \hat{H}(t)] \quad (1-35)$$

对同一系统状态, 其力学量平均值不因绘景而变化。因此有

$$\langle \psi_s(t) | \hat{M}_s | \psi_s(t) \rangle = \langle \psi_H | \hat{M}_H(t) | \psi_H \rangle \quad (1-36)$$



## (3) 相互作用绘景

若系统受到某种微扰作用,如在辐射场中的原子系统,则其哈密顿算符为

$$\hat{H} = \hat{H}_0 + \hat{V} \quad (1-37)$$

其中,  $\hat{H}_0$  为原子内部哈密顿量,  $\hat{V}$  为相互作用哈密顿量。对这系统的研究可以利用相互作用绘景,在这绘景中,态矢量和算符都随时间变化

$$\langle M \rangle = \langle \psi_1(t) | \hat{M}_1(t) | \psi_1(t) \rangle \quad (1-38)$$

相互作用绘景中的态矢量和算符与薛定谔绘景中的态矢量和算符之间的关系,可以通过么正变换得到

$$|\psi_1(t)\rangle = e^{i\hat{H}_0 t/\hbar} |\psi_s(t)\rangle, \quad \hat{M}_1(t) = e^{i\hat{H}_0 t/\hbar} \hat{M}_s e^{-i\hat{H}_0 t/\hbar} \quad (1-39)$$

其中态矢量  $|\psi_1(t)\rangle$  满足方程

$$i\hbar \frac{\partial}{\partial t} |\psi_1(t)\rangle = \hat{V}_1(t) |\psi_1(t)\rangle \quad (1-40)$$

这里

$$\hat{V}_1(t) = e^{i\hat{H}_0 t/\hbar} \hat{V}_s e^{-i\hat{H}_0 t/\hbar} \quad (1-41)$$

而算符  $\hat{M}_1(t)$  满足海森堡方程

$$i\hbar \frac{\partial}{\partial t} \hat{M}_1(t) = \hat{M}_1(t) \hat{H}_0 - \hat{H}_0 \hat{M}_1(t) = [\hat{M}_1(t), \hat{H}_0] \quad (1-42)$$

## 3. 二能级原子模型与量子双态系统

原子由原子核与核外电子组成,且其物理化学性质主要由核外电子决定。原子光谱为线状光谱显示核外电子处在分离能态上。当电子从高能态跃迁到低能态,就会放出一个光子,放出光子的频率满足频率定则

$$\nu = \frac{E_n - E_i}{\hbar} \quad (1-43)$$

该定则表明光子辐射主要涉及原子中两个电子的能态。因此,在研究光子与原子相互作用时,仅考虑原子中两个能级而忽略其他能级作用,称二能级原子模型。

二能级原子模型中,原子仅两个能态,分别为  $a$  与  $b$ , 其中  $b$  为基态,态矢量表示为  $|b\rangle$ , 激发态为  $|a\rangle$ , 如图 1.1 所示。

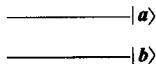


图 1.1 二能级原子模型

原子的哈密顿量为  $\hat{H}_0$ , 且有

$$\hat{H}_0 |a\rangle = E_a |a\rangle, \quad \hat{H}_0 |b\rangle = E_b |b\rangle \quad (1-44)$$

因可以用来构成一个量子比特,二能级原子在量子信息中有重要应用,其状态可表为

$$|\psi\rangle = a|a\rangle + b|b\rangle \quad (1-45)$$