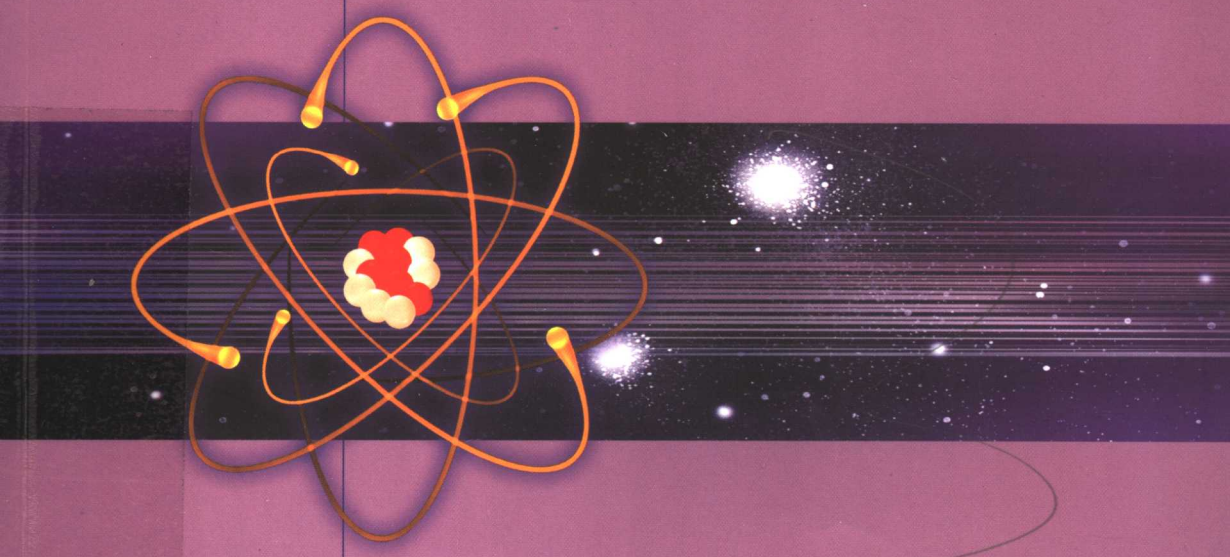
突破经典信息科学的极限——

量子信息论

QUANTUM INFORMATION THEORY

[日] 佐川弘幸　吉田宣章　著

宋鹤山　宋　天　译



大连理工大学出版社

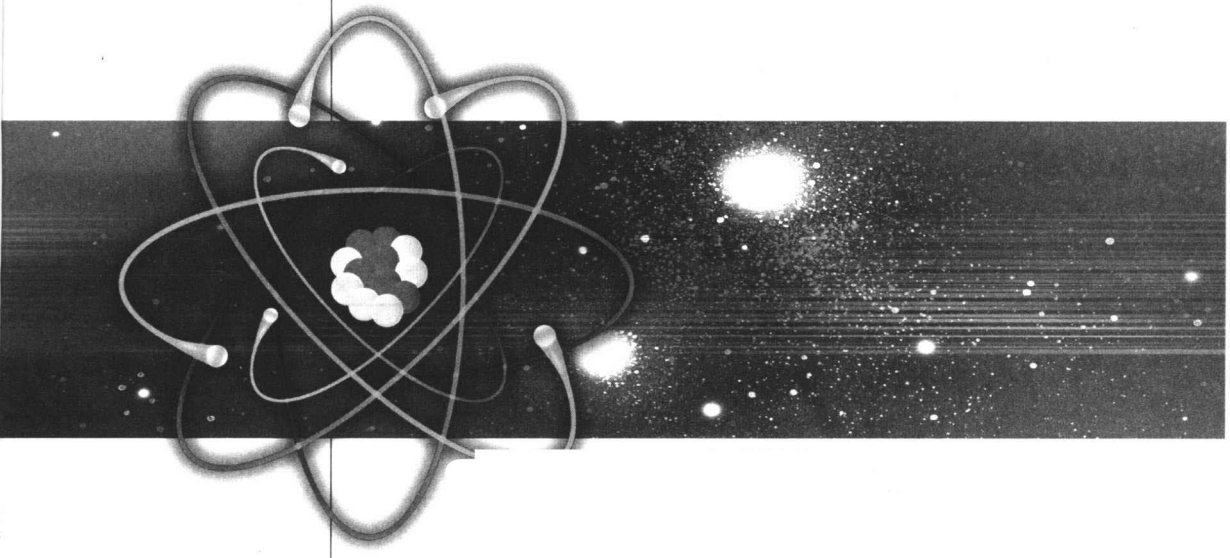
DALIAN UNIVERSITY OF TECHNOLOGY PRESS

突破经典信息科学的极限——

量子信息论

QUANTUM INFORMATION THEORY

[日] 佐川弘幸　吉田宣章　著
宋鹤山　宋　天　译



大连理工大学出版社
DALIAN UNIVERSITY OF TECHNOLOGY PRESS

图书在版编目(CIP)数据

量子信息论 /(日)佐川弘幸,(日)吉田宣章著;宋鹤山,宋天译. —大连:大连理工大学出版社,2007.9
ISBN 978-7-5611-3743-7

Ⅰ.量… Ⅱ.①佐…②吉…③宋…④宋… Ⅲ.量子力学-信息技术 Ⅳ.O413.1

中国版本图书馆 CIP 数据核字(2007)第 131773 号

大连理工大学出版社出版
地址:大连市软件园路 80 号 邮政编码:116023
电话:0411-84708842 邮购:0411-84703636 传真:0411-84701466
E-mail:dutp@dutp.cn URL:http://www.dutp.cn
大连理工印刷有限公司印刷 大连理工大学出版社发行

幅面尺寸:170mm×240mm 印张:13.75 字数:219 千字
2007 年 9 月第 1 版 2007 年 9 月第 1 次印刷

责任编辑:刘新彦 责任校对:碧 海
封面设计:姜春媛

ISBN 978-7-5611-3743-7 定 价:35.00 元

译者前言

量子信息论是信息科学和量子理论的交叉学科，它将量子力学应用于信息科学技术，为信息科学的发展提供了崭新的原理、方法和途径。在量子信息处理过程中，信息的载体是量子态，从而可通过直接调控微观体系的量子态来完成逻辑运算。量子信息论诞生以来已经取得举世瞩目的成果，并显示出了十分广阔的应用前景。

佐川弘幸、吉田宣章两位教授所著的《量子信息论》以通俗易懂的语言和直观的图解介绍了量子信息论的基本思想，并提供了很多例题来帮助读者理解量子信息论中的基本概念和基本原理。该书覆盖量子信息论全方位的基础知识，章节结构合理，理论描述简练直观，计算简捷易懂，适合于做研究生的入门教材或专业人员和业余爱好者的参考书。

佐川弘幸、吉田宣章两位教授都是在东北大学、东京大学等国际知名大学获得理学博士学位以后，又在日本、欧洲等地的大学或科研单位从事教学、科研工作的学者。他们不仅活跃在科学研究的前沿领域，而且著有大量读者喜爱的教材与著作。相信他们合著的这本书也会受到中国广大读者的喜爱。

最后，向在本书的翻译过程中提出宝贵意见的大连理工大学温小琼博士和日本大阪大学的郑涛博士表示诚挚的谢意。

宋鹤山　宋　天

2007 年 8 月

中文版前言

我和吉田宣章教授所著的日文版《量子信息论》一书，即将由宋鹤山教授与宋天博士翻译出版，对本书中文版的问世，我们感到非常高兴。

面对21世纪计算机科学的发展，人们越来越清楚地感觉到量子力学的重要作用。近年来，随着量子力学的新进展和量子信息科学的发展，量子计算机、量子密码科学与技术等领域呈现出令人兴奋的景象，不断出现举世瞩目的研究成果。过去认为几乎不可能的超大数的素数分解已成为可能，编制不可窃取和不可破译的密码也成为可能。不仅如此，量子信息科学还潜在着量子钱币(quantum money)、量子数据的压缩等各种可能性。

年轻的中国学生正在挑战这一崭新的科学前沿，如果本书能够为这些年轻人的成长提供必要的帮助，我们将深感荣幸。

最后，向翻译本书的宋鹤山教授、宋天博士以及为本书的问世做出贡献的各位同仁表示衷心的谢意。

佐川弘幸

于樱花盛开的会津

2007年4月

前　言

计算机在现代社会中的作用变得越来越重要。与十年前相比，计算机与人类生活的密切程度，已远远超出我们的想象，计算机的计算速度、存储量均按 Moore 定律，每三年翻四番。尽管计算机以惊人的速度在发展，但在过去的 40 年里，计算机的基本原理却一直没有变化。那么，再过 20 年，计算机的硬件将会是怎样的一种状态呢？预计到那时，计算机的基本记忆单元将是一个一个的原子、分子，届时，自然会出现新的物理装置，其设计原理也与现在的计算机原理大不相同。在通信手段、密码技术、数据搜索等领域里，基于量子力学原理的一个崭新的电脑世界正在被逐步构建。作为描述 21 世纪以后计算机世界的理论——量子信息论已经初露端倪。利用量子计算机进行大数因数分解的划时代的算法也已经被开发，并得到实验验证。利用二粒子之间的强大关联-纠缠(entanglement)性质的量子通信实验已经成功实现，窃听者无法破译的量子密码技术方案也已被提出。

量子信息论的基础是量子力学原理。晶体管和集成电路当然也是基于量子力学，但在量子信息论中，其算法引入量子力学的原理和方法，这一点是与经典理论的根本区别。也就是说，利用量子力学中波函数的叠加性质，将由 0 和 1 的二进制构成的经典比特推广到含复数的量子比特。换句话说，将比特由整数推广到含有实数和相位的多维复空间。将量子比特作为量子计算机的基本信息单元，才使量子计算变为可能。在量子通信中，需要利用叫做 EPR 光子对的

纠缠态。EPR 光子对的概念是 Einstein 作为对量子力学的几率诠释的质疑而提出的概念，但很滑稽的事实是，这一概念却变成了确立量子力学的几率诠释或远程作用的关键。

本书的目的是从量子力学的基本思想出发，描述量子信息论的基本框架和量子算法。本书并没有追求数学、物理的严密性，而是为了使读者易于理解其基本思想，把抽象概念具体化和充实内容（self-contain）作为讲述的重点。本书主要以学过量子力学的高年级本科生和硕士研究生为对象而写的。如果本书能够成为读者打开量子信息论的超出人们想象的未知世界的窗口，我们将倍感荣幸。在 21 世纪的计算机、通信世界中，量子力学不只是一种“假想实验”（Gedanken Experiment）的手段，而且也将是一种了解未知世界的基本理论依据。

为了充实内容，本书首先在第 1 章、第 3 章介绍量子信息论所必要的量子力学与信息理论的基础知识。第 2 章和第 4 章以后的各章节是量子信息论的核心部分。第 9 章阐述量子计算机的物理实现。第 10 章介绍密码理论所需要的整数论的基础知识。

最后，向全力协助我们制作本书 Latex 文本的日本会津大学的吉野大志君和对整数论的基础知识提出宝贵意见的日本会津大学的渡部繁先生表示感谢。

2003 年 4 月

佐川弘幸

吉野宣章

目 录

第 1 章 量子力学基础 …… 1

1.1 态矢量 …… 2

1.2 态矢量的时间演化 …… 4

1.3 对易关系和不确定性关系 …… 6

1.4 自旋$\frac{1}{2}$体系的量子态 …… 9

1.5 量子比特 …… 13

1.6 角动量、自旋与旋转 …… 14

习 题 …… 19

第 2 章 EPR 对和观测问题 …… 21

2.1 EPR 对 …… 22

2.2 量子态的传送 …… 23

2.3 Einstein 的量子力学局域性原理 …… 25

2.4 二粒子关联系的观测与隐变量理论 …… 29

2.4.1 CHSH 不等式 …… 29

2.4.2 经典关联和量子关联:核分裂问题 …… 33

2.5 基于光子对的 EPR 实验 …… 35

习 题 …… 39

第 3 章 经典计算机 …… 41

3.1 逻辑电路 …… 42

3.2 时序电路和存储器 …… 46

3.3 Neumann 型计算机 …… 50

3.4 图灵机 …… 50

3.5 可计算性和计算的复杂性 …… 54

3.5.1 四则运算 …… 55

3.5.2 素数分解和素数的判定问题 …… 56

3.5.3 组合问题 …… 57
3.5.4 计算的复杂性和计算量 …… 59
习 题 …… 59
第 4 章 量子逻辑门 …… 61
4.1 基本量子门 …… 62
4.2 受控量子门 …… 67
4.3 量子图灵机 …… 72
4.4 量子 Fourier 变换(3 比特情况) …… 73
习 题 …… 77
第 5 章 信息、通信理论 …… 79
5.1 熵 …… 80
5.1.1 信息量的定义 …… 80
5.1.2 熵 …… 80
5.1.3 信息的编码 …… 82
5.1.4 Von Neumann 熵 …… 84
5.2 通信中的信息量 …… 85
习 题 …… 89
第 6 章 量子计算 …… 91
6.1 量子比特和量子寄存器 …… 92
6.2 Deutsch-Josza 算法 …… 95
6.3 Shor 的素数分解算法 …… 96
6.4 n 比特量子 Fourier 变换 …… 99
6.5 量子相位的计算和阶算法 …… 101
6.6 同余式指数计算 …… 108
习 题 …… 109
第 7 章 量子密码 …… 111
7.1 密钥密码 …… 112
7.2 单时拍密码 …… 113
7.3 公开钥密码 …… 114
7.4 量子密钥分发 …… 118
7.4.1 不可克隆定理 …… 118
7.4.2 BB84 协议 …… 119

7.4.3 B92 协议 …… 124
7.4.4 E91 协议 …… 126
习 题 …… 129
第 8 章 量子搜索算法 …… 131
8.1 Oracle 函数 …… 132
8.2 量子 Oracle …… 133
习 题 …… 141
第 9 章 量子计算机的设计 …… 143
9.1 核磁共振计算机 …… 145
9.1.1 核磁共振计算机的原理 …… 145
9.1.2 核磁共振与自旋进动 …… 147
9.1.3 统计处理 …… 151
9.1.4 计算例子——素数分解量子计算实验 …… 153
9.2 捕获离子计算机 …… 157
9.2.1 基本原理 …… 157
9.2.2 捕获离子 …… 158
9.2.3 算 法 …… 163
9.2.4 初始态的制备 …… 164
9.2.5 计算结果的读出 …… 164
9.2.6 量子门举例 …… 165
9.3 量子点计算机 …… 167
9.3.1 基本原理 …… 167
9.4 光子计算机 …… 172
习 题 …… 173
第 10 章 整数论简介 …… 175
10.1 整数论基础 …… 176
10.1.1 同余式 …… 176
10.1.2 Euler 定理 (Fermat 小定理) …… 179
10.1.3 欧氏相除法 …… 181
10.1.4 Diophantus 方程(不定方程) …… 182
10.1.5 中国式剩余定理 …… 183
10.2 连分数展开 …… 185

习题参考解答…… 189
参考文献…… 203
索　引…… 205
附　表…… 208
附表 1　希腊字母及其读法 …… 208
附表 2　基本物理常数 …… 208
附表 3　SI 词头…… 208

第1章　量子力学基础

微观世界粒子的运动显示出粒子与波动二重性质。光的衍射与干涉反映光的波动性，而光电效应或黑体辐射只能用光的粒子性才能解释。微观世界的这种二重性质不只是光的性质，而是电子、质子、中子等所有粒子的共同性质。由此可以得出结论：微观世界粒子的运动只能通过“具有波动性质的波函数 ψ 给出粒子的存在几率”这一统计诠释才能理解。这就是以玻尔(Niels Bohr)为核心发展起来的量子力学的哥本哈根学派的观点。另一方面，爱因斯坦(A. Einstein)对这个几率诠释提出异议，坚持认为“上帝不会玩骰子”，自然规律应像牛顿力学那样遵从决定论。他始终没有接受量子力学的统计诠释。直到现在，虽然仍有人鉴于量子力学的几率诠释认为量子力学是不完备的理论，但用哥本哈根学派的观点去解释任何微观现象，都没有发生实质性困难。爱因斯坦的决定论观点的进一步发展就是所谓的隐变量理论，它以贝尔(Bell)不等式的形式与哥本哈根学派的观点相对立。这两种理论对量子力学的测量问题具有很大冲击，成为量子信息论的焦点与特征。

1.1 态矢量

描述微观粒子在三维空间运动的波函数 ψ 可以用坐标矢量 $\boldsymbol{r}=(x,y,z)$ 和时间 t 的函数 $\psi(\boldsymbol{r},t)$ 来表示。由于粒子的量子态包括取离散值的轨道角动量 $\boldsymbol{l}$，自旋 $\boldsymbol{S}$ 等，量子态也可以用这些量的量子数来区别。粒子的波函数也叫做几率幅，当其绝对值的平方

$$|\psi(\boldsymbol{r},t)|^2=\psi^*(\boldsymbol{r},t)\psi(\boldsymbol{r},t) \tag{1-1}$$

在全空间中的积分归一时，上式代表粒子在时刻 t 出现在位置 $\boldsymbol{r}$ 上的几率密度。其中，ψ^* 表示 ψ 的复共轭。波函数 ψ 也可以用复矢量空间中的右矢

$$|\psi\rangle \tag{1-2}$$

表示。这一符号是由 P. M. Dirac 引进的，$|\psi\rangle$ 也叫做态矢量，它可以用 n 维复矢量空间中的列矢量

$$|\psi\rangle=\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \tag{1-3}$$

表示。$a_1,a_2,\cdots,a_n$ 为坐标矢量 $\boldsymbol{r}$、时间 t 和自旋 $\boldsymbol{S}$ 的函数。在量子信息论中自旋自由度起重要作用。利用 Dirac 符号，两个量子态 $|\psi\rangle$，$|\varphi\rangle$ 的叠加态可以表示

成

$$c_1|\psi\rangle+c_2|\varphi\rangle \tag{1-4}$$

其中，c_1，c_2 为复数。

右矢量的复共轭矢量叫做左矢量，n 维左矢量可表示为

$$\langle\psi|=(|\psi\rangle)^{\dagger}=(a_1^*,a_2^*,\cdots,a_n^*) \tag{1-5}$$

波函数满足归一化条件

$$\langle\psi|\psi\rangle=1 \tag{1-6}$$

n 维矢量空间中的单位矩阵可以用任意的、构成完备系的基矢$|i\rangle$表示：

$$\boldsymbol{I}=\sum_i|i\rangle\langle i| \tag{1-7}$$

从而，态矢量$|\psi\rangle$可以表示成基矢$|i\rangle$的线性组合

$$|\psi\rangle=\sum_i|i\rangle\langle i|\psi\rangle \tag{1-8}$$

其中，基矢$|i\rangle$满足正交、归一条件

$$\langle i|j\rangle=\delta_{ij} \tag{1-9}$$

由于单位矩阵 $\boldsymbol{I}$ 是 n 维行矢量和列矢量的张量积，因此，它是一个 n 行 n 列的矩阵。

各种可观测物理量均可以表示为坐标 $\boldsymbol{r}$ 或动量 $\boldsymbol{p}$ 的函数，但 $\boldsymbol{r}$ 或 $\boldsymbol{p}$ 本身也是可观测量，因此，也叫做作用于波函数上的算符。任何一个物理量算符 A 的期待值或平均值为

$$\langle A\rangle\equiv\langle\psi|A|\psi\rangle=\int\psi^*(\boldsymbol{r},t)A\psi(\boldsymbol{r},t)\mathrm{d}\boldsymbol{r} \tag{1-10}$$

物理量 A 的测量值必须为实数。因此，在经典力学中，要满足 $A=A^*$ 的条件，而在量子力学中，这个条件变为 A 的期待值$\langle A\rangle$必为实数。对两个态矢量$|\psi_1\rangle$和$|\psi_2\rangle$之间的矩阵元，

$$\langle\psi_2|A|\psi_1\rangle=\langle\psi_1|A|\psi_2\rangle^* \tag{1-11}$$

就是 A 为一个物理量的条件。任意算符 A 的厄米共轭算符 $A^{\dagger}$ 定义为

$$\langle\psi_1|A^{\dagger}|\psi_2\rangle=\langle\psi_2|A|\psi_1\rangle^* \tag{1-12}$$

通常，称 A 和 $A^{\dagger}$ 互为厄米共轭。特别是，当 $A^{\dagger}=A$ 时，称 A 为厄米算符。由式(1-12)看到，厄米算符的期待值必为实数，也就是说，将实数推广到算符就是厄米算符，复共轭的推广就是厄米共轭。在量子力学中，所有的物理量都可以用厄米算符表示。

1.2 态矢量的时间演化

决定波函数随时间演化的运动方程就是量子力学的基本方程——Schrödinger 方程：

$$\mathrm{i}\hbar\frac{\partial\psi(\boldsymbol{r},t)}{\partial t}=H\psi(\boldsymbol{r},t) \tag{1-13}$$

其中，H 代表体系的 Hamilton 量，它是动能和势能之和，$\hbar\equiv\frac{h}{2\pi}$，而 $h=6.63\times10^{-34}\mathrm{J}\cdot\mathrm{s}$，是 Planck 常数。如果 Hamilton 量不依赖于时间，则由于

$$\frac{\mathrm{d}\psi(t)}{\mathrm{d}t}=\lim_{\Delta t\to\infty}\frac{\psi(t+\Delta t)-\psi(t)}{\Delta t} \tag{1-14}$$

对无穷小的 Δt，由式(1-13)，波函数随时间的变化可以表示为

$$\psi(t+\Delta t)=\left(1-\frac{\mathrm{i}H\Delta t}{\hbar}\right)\psi(t) \tag{1-15}$$

定义时间演化算符 $U(\Delta t)$，则波函数随时间的变化也可以表示成

$$U(\Delta t)\psi(t)=\psi(t+\Delta t) \tag{1-16}$$

由此可以得到

$$U(\Delta t)=1-\frac{\mathrm{i}H\Delta t}{\hbar} \tag{1-17}$$

上式中的 Hamilton 量 H 必须是厄米算符，$H^{\dagger}=H$，因此，$U(\Delta t)$应该是 Δt 的一阶函数，从而得到

$$U(\Delta t)U^{\dagger}(\Delta t)=\left(1-\frac{\mathrm{i}H\Delta t}{\hbar}\right)\left(1+\frac{\mathrm{i}H\Delta t}{\hbar}\right)\approx1 \tag{1-18}$$

这就是说，$U(\Delta t)$是一个幺正算符。把 $t+\Delta t$ 替换成 t'，则 $U(\Delta t)$可以写成

$$U(\Delta t)=U(t',t) \tag{1-19}$$

其中，$t'-t=\Delta t$ 表示无穷小时间变化。在时间演化算符的作用下，波函数 ψ 在时间 $t_0\to t=t_0+\Delta t\to t'=t+\Delta t$ 的变化可以写成

$$\psi(t')=U(t',t)\psi(t)=U(t',t)U(t,t_0)\psi(t_0)=U(t',t_0)\psi(t_0) \tag{1-20}$$

由此得到

$$U(t',t_0)=U(t',t)U(t,t_0) \tag{1-21}$$

也就是说，$U(t',t_0)$可以用无穷小时间演化算符的乘积表示。再利用

$$U(t',t_0)=\left(1-\frac{\mathrm{i}H}{\hbar}\Delta t\right)U(t,t_0) \tag{1-22}$$

可以得到

$$\frac{U(t',t_0)-U(t,t_0)}{\Delta t}=-\frac{\mathrm{i}H}{\hbar}U(t,t_0) \tag{1-23}$$

在 $\Delta t\to 0$ 的极限下

$$\frac{1}{U(t,t_0)}\frac{\mathrm{d}U(t,t_0)}{\mathrm{d}t}=-\frac{\mathrm{i}H}{\hbar} \tag{1-24}$$

同时对上式两边积分得

$$U(t,t_0)=\mathrm{e}^{-\frac{\mathrm{i}}{\hbar}H(t-t_0)} \tag{1-25}$$

积分时，利用了 $U(t_0,t_0)=1$ 的归一化条件。从 t_1 到 t_2 的有限时间内波函数的变化也可以用幺正算符(1-25)求得

$$\psi(\boldsymbol{r},t_2)=U(t_2,t_1)\psi(\boldsymbol{r},t_1) \tag{1-26}$$

当 Hamilton 量 H 不依赖于时间时，可以把波函数 $\psi(\boldsymbol{r},t)$进行分离变量，写成不含时间的部分 $\varphi(\boldsymbol{r})$和含时间的部分 $f(t)$的乘积，

$$\psi(\boldsymbol{r},t)=\varphi(\boldsymbol{r})f(t) \tag{1-27}$$

并把 $\psi(\boldsymbol{r},t)$代入到 Schrödinger 方程(1-13)，则得

$$\mathrm{i}\hbar\varphi(\boldsymbol{r})\frac{\partial f(t)}{\partial t}=H\varphi(\boldsymbol{r})f(t) \tag{1-28}$$

用 $\psi(\boldsymbol{r},t)$除式(1-28)的两边得到

$$\mathrm{i}\hbar\frac{1}{f(t)}\frac{\partial f(t)}{\partial t}=\frac{1}{\varphi(\boldsymbol{r})}H\varphi(\boldsymbol{r})(\equiv E) \tag{1-29}$$

可以看到，方程被分离成分别依赖于时间和位置的两个部分，此方程对所有的时间和位置都成立的条件是方程的两边均等于某一常数。假定此常数为 E，则通过积分得到

$$f(t)=\mathrm{e}^{-\mathrm{i}\frac{E}{\hbar}t} \tag{1-30}$$

依赖于位置的波函数 $\varphi(\boldsymbol{r})$满足方程

$$H\varphi(\boldsymbol{r})=E\varphi(\boldsymbol{r}) \tag{1-31}$$

可见，常数 E 代表 Hamilton 量 H 的本征值，波函数 $\varphi(\boldsymbol{r})$代表相应的本征函数。Hamilton 量 H 不含时间的 Schrödinger 方程的解可以写成时间和空间变量分离的形式：

$$\psi(\boldsymbol{r},t)=\varphi(\boldsymbol{r})\mathrm{e}^{-\mathrm{i}\frac{E}{\hbar}t} \tag{1-32}$$

一般来说，如果空间波函数 $\varphi(\boldsymbol{r})$局限在空间的有限领域，则体系的能量 E 取离散的不连续值，但如果 $\varphi(\boldsymbol{r})$延拓到无限空间领域，则能量取连续值。不依

赖于时间的 Hamilton 量 H 的本征态叫做具有能量 E 的定态。因为能量 E 是 Hamilton 量 H 的本征值，应具有下限，把这个能量最低的状态叫做基态，其他状态叫做激发态。在激发态中，能量最低的状态叫做第一激发态，其次叫做第二激发态，…，这些不同能量的状态构成体系的能级，能级与波函数如图 1-1 所示。

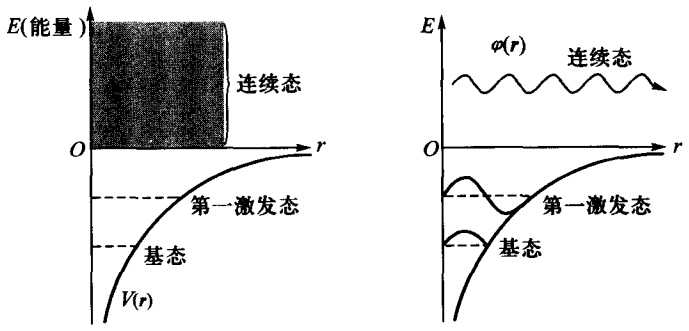


图 1-1 能级与波函数

孤立的原子、分子等体系，由于与外界没有能量交换，体系将处于能量最低的基态。但如果外界对体系提供光等能量时，体系将吸收能量而跃迁到激发态，并要重新放出能量回到基态。由于能级间的跃迁必须满足能量守恒定律，只有当从外界所吸收的能量等于两个能级之间的能量差时，跃迁才能发生。放出能量回到低能级的过程也要满足所放出的能量必须等于两个能级之间的能量差这一选择定则(图 1-2)。选择定则在制备量子比特时起非常重要的作用。

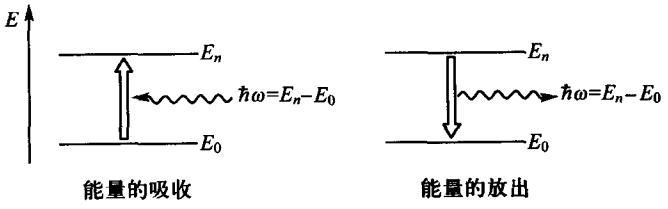


图 1-2 两个能级之间能量的吸收和放出过程中的选择定则

1.3 对易关系和不确定性关系

在量子力学中，描述粒子运动的坐标 $\boldsymbol{r}$ 和动量 $\boldsymbol{p}$ 是作用于波函数 $\psi(\boldsymbol{r},t)$ 上