

陈余 著

量子连续变量系统的 信道和纠缠



科学出版社
www.sciencep.com

量子连续变量系统的 信道和纠缠

陈余小 著

科学出版社

北 京

内 容 简 介

本书系统、详细地介绍了量子信道用于传输经典信息的经典容量,用于传输量子信息的量子容量及其编码定理,以及量子纠错编码的基本理论,论述了经典容量的不可加性和量子容量的不可加性.在此一般框架下,着重研究了量子连续变量系统的信道和纠缠两个相互联系的论题,研究了量子高斯信道的经典容量、一些特殊的量子高斯信道的量子容量或其上下界、量子高斯态和非高斯态的纠缠和可分离性准则,最后研究了量子连续变量态包括 NOON 态的演化.

本书适用于通信、计算机及物理等学科领域中以量子信息为研究方向的高年级本科生、研究生、教师和科研人员,也可以作为量子信息高级课程的参考资料.

图书在版编目(CIP)数据

量子连续变量系统的信道和纠缠/陈小余著. —北京: 科学出版社, 2010

ISBN 978-7-03-027411-3

I. 量… II. 陈… III. 量子力学-信息技术-研究 IV. O413.1

中国版本图书馆 CIP 数据核字 (2010) 第 079921 号

责任编辑: 刘凤娟 / 责任校对: 陈玉凤

责任印制: 钱玉芬 / 封面设计: 王 浩

科学出版社出版

北京东黄城根北街 16 号

邮政编码: 100717

<http://www.sciencep.com>

源海印刷有限责任公司印刷

科学出版社发行 各地新华书店经销

*

2010 年 6 月第 一 版 开本: B5 (720×1000)

2010 年 6 月第一次印刷 印张: 14 1/2

印数: 1—2 000 字数: 280 000

定价: 48.00 元

(如有印装质量问题, 我社负责调换)

前 言

量子信道,特别是量子高斯信道容量具有重要的信息论意义.像经典信息系统分为模拟和数字系统一样,量子信息系统分为量子比特系统和连续变量系统.在所有的连续变量量子态中,量子高斯态在实用上最重要,基本上包含了所有在实验上能实现的连续变量系统,而且理论上简单,并易于解析处理有关问题.量子信道的容量有两类:一类是用量子信道传输经典信息,如在光纤上传输 0、1 串,量子态为已知,这时我们谈论经典信息容量;另一类是量子信道传输未知的量子态,这时我们要考虑的是量子信息,是整个希尔伯特空间的传输,其内部的态、纠缠等包含量子相位信息的部分不能被破坏.本书将系统叙述量子信道对经典信息传输和量子信息传输的编码定理,着重讨论量子连续变量系统的信息在信道中的传输特性及态的纠缠,包括高斯系统和非高斯系统.

第 1 章简介了量子信息论,引入一些必要的符号和量子态、量子信道、量子测量以及信源的熵.

第 2 章回顾了量子信道传输经典信息的编码定理以及经典容量的一般结果.列出了在输入乘积态输出纠缠测量时的经典通信容量的 Holevo-Schumacher-Westmoreland 定理,和发送者与接收者间有量子纠缠作为辅助时的经典通信容量的 Bennett-Shor-Smolín-Thapliyal 定理.

第 3 章叙述了玻色量子高斯态和量子高斯信道.研究和计算了量子纠缠辅助下输入功率受限时的单模热辐射噪声信道以传输经典信息的容量,给出单模压缩信道的相应问题的计算方法.对热噪声信道,表明了容量在输入信号为热噪声信号时达到,压缩态无助于达到信道容量;对于压缩信道,容量一般在输入压缩态时达到.给出经典容量严格可求的例子——单纯衰减信道.

关于量子信息的传输的有关内容,放在第 4~6 章讨论,分别涉及量子容量、量子纠错码和量子纠缠.

第 4 章首先介绍量子信道的量子容量,研究了双边量子高斯态的纠缠的上下限.给出量子高斯混合态的三种界限,用只有两个参数的叫做压缩热态的量子高斯态来检验它们是否是较好的上下限,同时计算了态的相干信息以作比较.根据 Horodecki 等的研究,纠缠态的相干信息推测是单向蒸馏纠缠的下限,该假设称为散列不等式,对证明有噪信道编码定理至关重要.2005 年证明了量子信道编码定理,我们采用直接编码证明的方法系统地予以介绍.讨论了由 Holevo 和 Werner 引入的量子高斯

信道量子容量的上界及由量子编码所确定的下界. 高斯信道量子容量的迷人特征是普朗克常量 $\hbar$ 取代了经典容量中输入信号功率限制条件的位置.

第 5 章介绍了量子纠错码的基本理论, 介绍了量子连续变量编码.

第 6 章介绍了纠缠的一般理论、可分离性条件、可蒸馏条件以及对量子高斯态的应用, 研究了三模高斯态的分类和分离条件. 研究纠缠测度对量子高斯态的应用, 着重于量子高斯相对熵纠缠.

第 7 章研究量子非高斯态, 对一大类高斯态经相位衰减后得到的非高斯态, 给出了 Peres-Horodecki 完全条件. 也就是由部分转置密度矩阵的负本征值中最小的一个 (绝对值最大) 确定纠缠的充分条件. 用 Fock 空间可分离准则刻画量子非高斯态的纠缠, 并与基于各阶矩的准则比较.

第 8 章研究量子连续变量态的时间演化, 引入特性函数的微分方程代替密度算符的演化主方程, 求解微分方程以后, 通过算符有序乘积下的积分得到密度算符的演化公式. 应用于 NOON 态等非高斯态的演化.

由于量子信息论是正在发展的学科, 许多问题还没有结论, 论述必然是不完备的. 另外, 作者学识所限, 本书中难免有不妥之处, 望读者批评指正.

本书的出版得到了国家自然科学基金资助 (资助号: 10347119、10575092、10711240141、60972071).

目 录

前言

第 1 章	量子信息导论	1
1.1	引言	1
1.2	可观察量的代数	3
1.3	纯态和混合态	4
1.4	分离态和纠缠态	6
1.5	信道	7
1.6	么正变换和测量作为信道的两个例子	8
1.7	量子态的熵	8
第 2 章	量子信道的经典容量	10
2.1	量子信道经典容量概述	10
2.1.1	定义与记号	10
2.1.2	定理梗概	13
2.2	发送端纠缠	13
2.3	接收端纠缠测量	14
2.3.1	混合态编码, Holevo 信息的引入	14
2.3.2	可达信息	16
2.3.3	Holevo 界	17
2.3.4	Holevo 界的可达性	19
2.3.5	信道容量	20
2.4	纠缠发送纠缠接收信道	21
2.4.1	信道噪声的测度	22
2.4.2	纠缠破坏信道	23
2.4.3	保一量子比特信道	26
2.5	量子多接入信道的经典容量的非可加性效应	29
2.5.1	容量区域与几何和	29
2.5.2	基本反例信道	30
第 3 章	量子高斯信道的经典容量	33
3.1	量子高斯态	34
3.2	高斯信道	37

3.3	CQ 高斯信道的经典容量	40
3.4	限于高斯态输入的高斯信道	43
3.5	高斯纠缠的密集编码	46
3.6	量子高斯信道的纠缠辅助经典容量	48
3.6.1	单模热噪声信道的纠缠辅助容量	49
3.6.2	单模压缩信道的纠缠辅助容量的计算方法	52
3.7	玻色衰减信道的经典容量	53
第 4 章	量子信道的量子容量	56
4.1	码率与量子编码定理	56
4.2	量子擦除信道	57
4.3	量子热噪声信道上的相干信息	59
4.3.1	量子热噪声信道	60
4.3.2	相干信息	64
4.4	量子热噪声信道的量子容量的上下限	64
4.5	单纯衰减信道的量子容量	66
4.6	量子编码定理的证明	68
4.6.1	绪论	68
4.6.2	量子纠错和量子容量	69
4.6.3	编码纠缠保真度的下界	72
4.6.4	量子随机码	75
4.6.5	选择性噪声下的纠错	79
4.6.6	量子容量的下界	81
4.6.7	一些关系式	88
第 5 章	量子纠错码	94
5.1	量子纠错编码的准则	94
5.2	例子: 量子纠错 8 编 3 等价码	99
5.2.1	量子纠错码的错误类型群	99
5.2.2	稳定子的普遍形式	100
5.2.3	关于稳定子 H 群的生成元相互对易的证明	101
5.2.4	码字	101
5.3	确定量子纠错循环码的一种方法及一类量子纠错循环码	102
5.3.1	最小的纠两位随机量子错误的量子纠错码	103
5.3.2	二次剩余用以构造量子码	104
5.4	量子高斯态的嵌入编码	105
5.4.1	量子底特系统的稳定子码	106

5.4.2	连续变量系统的量子纠错码	107
5.4.3	从有效球包限得到的可达码率	111
第 6 章	量子高斯态的纠缠	113
6.1	纠缠与量子容量的关系	113
6.2	高斯态量子纠缠定性理论	114
6.2.1	量子纠缠的一般性质	115
6.2.2	高斯态的纠缠特性	116
6.2.3	小结及纠缠度量理论概略	129
6.3	量子高斯态纠缠的上下界	129
6.3.1	热压缩态	130
6.3.2	纠缠下限	132
6.3.3	生成纠缠的上限	134
6.3.4	相对熵纠缠测度的上限	136
6.3.5	散列不等式和纠缠限的比较	137
6.3.6	讨论	139
6.4	三组分压缩热态的纠缠界	139
6.4.1	多组分压缩热态	140
6.4.2	$1 \times 1 \times 1$ 型压缩热态的可分离性	142
6.4.3	相对熵和纠缠界	144
6.5	高斯相对熵纠缠	146
6.5.1	二次方算符矩阵	148
6.5.2	高斯相对熵纠缠和边界态	151
6.5.3	高斯相对熵纠缠和 1×1 型高斯态的分类	155
6.5.4	1×1 型高斯态系统的指数二次方矩阵	160
第 7 章	量子非高斯态的纠缠	163
7.1	x - p 对称态的同时振幅和相位衰减	163
7.1.1	特性函数的时间演化	163
7.1.2	PPT 可分离性	165
7.1.3	可分离性	169
7.1.4	积分公式	171
7.2	Fock 空间表示的两组分连续变量量子态的不可分离性准则	172
第 8 章	量子连续变量态的演化	180
8.1	量子连续变量态演化的特征函数和纠缠	180
8.1.1	特征函数的时间演化	180
8.1.2	一些特殊情况的解	182

8.1.3 参量放大器和相位衰减	182
8.1.4 单模高斯系统	184
8.1.5 双模高斯系统	186
8.2 双模高斯态同时放大和非对称振幅衰减	190
8.2.1 跨模放大器	191
8.2.2 对称放大器	193
8.2.3 剩余矩阵 α 和 β	194
8.3 放大和对称衰减下双模高斯态的可分离性	195
8.3.1 双模高斯系统的对称衰减	196
8.3.2 对称放大	197
8.3.3 非对称放大	199
8.3.4 对称衰减系统剩余复相关矩阵的解	200
8.4 衰减 NOON 态的纠缠和相位测量性能	202
8.4.1 消相干	202
8.4.2 衰减态的纠缠	203
8.4.3 纠缠增强相位测量中衰减态的性能	206
8.4.4 极值态的证明	209
参考文献	212

第 1 章 量子信息导论

1.1 引言

量子力学的最基础部分对信息和计算产生了影响, Einstein、Podolsky 和 Rosen 于 1935 年指出, 考虑量子力学, 就存在所谓的纠缠光子对, 即使在以后它们之间在空间相隔任意远而没有相互作用, 测量其中的一个光子的偏振就可以确定另一个光子的偏振状态. 而根据“局域实在论”观点, 对于两个分离开的并且没有相互作用的系统, 对其中一个的测量不能改变对另一个的系统状态的描述, 也就是不存在超距作用. 这被称为 EPR 两难问题. Bohm 试图给量子纠缠现象以隐变量理论解释. J. Bell 在 1964 年指出量子力学的预言不可能由任何局域隐变量理论所重现. Bell 实际上指出量子信息可以被编码于系统的不同部分之间的非局域关联之中, 这种关联没有经典对应. 1982 年 Aspect 的实验证实了量子非局域纠缠确实存在.

量子计算机的研究发端于对可逆计算机的寻求, R. Landauer (IBM 工程师) 于 1961 年指出, 信息的擦除是一个耗散过程, 是不可逆的. 对于简单的与门、或门、异或门, 两个输入导致一个输出, 过程是不可逆的, 我们不可能从一个输出恢复出原来的两个输入. 而根据热力学, 不可逆过程必然导致熵的增加, 系统要向环境放热, 这导致芯片在计算过程中的发热, 限制了其信息处理能力. Bennett 于 1973 年指出任何计算都可以只由可逆的操作来构造, 如与门, 我们可以将其中的一个输入直接引出, 和与门结果一起就有两个输出, 从而是可逆的, 这时计算不需要能量消耗. Wootters、Zurek 和 Dieks 于 1982 年证明了量子不可克隆定理. 量子计算的能力在 1982 年就被 Benioff 和 Feynman 独立地指出. 1985 年 Deutsch 提出量子并行计算. 1994 年 Shor 阐明可以进行快速的大数因子分解.

量子信息和量子计算受到广泛的关注. 可能造就的新技术如安全的量子密码术、量子超级计算机、解决经典方法无法处理的问题的能力等不仅激励着研究者也引起民众的兴趣.

那么何谓量子信息? 我们引用 Werner 在一篇综述文章^[1] 中的定义作答:

所谓量子信息, 是这样一种信息, 它在量子力学实验中被量子系统从制备装置带到测量设备上.

故量子信息的“发送者”就是制备量子粒子的装置, “接收者”则是测量仪器. 不过, 这等于什么都没说. 但是, 在经典信息理论的观点看来, 这样的叙述就已经是够奇怪的了. 因为在经典信息论中, 人们通常不关心信息的物理载体, 否则就要区

分“电信息”、“磁信息”、“印刷信息”以及其他许多种信息. 实际上, 经典信息论的成功很大程度上依赖于从物理载体上抽象出来的、走到根本的信息交换的一般原理. 这种抽象之所以成功是因为我们很容易将信息在不同的载体或类型之间转换, 如导线上的电流、光纤上的激光脉冲、纸上的字符, 之间的转换不会丢失数据, 即使丢失也知道怎样恢复和处理. 但是量子信息理论打破了这种信息转换的观点, 因为将量子信息无损地转换为经典信息是不可能的, 故量子信息是一类新的信息.

将量子信息先转换为经典信息然后再转换回量子信息的过程被 Werner 称为经典隐形传态 (teleportation), 最后产生的状态与输入时的状态“不可区分”. 这样一个装置是不可能存在的, 其不可能性可以通过其他“不可能机”追溯到量子力学基本原理. 因为假如能够进行经典隐形传态, 我们可以在中间的经典信息阶段进行复制, 然后转换为量子信息, 总的过程等价于量子复制, 从量子不可克隆定理知道这是一种不可能机. 如果量子克隆是可能的, 我们就可以利用克隆进行不对易量的同时测量, 如输入系统 C 的输出是 A 和 B , A 和 B 都是与 C 一样的量子态, 那么我们可以进行如下的测量, 如用 A 来测量动量, 用 B 来测量位置, 总的过程等价于对 C 同时进行动量和位置的精确测量, 由量子力学的基本原理知道这是一种不可能机.

我们能用量子信息做些什么?

第 1 个回答^[2]: 实际上现代信息处理中的所有信息是加载于微观粒子 (如电子、光子) 之上的, 因此量子信息自然要起作用. 现在人们可以忽略这一点, 仅仅用经典信息论描述所有有关的过程而不出问题. 但是, 如果在典型的线路上元件的大小减小到某一界限, 经典信息论将不再有效, 量子信息论将进入角色.

第 2 个回答: 虽然具体哪一项量子信息技术在将来会出现还很难说, 理论上已经指出基于量子信息的装置能比经典信息更好地处理解决某些实际问题. 其中最著名的无疑是量子计算, 其基本思想可以粗略地描述为: 量子计算机不只是对每个寄存器上的一个数进行处理, 而是可对这些数的叠加进行操作. 这种可能性导致对某类经典不可解问题的计算速度指数增长, 如 Shor^[3, 4] 的因子分解算法. 另一个接近实用的是量子密码术, 量子测量不可避免地影响被测量子系统这一原理被用于密钥的安全传送 (任何窃听都可探测到).

第 3 个回答: 用信息的观点讨论量子力学在许多情况下能够加深对量子理论的更定量的理解, 其中最明显的例子是纠缠, 即量子系统之间的非经典相关. 纠缠是量子力学区别于经典物理的最显著的特征, 这可以由检验 Bell 不等式的实验, 如 Aspect 等^[5] 实验看出. 但是, 纠缠长期以来被认为是量子力学基础之外的一种特性. 在量子信息中, 纠缠是一种基本的资源, 如在量子隐形传态的实验中^[6~8], 量子隐形传态是利用纠缠传送未知量子态^[9], 这时发送者与接收者之间共享一对纠缠粒子对, 发送者对未知量子态和她自己拥有的纠缠部分进行联合测量, 把测量结果通

过经典信道发送给接收者,接收者根据测量结果对他自己拥有的纠缠部分进行适当的操作,就能得到未知的量子态.量子信息论还对计算机理论中的基本假设——丘奇-图灵假设提出挑战.

如何在实验上实现?首先是量子计算,需要有量子比特、量子门和读出装置.一种方法是捕陷离子技术^[10, 11].量子寄存器由内部高真空的 Paul 陷阱中的电磁场所保持的一串离子来实现,选用每个离子的两个长寿命态代表“0”和“1”.激光束可用来操纵每个量子离子从而可实现所有的单量子比特门.得到双量子比特门要用离子的集体运动态,读出通常用激光束分别照射每一个离子来得到,光束被调到快跃迁,通常只影响到其中的一个量子比特态,然后探测发出的荧光^[12, 13].另一种比较成功的方法是核磁共振量子计算^[14].这时量子比特是一种适当的原子核的不同自旋态,量子门由脉冲长短可控的高频振荡电磁场来实现.这种方法由于是对宏观样品做的,初态的制备和结果的读出都有些问题^[15].这两种方法都不能级联,能做到 10 来个量子比特,做不到成千上万个.有可能解决级联问题的方案有光学晶格中的原子^[16, 17],半导体纳米结构如量子点^[18~21]、约瑟夫森结阵列^[22, 23]等.

其次是量子通信和量子密码术^[24].量子密码术在光纤上可达到 100km 以上的传输距离而仍有可观的码率.用普通的通信光纤已经能在 10km 或更长的距离上产生纠缠光子对^[25],基于纠缠的量子密码分布^[26]、光子隐形传态^[6~8]和超密编码^[27]已得以实现.

以上我们对量子信息作了大概的介绍,进一步的描述需要用到记号和数学.用量子系统进行通信分为两个方面:传送未知的量子态和传输 0、1 串,对应的容量分别为量子容量和经典容量.

经典系统与量子系统有许多区别,在尺度上的宏观对微观,在能谱上的连续对离散,等等.例如,光纤上传送的电磁脉冲可以看成是经典的,但是同一根光纤上传送的单个光子却认为是量子的.最显著的区别是统计方面,多个经典随机变量的联合概率分布总是可以写成各自概率分布乘积的凸线性组合形式,但是在量子情况下一般不具有这样的形式.

我们下面介绍的系统可以是经典的,也可以是量子的.表征系统类型的较好的方法是用可观察量的代数.我们尽可能以与经典系统统一和类比的方式来介绍量子系统的基本概念.

1.2 可观察量的代数

量子力学的基本特征是使用不对易可观察量,因此量子系统的可观察量的代数可以默认为是不对易的,经典系统的可观察量的代数是对易的(阿贝尔的).故不失一般性,量子系统的可观察量的代数是某希尔伯特(内积)空间 $\mathcal{H}$ 上的有界算符

$\mathcal{B}(\mathcal{H})$ 代数, 希尔伯特空间 $\mathcal{H}$ 是线性内积空间, 对 $\mathcal{H}$ 内的任意两个矢量 $|\psi\rangle, |\phi\rangle$ 定义有内积 $\langle\psi|\phi\rangle$. 而对应的经典系统的可观察量代数是紧致集 $\mathcal{X}$ 上的连续复值函数 $C(\mathcal{X})$ 代数.

我们可以用一些具体的例子来说明这些概念. 最简单的经典例子是经典比特, 此时集合 $\mathcal{X}$ 是两个元素的集合 $\{0, 1\}$, 对应的可观察量代数 $C(\mathcal{X})$ 是集合 $\{0, 1\}$ 上的所有复值函数 $f: \mathcal{X} \rightarrow \mathbb{C}$ 的集合, 其中 $\mathbb{C}$ 是复数域. 我们可以认为该可观察量代数的一个元素是定义于两值样本空间 $\mathcal{X}$ 上的一个随机变量. 最简单的量子系统是量子比特, 这时须考虑二维复希尔伯特空间 $\mathcal{H}_2 \approx \mathbb{C}^2$. 可观察量代数正是 2×2 复矩阵的集合 $\mathcal{M}_2$.

一般地, 经典情况下的集 $\mathcal{X}$ 和量子情况下的希尔伯特空间反映了系统的字母表空间的结构. $|\mathcal{X}| = n$ 的集 $\mathcal{X}$ 应与 n 元素字母表空间的经典空间相联系. 类似地, 一个自旋为 s 的量子客体的希尔伯特空间是 $2s+1$ 维的. 我们还可以描述具有可数无穷或不可数的字母表空间的系统, 如经典 Heisenberg 自旋系统, 其 $\mathcal{X}$ 是三维实空间 $\mathbb{R}^3$ 上的单位球面, 而单模电磁场的希尔伯特空间同态于无穷复数序列的平方可求和空间 l^2 .

为简单起见, 可限于有限维空间, 并且集 $\mathcal{X}$ 一般是紧致的, 因为要求可观察量的代数包含恒等元, 在计算中经常将代数的元素按基组展开, $C(\mathcal{X})$ 的正则基组是一集函数 $e_x (x \in \mathcal{X})$, 定义为: 当 $x = y$ 时, $e_x(y) = 1$; 当 $x \neq y$ 时, $e_x(y) = 0$, 任意函数 $f \in C(\mathcal{X})$ 可以展开为 $f = \sum_{x \in \mathcal{X}} f(x)e_x$. 而 $\mathcal{B}(\mathcal{H})$ 的基组的构造是先找出 $\mathcal{H}$ 的正交归一基组 $\{e_i\}$, 然后为 $\mathcal{B}(\mathcal{H})$ 定义“标准矩阵元” $e_{ij} = |e_i\rangle\langle e_j|$.

1.3 纯态和混合态

量子系统和经典系统的可观察量的统计解释是一样的, 都与代数中的正元素有关. $f \in C(\mathcal{X})$ 是正的, 当且仅当 $f(x) \geq 0$ 对所有的 x 成立. $Y \in \mathcal{M}_d(\mathcal{M}_d$ 是 $d \times d$ 复矩阵的集合) 是正的, 当且仅当它是半正定矩阵. 我们现在在可观察量的代数上引入态. 我们考虑的代数 $\mathcal{A}$ 属于 C^* 代数, 对纯经典系统 $\mathcal{A} = C(\mathcal{X})$, 对纯量子系统 $\mathcal{A} = \mathcal{B}(\mathcal{H})$. 代数 $\mathcal{A}$ 上的态是 $\mathcal{A}$ 上的归一的正的线性函数, 是映射 $\omega: \mathcal{A} \rightarrow \mathbb{C}$ 将 $\mathcal{A}$ 中的所有正元素映射为非负数, 且有 $\omega(I_{\mathcal{A}}) = 1$, 其中 $I_{\mathcal{A}}$ 是 $\mathcal{A}$ 的恒等元. 数 $\omega(\mathcal{A})$ 给出可观察量 $\mathcal{A}$ 在系统的态 ω 中测量的期望值, 每一个态都完备描述了系统制备方法, 这些与系统的后续统计测量有关.

对量子信息特别有用的是 $\mathcal{A}$ 的子集, 包含的元素 E 满足 $E \geq 0$ 和 $I_{\mathcal{A}} - E \geq 0$ (合写为 $0 \leq E \leq I_{\mathcal{A}}$), 这些可观察量称为“效应”, 对任何效应 E 和任意态 ω , 有 $0 \leq \omega(E) \leq I_{\mathcal{A}}$. 给定集合 $\{E_a\}$, $\sum_a E_a = I_{\mathcal{A}}$, 有 $\sum_a \omega(E_a) = 1$, 因而, 对系统施行

的实验的每一个结果,不论是经典的还是量子的,都可以与一个效应 E_o 相联系,当系统处于态 ω 时,得到相应输出结果的概率是 $\omega(E_o)$. 若用 $\mathcal{O}$ 表示实验的所有可能的输出结果,则有 $\sum_{o \in \mathcal{O}} \omega(E_o) = 1$.

若 ω 是代数 $C(\mathcal{X})$ 上的态,则很明显有 $0 \leq \omega(e_x) \leq 1$ 对所有的 $x \in \mathcal{X}$ 成立,这可由 $\omega(I_A) = \sum_x \omega(e_x) = 1$ 和 ω 的正定性得到. 可见代数 $C(\mathcal{X})$ 上的任意态 ω 给出 $\mathcal{X}$ 上的概率分布 $\{p_x\}$, 其中 $p_x = \omega(e_x)$. 相反地,给定 $\mathcal{X}$ 上的概率分布 $\{p_x\}$, 可以在 $C(\mathcal{X})$ 上显式地定义正的归一的线性函数. 故 $C(\mathcal{X})$ 上的态和 $\mathcal{X}$ 上的概率分布具有一一对应的关系.

类似地,给定量子系统的代数 $B(\mathcal{H})$ 上的态 ω , 可以将它与矩阵 ρ 相联系,在基组 $\{e_i\}$ 下,其元素为 $\rho_{ij} = \omega(e_{ji})$. 给定 $B(\mathcal{H})$ 上的任意元素 $X = \sum_{ij} X_{ij} e_{ij}$, 有 $\omega(X) = \sum_{ij} X_{ij} \rho_{ji} \equiv \text{tr}(\rho X)$. 矩阵 ρ 的迹为 1, 这是因为 $\omega(I_A) = \sum_i \omega(e_{ii}) = \sum_i \rho_{ii} = \text{tr}(\rho)$. 同时可看出 ρ 是正定的, 因为对任意的 $\psi \in \mathcal{H}$, 有 $\langle \psi | \rho | \psi \rangle = \omega(|\psi\rangle\langle\psi|) \geq 0$. 相反,给定迹为 1 的半正定矩阵 ρ , 我们可以令 $\omega(e_{ij}) = \text{tr}(\rho e_{ij}) \equiv \rho_{ji}$. 可见,当系统的希尔伯特空间 $\mathcal{H}$ 具有有限的维数 n 时, $B(\mathcal{H})$ 上的态与迹为 1 的半正定 $n \times n$ 矩阵之间存在一一对应关系,该矩阵称为密度矩阵或密度算符. 对无限维的 $\mathcal{H}$ 这是不成立的,不是 $B(\mathcal{H})$ 上的每一个态 ω 都对应于一个密度算符. 有密度算符相对应的态称为正规态.

代数 $\mathcal{A}$ 上的态集 $S(\mathcal{A})$ 是凸集,其边界点对应的态称为纯态. 纯态作为集 $S(\mathcal{A})$ 上的边界点,不能写成其他态的非平凡的凸线性组合. 对 $C(\mathcal{X})$ 上的纯态对应于 $y \in \mathcal{X}$ 点上的概率测度 δ_y , 称为点测度. 对量子系统,有限维系统的代数 $B(\mathcal{H})$ 上的态集与 $\mathcal{H}$ 上的密度算符的凸集 $S(\mathcal{H})$ 存在一一对应关系,同时 $B(\mathcal{H})$ 上的态集的凸线性组合对应于 $\mathcal{H}$ 上的密度算符的凸线性组合. 故集的相应边界也是一一对应的. $S(\mathcal{H})$ 的边界是一维投影算符,其密度算符满足 $\rho^2 = \rho$. 纯态对应于 $\mathcal{H}$ 中的矢量 $\psi \in \mathcal{H}$. 经典的纯态是概率集中于一个点上的情况,即对某一 $z \in \mathcal{X}$, 有 $p_z = 1$. 在量子系统中,纯态为 $\rho = |\psi\rangle\langle\psi|$. 经典比特情况纯态就是两个端点,即以概率 1 出现的 0 和以概率 1 出现的 1. 在量子比特的情况下,边界点连成三维空间的单位球面. 态为

$$\rho = \frac{1}{2} \begin{bmatrix} 1 + x_3 & x_1 - ix_2 \\ x_1 + ix_2 & 1 - x_3 \end{bmatrix}, \quad (1.1)$$

态的正定性要求 $|x|^2 \leq 1$, 等号对应于边界,即纯态的 ρ . 量子比特纯态单位球面的北极 $|+\rangle$ 和南极 $|-\rangle$ 粗略地对应于经典比特的两个端点,但我们还有其相干叠加态

$\alpha|+\rangle + \beta|-\rangle$, 其中, $\alpha, \beta \in \mathbf{C}$, $|\alpha|^2 + |\beta|^2 = 1$. 这额外的自由度是量子信息的关键所在, 也是量子并行计算的基础.

不是纯态的态都叫混合态, 它们对应于态空间中的非边界点, $C(\mathcal{X})$ 上的任意混合态都可以表示为 $\mathcal{X}$ 上的点测度的凸混合, 而 $B(\mathcal{H})$ 上的任意混合态可以表示为 $\mathcal{H}$ 上的一维投影算符的凸混合. 不论是经典还是量子情况, 对纯态的凸组合都可以认为是引入了“经典”的随机性. 一个重要的态是所谓最大混合态, 也就是最随机的态. 经典可观察量代数 $C(X)$ 上的最大混合态对应于 $\mathcal{X}$ 上的归一化计数测度, 该测度赋予每一个 $x \in \mathcal{X}$ 以值 $1/|\mathcal{X}|$, 也就是等概率测度. $B(\mathcal{H})$ 上的最大混合态对应于归一化恒等矩阵, 即 $I/\dim(\mathcal{H})$.

1.4 分离态和纠缠态

复合系统可以用张量积的方法来构造, 在经典情况下, 设 $\mathcal{A} = C(\mathcal{X})$, $\mathcal{B} = C(\mathcal{Y})$, 复合系统 $\mathcal{A} \otimes \mathcal{B}$ 的纯态对应于点测度 $\delta_{x,y} \equiv \delta_x \otimes \delta_y$, 因而 $C(\mathcal{X}) \otimes C(\mathcal{Y})$ 上的任意态具有形式 $\omega = \sum_{x,y} p_{xy} \delta_x \otimes \delta_y$, 其中 $0 \leq p_{xy} \leq 1$, $\sum_{x,y} p_{xy} = 1$, 它可以写成乘积测度的凸组合. 但是对于希尔伯特空间 $\mathcal{H}$ 和 $\mathcal{K}$ 上的代数的张量积 $B(\mathcal{H}) \otimes B(\mathcal{K})$ 上的态而言却不具备这样的性质. 纯态还是对应于 $\mathcal{H} \otimes \mathcal{K}$ 上的矢量, 但是张量积理论的一个基本点是并非 $\mathcal{H} \otimes \mathcal{K}$ 中的每一个矢量都可以写成各空间中的矢量的直乘积 $\psi \otimes \phi$, 其中 $\psi \in \mathcal{H}, \phi \in \mathcal{K}$, 故在下述意义上复合量子系统的各态并非都是可分的.

定义 1.1 若具有可观察量代数 $\mathcal{A} \otimes \mathcal{B}$ 的复合系统上的态 ω 可以写成

$$\omega = \sum_i p_i \omega_i^{\mathcal{A}} \otimes \omega_i^{\mathcal{B}}, \quad (1.2)$$

则 ω 称为可分离的, 其中 $\omega_i^{\mathcal{A}} \in \mathcal{S}(\mathcal{A})$, $\omega_i^{\mathcal{B}} \in \mathcal{S}(\mathcal{B})$, 权重 p_i 非平凡. 若不能写为上述形式, 则 ω 称为纠缠的.

纠缠态的最简单的例子是 Bell 基组. 令 $|e_1\rangle, |e_2\rangle$ 是 $\mathbf{C}^2$ 中的正交归一基组, 则

$$|\Psi_1^+\rangle = \frac{1}{\sqrt{2}}(|e_1\rangle \otimes |e_1\rangle + |e_2\rangle \otimes |e_2\rangle), \quad (1.3)$$

$$|\Psi_2^+\rangle = \frac{1}{\sqrt{2}}(|e_1\rangle \otimes |e_2\rangle + |e_2\rangle \otimes |e_1\rangle), \quad (1.4)$$

$$|\Psi_1^-\rangle = \frac{1}{\sqrt{2}}(|e_1\rangle \otimes |e_1\rangle - |e_2\rangle \otimes |e_2\rangle), \quad (1.5)$$

$$|\Psi_2^-\rangle = \frac{1}{\sqrt{2}}(|e_1\rangle \otimes |e_2\rangle - |e_2\rangle \otimes |e_1\rangle), \quad (1.6)$$

这些纯态都是纠缠的, 称为 Bell 基组. 对任意混合态 ρ , 确定它是否是可分离的是一项困难的工作.

1.5 信 道

在引入量子系统和经典系统的可观察量的代数和态的概念之后, 还需要对施于系统上的任意处理过程进行描述. 本书主要描述量子系统. 量子信息的任何处理步骤都可以用“信道”的作用来表示, 这覆盖了各种不同的操作, 从态的制备到时间演化以及测量. 信道输入和输出可以是经典信息及量子信息的任意组合, 信道的数学描述的基本要点是根据它对后续测量的影响方式来表达它. 设信道的作用将系统从代数 $\mathcal{A}$ 转化为代数 $\mathcal{B}$, 对“新”的系统, 测量到效应 $F \in \mathcal{B}$, 但是也可以将一系列的作用看成是对“原”系统的某一效应 $F' \in \mathcal{A}$ 的测量, 因而信道的作用可以看成是将 $\mathcal{B}$ 上的效应转化为 $\mathcal{A}$ 上的效应的一个变换 $\hat{\Phi}$, $F' = \hat{\Phi}(F)$. 信道可以用映射 $\hat{\Phi} : \mathcal{B} \rightarrow \mathcal{A}$ 来表示. 当然, 信道的作用也可以看成是将 $\mathcal{A}$ 上的态转化为 $\mathcal{B}$ 上的态的变换 Φ . 很明显, 对信道作用的这两种解释应该在统计的意义上等价 (分别对应于海森伯表象和薛定谔表象), 故对 $\mathcal{A}$ 上的任意态 ω 和 $\mathcal{B}$ 上的任意可观察量 X , 有

$$(\Phi(\omega))(X) = \omega(\hat{\Phi}(X)), \quad (1.7)$$

这表示任何测量的期望值关于 $\hat{\Phi}$ 和 Φ 是一样的. 由信道的描述可以导出信道的一些性质, $\hat{\Phi}$ 是线性的正定的映射, 同时还要求将恒等效应 $I_{\mathcal{B}}$ 映射为 $I_{\mathcal{A}}$, $\hat{\Phi}$ 还是保一的映射. 对偶映射 Φ 对态的作用也可以认为是将 $\mathcal{A}$ 中的密度算符映射为 $\mathcal{B}$ 中的密度算符. 故方程 (1.7) 可以改写为 $\text{tr}[\hat{\Phi}(\rho)X] = \text{tr}[\rho \text{tr}(X)]$, 若令 $X = I_{\mathcal{A}}$, 因为 $\hat{\Phi}$ 是保一的, 我们得到 Φ 是保迹的并且正定, $\text{tr}[\Phi\rho] = \text{tr}\rho$, 因而密度算符被映射为密度算符.

映射 $\hat{\Phi}$ 和 Φ 仅有正定性还不够, 在许多情况下我们需要考虑同时对多个量子系统实施处理, 如变换 $\hat{\Psi} \otimes \hat{\Phi} : \mathcal{B}_1 \otimes \mathcal{B}_2 \rightarrow \mathcal{A}_1 \otimes \mathcal{A}_2$, 其中 $\mathcal{A}_1, \mathcal{A}_2, \mathcal{B}_1, \mathcal{B}_2$ 是可观察量代数. 为使处理过程具有物理意义, $\hat{\Psi}$ 和 $\hat{\Phi}$ 必须是线性正定保一的映射, 但是两个正定映射的乘积在量子情况下可能不再具有正定性. 而对信道我们要求完全正定性.

定义 1.2 令 $\hat{\Phi} : \mathcal{B} \rightarrow \mathcal{A}$ 是算符代数间的映射, 定义映射 $\hat{\Phi}_n : \mathcal{B} \otimes \mathcal{M}_n \rightarrow \mathcal{A} \otimes \mathcal{M}_n$, $\hat{\Phi}_n = \hat{\Phi} \otimes I$, I 为恒等映射. 若 $\hat{\Phi}_n$ 正定, 则称 $\hat{\Phi}$ 为 n 正定的. 若对所有的 n , $\hat{\Phi}_n$ 都正定, 则 $\hat{\Phi}$ 称为完全正定的.

对两个完全正定的映射, 可以证明其复合映射是正定的. 信道可定义如下.

定义 1.3 将具有可观察量代数 $\mathcal{B}$ 的系统转化为具有可观察量代数 $\mathcal{A}$ 的系统的信道是完全正定的保一线性映射 $\hat{\Phi} : \mathcal{B} \rightarrow \mathcal{A}$. 其对偶映射 Φ 是完全正定的保迹线性映射.

1.6 么正变换和测量作为信道的两个例子

作为信道的例子, 我们介绍么正变换和量子测量.

么正变换

量子系统的可观察量代数 $\mathcal{A}$ 到自身的可逆映射也是一种信道. 对信道 $\hat{\phi}: \mathcal{A} \rightarrow \mathcal{A}$, 存在逆信道是 $\hat{\psi}$, 使得 $\hat{\psi}\hat{\phi} = \hat{\phi}\hat{\psi} = I_{\mathcal{A}}$. 若 $\hat{\phi}: \mathcal{A} \rightarrow \mathcal{A}$ 是可逆线性映射, 则有 $\hat{\phi}(AB) = \hat{\phi}(A)\hat{\phi}(B)$, $\hat{\phi}(A^+) = \hat{\phi}(A)^+$, 伴随算符的矩阵元由 $(A^+)_{\mu\nu} = A_{\nu\mu}^*$ 给出, 伴随作用由转置和复共轭组成, 称为厄米共厄. 信道的作用可以表达为形式 $\hat{\phi}(A) = UAU^+$, 其中 U 是 $\mathcal{A}$ 的么正 (unitary) 元素, 满足 $U^+U = UU^+ = I_{\mathcal{A}}$.

测量

量子系统用态表示, 要获得态的信息, 需要对态进行测量. 测量也是一种信道, 这种信道的输出是经典代数, 即 $\mathcal{B} = C(\mathcal{X})$. 很明显, $\hat{\phi}: \mathcal{B} \rightarrow \mathcal{A}$ 唯一地确定了算符集 $\{E_a\}$, $F_a = \hat{\phi}(e_a)$, 故 $\hat{\phi}(f) = \sum_a f(a)E_a$. $\hat{\phi}$ 信道具有性质 $E_a \in \mathcal{A}$, $E_a \geq 0$, $\sum_a E_a = I_{\mathcal{A}}$. 恒等算符的拆分 $\{E_a\}$ 或信道 $\hat{\phi}$ 称为 POVM (positive operator valued measure), E_a 与量子力学里定义的可观察量有两点区别. 其输出 $x \in \mathcal{X}$ 有可能是复数, 算符 E_a 不一定是投影算符, 尽管其期望值是得到输出结果 x 的概率. 而量子力学里定义的可观察量是投影算符, 满足 $E_a^2 = E_a$, 也就是所谓的测量相容性, 即重复测量得到相同结果.

标准的量子力学的测量称为冯·诺伊曼测量, 用一集投影算符 $\{P_a\}$ 来表示, 满足 $P_a^2 = P_a$, $P_a^+ = P_a$, 对 $a \neq b$ 有 $P_a P_b = 0$, 且 $\sum_a P_a = I_{\mathcal{H}}$. 投影算符将希尔伯特空间 $\mathcal{H}$ 分解为相互正交的子集.

1.7 量子态的熵

一个量子信源是一个可以制备并发送不同量子信号态的物理装置, 假设量子信源以概率 π_j 产生量子纯态 ρ_j , (或表示为态矢量 $|\psi_j\rangle$, 也称信号或信号态, 这些信号态不必是相互正交的), 令 $\mathcal{E} = \{\pi_j, \rho_j\}$ 表示该输入态系综, 则 $\rho = \sum_j \pi_j \rho_j$ 是信源的信号态系综的密度算符. 不同的系综可以对应同一个密度算符, 从测量所能获得的信息角度而言, 对应于同一个密度算符的不同系综是不可区分的. 仅对相互正交的信号态, 信号态是密度算符的本征态, 其本征值就是该信号态出现的概率. 信源的冯·诺伊曼熵定义为

$$S(\rho) = -\text{tr}(\rho \ln \rho), \quad (1.8)$$