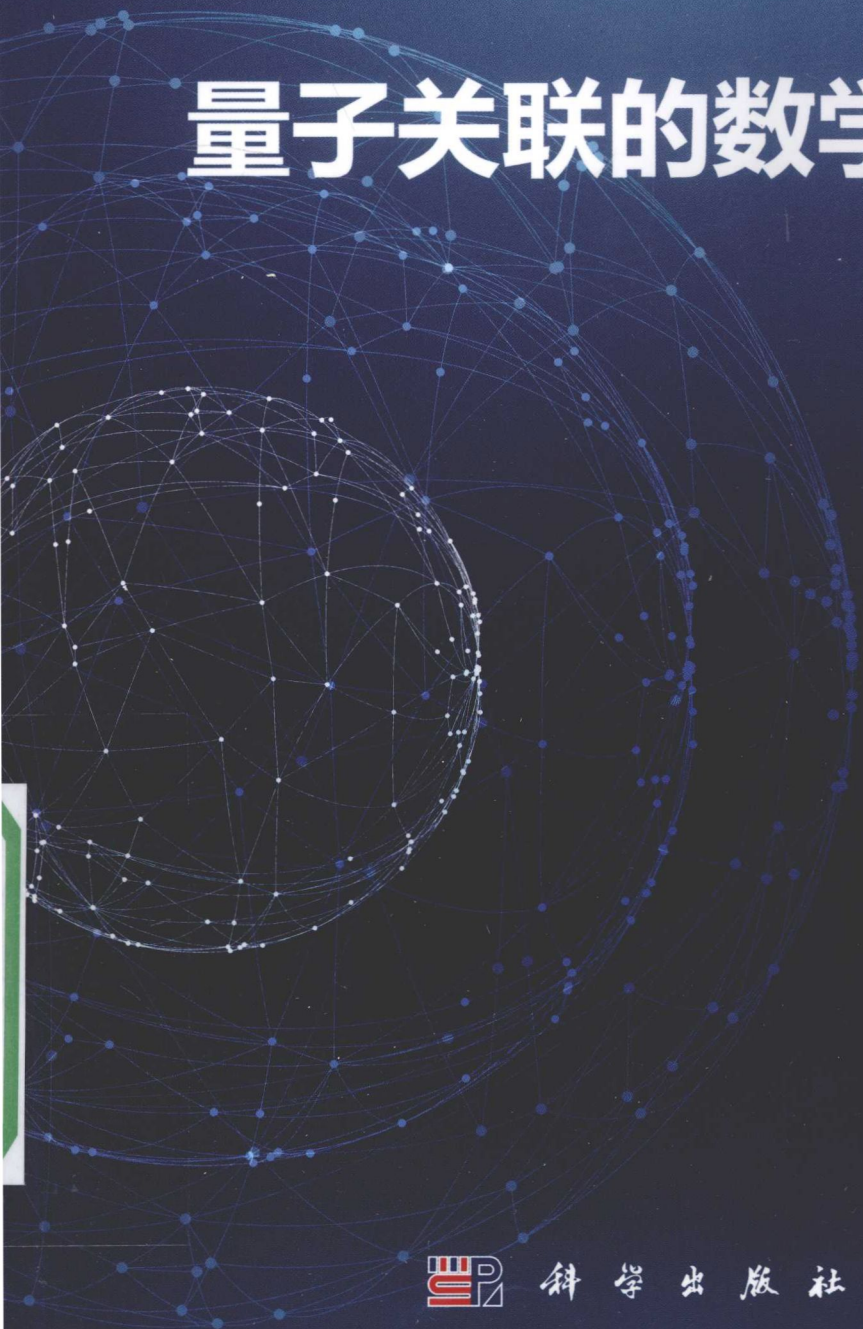
山西大同大学出版基金资助

量子关联的数学刻画

郭钰 著



科学出版社

山西大同大学出版基金资助

量子关联的数学刻画

郭 钰 著

科 学 出 版 社
北 京

内 容 简 介

量子纠缠是存在于复合量子系统之间的一种量子关联. 近年来, 人们发现在没有纠缠的情况下仍然有量子关联存在. 三十多年来, 以量子关联态为载体的信息处理技术在理论和实验上都取得了重要突破. 本书从数学角度主要介绍著者近年来对量子关联的研究成果. 全书共 10 章. 第 1 章介绍量子信息理论的一些基础知识, 第 2–6 章介绍无限维系统的几种量子纠缠判据, 第 7 章介绍纠缠度, 第 8 章介绍几种不同于纠缠的量子关联, 第 9 章讨论几种量子关联在局域量子信道下的演化, 最后一章讨论不可扩张纠缠基和纠缠基.

本书可供量子信息领域的科研人员使用, 也可以作为数学专业和物理学专业高校教师和研究生的量子信息课程参考书.

图书在版编目(CIP)数据

量子关联的数学刻画/郭钰著. —北京: 科学出版社, 2016. 7
ISBN 978-7-03-049434-4

Ⅰ. ①量… Ⅱ. ①郭… Ⅲ. ①量子论—研究 Ⅳ. ①O413

中国版本图书馆 CIP 数据核字 (2016) 第 170988 号

责任编辑: 胡庆家 / 责任校对: 彭 涛
责任印制: 张 伟 / 封面设计: 铭轩堂

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

北京教图印刷有限公司 印刷
科学出版社发行 各地新华书店经销
*
2016 年 7 月第 一 版 开本: 720 × 1000 B5
2016 年 7 月第一次印刷 印张: 17 5/8
字数: 342 000

定价: 98. 00 元

(如有印装质量问题, 我社负责调换)

前　言

数学是科学的语言. 随着各学科的发展, 数学作为工具所发挥的作用已日益明显和重要. 当代数学在向纵深发展的同时, 被空前广泛地应用于几乎一切领域. 尤其是物理学的发展, 一直与数学的发展密不可分. 用数学理论解决物理问题已有几百年的历史. 二十多年来, 以矩阵和算子理论作为主要数学工具的量子信息科学异军突起, 用数学方法分析和解决量子信息和量子计算问题已成为近年来信息科学领域中的热点问题之一. 其中对于以量子纠缠 (quantum entanglement) 为核心的量子关联的研究更是热点问题中的焦点之一.

量子关联对量子力学的基础具有决定性的影响. 人类发现的第一种量子关联是纠缠, 最早是被 Einstein, Podolsky 和 Roson (EPR) 在 20 世纪 30 年代发现的. 这一发现引起了人们对量子力学理论完备性的怀疑. 1964 年爱尔兰物理学家 John Bell 用数学不等式证明了局域隐变量理论是错误的, 肯定了量子力学理论的预测, 从而从理论上证实了这种反常关联现象的合理性. 纠缠至今没有严格的物理定义. 1989 年 Werner[396] 从数学上正式给出纠缠的定义. 此后, 纠缠刻画问题 (也就是如何判断一个复合量子态是否纠缠以及量化一个已知纠缠态的纠缠程度的问题) 受到了物理学领域、数学领域、信息科学领域乃至计算机科学领域的密切关注.

在相当长的时间里, 人们一直以为非纠缠的量子系统是不存在量子关联的, 对量子关联的研究只停留在是否纠缠的问题上. 事实上, 量子关联远不止纠缠, 人们陆续发现了各种不存在纠缠情形下的量子关联现象. 2001 年, Olivier 和 Zurek 提出了量子失协 (quantum discord). 几乎同时, Henderson 和 Vedral 独立地引入了类似的量来研究量子系统中的关联. 2008 年, Luo 引入了测量导致的扰动 (measurement-induced disturbance). 2011 年, Luo 和 Fu 又提出了测量导出的非定域性 (measurement-induced nonlocality). 2014 年, Wu 等提出了基于互补测量的量子关联度量. 此后不久, Guo 和 Wu 把该量子关联一般化, 提出了更本质的关联性. 2015 年 Guo 提出了由测量前后约化态之间的平均距离导出的量子关联度量. 这些量子关联都可以在非纠缠的情形下发生.

自从 1991 年第一个基于纠缠态的量子加密协议提出以来, 人们逐渐开始把量子关联这一非经典的特性应用到信息科学和计算科学中. 已经证明, 利用关联态作为载体的信息技术, 在提高运算速度、确保信息安全和增大信息容量等方面可以突破并远远超过现有经典信息系统功能的极限, 将在未来的保密通信、计算机领域以其独特、不可替代的功能发挥至关重要的作用.

算子理论和算子代数是量子力学的重要数学基础和工具, 特别是无限维量子力学、量子计算、量子信息中的许多问题需要借助算子和算子代数的理论、方法和技巧来加以分析解决. 实际上, 早在 20 世纪 30 年代, 著名的数学家 von Neumann 就曾经预言到 Hilbert 空间上的分析在量子力学的重要性. 事实也正是如此: 每一个孤立的量子系统都对应于一个可分的复 Hilbert 空间, 量子力学研究的就是在这个 Hilbert 空间的数学框架下的系统演化过程, 所有的运算都包容于这个 Hilbert 空间. 比如, 量子态用密度算子来描述, 所谓密度算子就是指所在系统对应的 Hilbert 空间上的迹为 1 的正算子; 观测算子 (observable) 用所在系统对应的 Hilbert 空间上的自伴算子 (可以是无界的) 来表示; 测量结果用观测算子和所考虑量子态的 Hilbert-Schmidt 内积来表示; 量子信道用保迹的正线性映射来描述; 量子操作用迹不增的正线性映射来描述; 量子门一般用酉算子来表示; von Neumann 熵则是通过密度算子来定义的; 量子码用状态空间的子空间来表示. 尤其是刻画量子关联, 从数学的角度考虑, 就是 Hilbert 空间上的算子理论中的算子张量积的相关问题. 本书就是以算子理论和算子代数为工具刻画量子关联.

第 1 章是预备知识, 介绍量子力学中与量子纠缠及其他量子关联相关的基本概念和基本理论以及本书将涉及的已知结论. 第 2 章主要给出无限维两体系统中的纯态纠缠的几个充要条件. 第 3 章给出无限维两体系统量子态的重排定义和可计算交叉范数的定义, 证明量子态的可计算交叉范数与其重排算子的迹范数相等, 进而给出无限维系统的重排判据和可计算交叉范数判据. 我们对重排运算作了详细分析, 并对重排判据与著名的 PPT 判据作了比较. 最后给出可分态都满足的两个不等式. 纠缠 witness 是探测已给量子态是否纠缠的有效工具, 其优点在于它可以通过物理装置在实验室里实现, 因而刻画纠缠 witness 具有重要的理论和实践意义. 第 4 章讨论无限维两体系统纠缠 witness 的性质并给出了两种构造纠缠 witness 的方法. 第 5 章则讨论 SPPT 判据和 SSPPT 判据, 证明 SSPPT 量子态一定是可分的而且这类可分态中包含经典量子态. 第 6 章给出无限维系统的广义部分转置判据、迹不等式判据和约化判据. 第 7 章介绍了几种常见的纠缠度, 主要证明无限维 concurrence 也是纠缠度并给出多体系统 Schmidt 数的一种推广形式. 第 8 章介绍量子失协、测量导出的非定域性、互不偏袒基导出的量子关联、约化态平均距离导出的量子关联, 这四种关联互不相同. 最后给出量子失协的一种非交换性度量, 通过分析几个例子发现这种度量可以用来估算原始量子失协且易于计算, 避免了原始量子失协几乎不可计算的缺陷. 第 9 章则研究量子失协和测量导出的非定域性在局域量子信道下的演化规律, 严格地证明了这两种关联都可以通过 LOCC 产生, 从而说明它们与纠缠有本质区别. 此外, 刻画了保持乘积态的量子信道和保持极大纠缠或 Schmidt 数的局域量子信道. 最后一章系统地研究不可扩张纠缠基和纠缠基, 把不可扩张乘积基和极大纠缠基推广到更一般的情形 —— 具有任意固定 Schmidt

数的不可扩张纠缠基并证明了这种不可扩张纠缠基的存在性, 同时给出了具有任意固定 Schmidt 数的纠缠基概念并给出一般的构造方法.

最后介绍一下书中所用符号. 本书采用量子力学中的惯用符号系统 ——Dirac 符号. 书中 Hilbert 空间均指复 Hilbert 空间, 向量用 ket 符号 $|\cdot\rangle$ 表示, 用 bra-ket 符号 $\langle\cdot|\cdot\rangle$ 表示给定 Hilbert 空间 H 中的内积. 这里, 内积 $\langle\cdot|\cdot\rangle$ 对第一个变量是共轭线性的而对第二个变量是线性的, 即 $(\langle\alpha\psi_1| + \langle\beta\psi_2|)|\phi\rangle = \bar{\alpha}\langle\psi_1|\phi\rangle + \bar{\beta}\langle\psi_2|\phi\rangle$, $\langle\psi|(\alpha|\phi_1\rangle + \beta|\phi_2\rangle) = \alpha\langle\psi|\phi_1\rangle + \beta\langle\psi|\phi_2\rangle$, $\alpha, \beta \in \mathbb{C}$, $\psi_i, \phi_i \in H$, $i = 1, 2$. 这里, $\bar{\alpha}$ 表示 α 的复共轭. 对给定 Hilbert 空间 H, K, $\mathcal{B}(H, K)$ 表示 H 到 K 上的有界线性算子组成的集合 (当 $H = K$ 时, 简记为 $\mathcal{B}(H)$); $\mathcal{C}_2(H, K)$ 表示由 $\mathcal{B}(H, K)$ 中的 Hilbert-Schmidt 类算子组成的 Hilbert 空间, 即 $\mathcal{C}_2(H, K) = \{A \in \mathcal{B}(H, K) : \|A\|_2 = (\mathrm{Tr}(A^\dagger A))^{\frac{1}{2}}\} < +\infty\}$, 其内积 $\langle A|B\rangle = \mathrm{Tr}(A^\dagger B)$, A, $B \in \mathcal{C}_2(H, K)$ (当 $H = K$ 时, 简记为 $\mathcal{C}_2(H)$). $\mathcal{C}_p(H)$ 表示 H 上 Schattern-p 类算子全体组成的 Banach 空间. 当 $p = 1$ 时, 即迹类算子空间, 用 $\mathcal{T}(H, K)$ 来表示 (当 $H = K$ 时, 简记为 $\mathcal{T}(H)$). 对于 H 上的算子 A, $\|A\|_{\mathrm{Tr}}$ 表示 A 的迹范数, $A^\dagger$ 表示 A 的伴随算子, A^T 表示在某组标准正交基下 A 的转置, $\mathrm{ran}(A)$ 表示 A 的值域, $\ker(A)$ 表示 A 的零空间, $\mathrm{rank}(A)$ 表示 A 的秩. 若 $A^\dagger = A$ 且 $\langle\psi|A|\psi\rangle \geqslant 0$ 对所有 (单位) 向量 $|\psi\rangle \in H$ 都成立, 则称 A 为正算子, 记作 $A \geqslant 0$. 若 A 为迹类算子, 则 $\mathrm{Tr}(A)$ 表示对 A 取迹.

本书所基于的研究工作得到了国家自然科学基金 (No.1130 1312) 和山西大同大学著作出版基金的资助, 在此表示衷心的感谢.

由于作者水平有限, 文献收集不全, 再加之研究成果不断更新, 难以反映本研究领域全貌, 疏漏不足之处也在所难免, 敬请读者批评指正.

郭　钰

2016 年 3 月

山西大同大学

目　　录

第 1 章　预 备 知 识

量子信息理论内容十分丰富, 本章主要介绍其中与量子纠缠及其他量子关联相关的基本概念、基本理论和主要结论, 侧重于所涉及每个概念的数学刻画.

1.1　量子力学基本假设

量子力学经过漫长的发展建立了称为量子力学基本假设的公理化体系, 这些假设提供了研究量子物理世界的数学框架.

假设 1　任一孤立的量子系统都与某个可分复 Hilbert 空间 H 相对应, 这个空间称为系统的状态空间. 系统的状态 (即量子态) 用密度算子 $\rho \in \mathcal{B}(H)$ 来描述. 所谓密度算子即迹为 1 的正算子, 即 $\rho \geqslant 0$, $\mathrm{Tr}(\rho) = 1$.

当 $\dim H < +\infty$ 时, 称对应的系统为有限维系统; 当 $\dim H = +\infty$ 时, 称所指系统为无限维系统. 量子态 (或简称为态) 是量子力学中的一个最基本的概念. 有确定状态的量子态称为纯态 (pure state), 或者说, 纯态就是指能用单一波函数描述的状态. 纯态既可用秩为 1 的密度算子 ρ 表示, 也可用单位向量 $|\psi\rangle$ 来表示, 此时 $\rho = |\psi\rangle\langle\psi|$, 且 $|\psi\rangle$ 和 $\mathrm{e}^{\mathrm{i}\theta}|\psi\rangle$ $(0 \leqslant \theta < 2\pi)$ 表示同一个量子状态. 在通常状况下, 我们很难知道量子系统的精确状态, 而只能知道系统以概率 p_i 处于状态 $|\psi_i\rangle \in H$. 在这种情形下, 系统的状态称为混合态. 换言之, 若干个纯态的非相干混合构成了混合态. 比如电子枪中受热金属发射的热电子的自旋状态就是混合态[425]. 混合态既可用密度算子 ρ 来表示也可用系综 (ensemble) $\{p_i, |\psi_i\rangle\}$ 来表示. 此时

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad \sum_i p_i = 1, \quad p_i \geqslant 0. \tag{1.1}$$

显然, ρ 为纯态 $\Leftrightarrow \rho^2 = \rho \Leftrightarrow \mathrm{Tr}(\rho^2) = 1$; ρ 为混合态 $\Leftrightarrow \rho^2 \neq \rho \Leftrightarrow \mathrm{Tr}(\rho^2) < 1$. 密度算子是用来描述系综的, 给定一个系综有一个唯一确定的密度算子. 但反过来不成立, 可以有无限多个不同的系综对应于同一个密度算子. 例如, 在单量子比特系统 (即 2 维系统) 中, 密度算子 $\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$ 对应的系综可以是以概率 $\frac{3}{4}$ 处于状态 $|0\rangle$, 以概率 $\frac{1}{4}$ 处于状态 $|1\rangle$; 也可以是以概率 $\frac{1}{2}$ 处于状态 $\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$, 以概率 $\frac{1}{2}$ 处于状态 $\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle$. 系统的所有态组成的集合用 $\mathcal{S}(H)$ 来表示. 显然

$\mathcal{S}(H)$ 是一个凸集, 其端点为纯态.

以下假设所指系统的状态空间为 H.

假设 2　任一封闭量子系统的演化都对应某个酉变换, 即系统在 t_0 时刻的状态 ρ 和在 t 时刻的状态 ρ' 有如下关系

$$\rho' = U\rho U^\dagger, \tag{1.2}$$

其中 $U \in \mathcal{B}(H)$ 是仅依赖于 t_0 和 t 的酉算子.

需要注意的是, 该假设要求所描述的系统必须是封闭的, 即它与外界不发生任何相互作用. 现实中绝对封闭的系统是几乎不存在的 (除非把宇宙整体看作一个系统), 但可以近似描述为封闭的系统是存在的, 而且至少可以在原则上把每个开放系统认为是一个更大的封闭系统[302].

假设 3　量子测量通过测量算子组 $\{M_i\}$ 来刻画, $M_i \in \mathcal{B}(H)$ 满足完备性

$$\sum_i M_i^\dagger M_i = I, \tag{1.3}$$

下标 i 指可能出现的测量结果, I 表示 $\mathcal{B}(H)$ 中的单位元. 若系统在测量前处于状态 ρ, 则测量得到结果 i 的概率为

$$p_i = \mathrm{Tr}(M_i^\dagger M_i \rho), \tag{1.4}$$

测量后的系统状态为

$$\rho_i' = \frac{M_i \rho M_i^\dagger}{\mathrm{Tr}(M_i \rho M_i^\dagger)}. \tag{1.5}$$

定义 $E_i = M_i^\dagger M_i$, 则 E_i 满足 $\sum\limits_i E_i = I$ 和 $p_i = \mathrm{Tr}(E_i\rho)$. 这样, $\{E_i\}$ 同样可以确定不同测量结果的概率. 此时算子 E_i 称为该测量的 POVM (positive operator-valued measure) 元, 集合 $\{E_m\}$ 称为一个 POVM. 目前最常用的量子测量是投影测量. 当 $\{M_i\}$ 是正交投影算子时, 即 $M_i^\dagger = M_i$ 且 $M_iM_j = \delta_{ij}M_i$, 称该测量为投影测量 (也称 Lüders 测量); 若 $\{M_i\}$ 是一组秩一正交投影算子, 则称其为 von Neumann 测量.

通常, 量子系统是由两个或多个子系统复合而成的, 即复合量子系统. 关于复合系统, 有如下假设.

假设 4　复合系统的状态空间是其子系统状态空间的张量积. 即若子系统的状态空间分别是 $H_1, H_2, \cdots, H_n$, 复合系统的状态空间则为 $H_1 \otimes H_2 \otimes \cdots \otimes H_n$. 若第 i 个子系统的状态为 $|\psi_i\rangle \in H_i$, 则整个系统的状态为 $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$.

本书主要研究两体复合系统 A+B. 若系统 A 对应于 Hilbert 空间 H_a, 系统 B 对应于 Hilbert 空间 H_b, 则由 A 和 B 组成的两体复合系统 A+B 的状态空间用空间张量积 $H = H_a \otimes H_b$ 来描述. 设 $N_a = \dim H_a$, $N_b = \dim H_b$, N_a 和 N_b 可能为 $+\infty$, $\{|m\rangle\}_{m=1}^{N_a}$, $\{|\mu\rangle\}_{\mu=1}^{N_b}$ 分别为 H_a 和 H_b 的标准正交基. 显然, $\{|m\rangle|\mu\rangle = |m,\mu\rangle = |m\rangle \otimes |\mu\rangle\}$ 是 $H_a \otimes H_b$ 的一组标准正交基. 在这组基下, 纯态 $|\psi\rangle \in H_a \otimes H_b$ 总可以表示为

$$|\psi\rangle = \sum_{m,\mu} d_{m\mu}|m\rangle|\mu\rangle. \tag{1.6}$$

在量子信息理论中, 除特别声明外, 由序数 m (i 或其他字母) 所表示的向量组 $\{|m\rangle\}$ 均指所对应空间标准正交基 (集). 本书用 $\mathcal{S}(H_a)$, $\mathcal{S}(H_b)$ 和 $\mathcal{S}(H_a \otimes H_b)$ 分别表示系统 A, B 和 A+B 中的量子态的集合. 此外, 在后文中, $I_{a,b}$ 表示 $\mathcal{B}(H_{a,b})$ 的单位元 (即 I_a 表示 $\mathcal{B}(H_a)$ 的单位元, I_b 表示 $\mathcal{B}(H_b)$ 的单位元, 这里下标 a, b 表示两种情形 a 或 b) 而不再做说明.

注 通常, 离散变量系统指有限维系统, 连续变量系统指无限维系统. 比如 1935 年 Einstein, Podolsky 和 Roson 最早引入的纠缠态就是连续变量的[124]. 目前关于连续变量系统的研究主要以高斯态 (Gaussian state) 为主[47, 77, 389]. 本书 (第 2 章—第 7 章) 则从更广的范围研究一般的无限维系统.

1.2 量子信息概述

通俗地讲, 利用微观粒子的状态表示的信息就是量子信息[69], 它是以量子力学基本原理为基础, 研究如何通过量子体系的各种相干方式进行计算、编码和信息传输的一般规律的学科. 量子信息是相对于经典信息而言的, 是量子力学与经典信息学结合的新型学科. 对于量子信息的认识最早可以追溯到 1935 年 Einstein, Podolsky 和 Rosen 提出的 EPR 佯谬[124]. 1964 年 Bell 从理论上验证了量子态可以违反 Bell 不等式[29], 这一令人吃惊的发现引起了人们的重视. 此后, 有大量的实验证明宏观世界遵守 Bell 不等式, 而微观世界却能违背 Bell 不等式. 从 20 世纪 90 年代开始, 陆续有令人兴奋的新发现: 1991 年 Ekert 发现利用量子态可以实现绝对安全的密码技术, 即量子密码术 (quantum cryptography)[129]; 1992 年 Bennett 和 Wiesner 建立了量子稠密编码 (quantum dense coding) 模型[39]; 1993 年 Bennett 和他的合作者首次发现量子系统可以实现量子隐形传态 (quantum teleportation)[33]. 更让人欣慰的是, 这些方案后来都在实验上证明是可以实现的. 此外, 1994 年 Shor 等提出了一种大数因子分解的量子多项式算法[346, 347, 348], 1997 年 Grover 提出了量子搜索算法[151, 152]. 如果量子计算机能够实现, 世界上现有的保密系统将受到严重威胁. 此后还有很多理论和实验上的新进展. 大量事实证明量子信息技术将会成

为 21 世纪带给人类的完美礼物, 将对于推动经济社会发展、改善人类生活质量以及保卫国家安全等诸多方面提供技术保障.

此外, 现有计算机的各种局限性也是导致量子信息兴起的一个重要原因. 目前计算机的电路器件主要是半导体. 研究表明, 当计算机存储器容量达到 1024M 位时, 其内部电路的线宽只有 0.1 微米, 而这种尺度被认为已经是集成电路密集程度的极限. Moore 定律表明, 当计算机芯片上的器件越来越密集, 电路线宽窄到不得不考虑电路中电子的量子效应时, 目前的半导体技术将走到终点. 取而代之的必将是基于微观粒子量子理论的量子计算机.

量子信息的主要研究内容是量子加密、量子通信和量子计算[278]. 量子密码是密码学与量子力学相结合的产物. 量子加密通信就是利用量子关联效应进行信息加密、传递的一种新型加密通信方式. 目前的加密方法通常都是用一个较大的整数作为公用密匙以保证安全, 因为要破解这样的密码必须求得这个整数的所有质因数. 比如求一个四百多位的整数的质因数目前最快的计算机大概要花数十亿年时间. 但 Shor 大数因子分解法可以在短时间内把大数分解, 这种保密方案完全可以被解密. 而用量子方式进行加密是无法解密的: 量子加密必须通过量子态来实现, 把信息加载于量子态, 任何窃取信息的行为都相当于对量子态进行一次测量, 但依据量子力学的测不准原理, 这种测量对系统发生干扰而立刻改变系统的状态, 也就是说窃取必然会被发现; 量子态的不可克隆原理又保证了窃听者也不可能复制信息, 因此第三方永远不会知道量子态携带的密码信息, 从而保证了加密信息的绝对安全. 量子密码技术并不是用于传输密文, 而是用于建立、传送解码本. 量子密码的优点是可检查解码本是否被盗. 由于量子状态很脆弱, 环境噪声也会破坏解码本信息, 因此如何在有噪声的环境下正常加密是量子密码技术实用化所面临的最大难题. 目前量子加密方案在理论和实验上不断有新突破, 但距离真正适用的量子密码还比较遥远.

量子信息在通信领域最奇妙的应用就是量子隐形传态, 它能够实现信息瞬时离物传输. 1993 年 Bennett 和他的合作者提出的量子隐形传态方案就是利用纠缠态的非定域关联性, 把经典信息方法与量子理念结合起来实现状态的传输. 假设 Alice 和 Bob 在很久以前在一起时共享一个 EPR 态 $|\phi^+\rangle = \dfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, 分开时每人带走 EPR 对中的一个量子比特. 设想两人分开后 Alice 需要向 Bob 发送一个单量子比特状态 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, 而 Alice 也不知道 $|\psi\rangle$ 的具体信息, 而且只能给 Bob 发送经典信息. 这个看起来不可能的事情却可以实现. Alice 让 $|\psi\rangle$ 和 EPR 对中她拥有的那一半相互作用得到

$$|\psi_0\rangle = |\psi\rangle|\phi^+\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)].$$

此时前两个量子比特属于 Alice, 第三个量子比特属于 Bob. Alice 把她拥有的两个比特送到一个受控非门, 即作用 $U_{cn}\otimes I_2$ 于 $|\psi_0\rangle$, 这里 $U_{cn}=I_2\oplus\begin{pmatrix}0&1\\1&0\end{pmatrix}$, I_2 表示 2 阶单位矩阵, 得到

$$|\psi_1\rangle=\frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle+|11\rangle)+\beta|1\rangle(|10\rangle+|01\rangle)].$$

再让第一个量子比特通过一个 Hadamard 门得到

$$|\psi_2\rangle=H\otimes I_2\otimes I_2|\psi_1\rangle=\frac{1}{\sqrt{2}}[\alpha(|0\rangle+|1\rangle)(|00\rangle+|11\rangle)+\beta(|0\rangle-|1\rangle)(|10\rangle+|01\rangle)],$$

这里 $H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$. 注意到 $|\psi_2\rangle$ 可以改写为

$$|\psi_2\rangle=\frac{1}{2}[|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle+\beta|0\rangle)+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(\alpha|1\rangle-\beta|0\rangle)].$$

显然此时如果 Alice 对她拥有的两个量子比特进行测量, 如果测量结果为 $|00\rangle$, 她打电话告诉 Bob 她的测量结果, Bob 就可在异地瞬时得到状态 $|\psi\rangle$. 这就实现了量子隐形传态. 在这个过程中, EPR 态是纠缠态 (1.6 节), 其非定域关联性起到了至关重要的作用. 事实上, 在几乎所有的量子信息处理技术中都离不开纠缠或其他量子关联性, 量子关联因此而成为量子信息处理最关键的资源. 量子隐形传态的实现让人们看到了量子通信的优势, 此后关于量子通信的研究迅速成为自然科学领域的一个重要研究课题, 引起了众多专家学者的关注. 但量子通信也面临很多问题, 一个首要的问题是量子纠缠性在噪声影响下随着传输距离的增加而减弱, 而且纠缠是很不稳定的, 会出现“突然死亡”现象[416], 因此如何在通信过程中保持纠缠态的稳定性是目前量子通信研究中的最大难题.

20 世纪 80 年代初, 计算机科学领域就出现了量子计算机概念[69]. 物理学家 Feynman 生前曾研究过用量子力学理论实现量子计算并构建量子计算机. 但由于量子状态的脆弱性以及测不准性, 当时人们对量子计算并不抱有多大希望, 只认为在原则上可行. 1994 年美国电话电报公司的计算机专家 Shor 证明了量子计算机能够快速进行大数分解并发展了第一套量子算法编码, 此后量子计算机进入实验时代. 1996 年, *Science* 科技新闻报道了量子计算机的理念及其研究现状. 同年, Bennett 在 *Nature* 杂志新闻与评论栏声称量子计算机将进入工程时代. 量子计算机因此而被人们广泛知晓. 通俗地讲, 量子计算就是利用量子态进行信息处理的方法, 其运行装置称为量子计算机. 量子计算机的基本原理就是将微晶体管压缩到原子尺度大小, 然后在极小的面积上放入数十亿颗量子微晶体管, 根据量子力学原理, 利用量子态的叠加性和相干性进行信息运算、保存和处理.

量子计算机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 年代人们就发现能耗会导致计算机芯片发热而影响芯片的集成度, 从而限制了计算机的运行速度. Landauer 最早分析了能耗的原因, 他指出能耗源于计算过程的不可逆操作[248, 255]. Bennett 后来更严格地研究了这个问题并证明所有经典不可逆计算机都可以改造为可逆计算机而不影响其计算能力[31]. 在经典计算机中, 基本信息单位是比特, 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正交态的叠加态上, 而且还可以处于纠缠态上. 这种特殊的量子态不仅提供了量子并行计算的可能, 而且还有许多奇妙的性质. 与经典计算机不同, 量子计算机可以做任意的酉变换, 在得到输出状态后, 进行测量得出计算结果. 因此, 量子计算对经典计算进行了极大的补充, 在数学形式上, 经典计算可以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, 并按一定概率幅叠加起来给出结果, 这就是所谓的量子并行计算. 除了量子并行计算外, 量子计算机还可以用来模拟量子系统, 这项工作也是经典计算机无法完成的.

迄今为止世界上还没有真正意义上的量子计算机, 但世界各地的科学家们正在以巨大的热情追寻这个梦想. 目前已经利用原子和光腔的相互作用、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、广义量子干涉等提出不同方案, 但哪一种方案更有前景还很难说. 量子计算机也存在缺陷, 比如酉操作使得量子计算能力有严格限制. 对于量子计算机最大的一个实际问题是在实际系统中量子相干性很难保持, 而量子计算正是要利用量子相干性. 因此, 实现量子计算机的一个核心问题是克服消相干. 目前发现的最有效的消相干办法是量子编码, 比如量子纠错码、量子避错码和量子防错码. 日益更新的新发现不断地让我们看到了量子计算机成功实现的希望, 随着现代科技的发展, 量子计算机会走向现实研制和运用. 可以比较肯定地预计, 在不远的将来, 量子计算机必将作为超级计算设备取代经典计算机.

不论是量子加密通信还是量子计算, 量子状态的量子关联 (尤其是纠缠) 始终是信息处理的核心资源, 离开量子关联就无法执行超越经典技术的保密、通信和计算任务. 也就是说复合系统量子状态的量子关联性是量子信息技术得以实现的首要保障条件, 因此, 研究量子信息首先要研究量子关联.

1.3　偏迹与约化态

本节讨论为什么对于复合系统来说, 通过求偏迹得到的约化态能够表示子系统的状态.

我们先给出偏迹运算的定义. 设 $\dim H_a \otimes H_b \leqslant +\infty$, $X \in \mathcal{T}(H_a \otimes H_b)$, 则称

$$X \mapsto X_a := (\mathrm{Tr} \otimes \mathbb{1}_b)X \quad \text{和} \quad X \mapsto X_b := (\mathbb{1}_a \otimes \mathrm{Tr})X \tag{1.7}$$

分别为 X 对子系统 B 和 A 求偏迹. 这里 Tr 表示取迹运算, $\mathbb{1}_a$ 和 $\mathbb{1}_b$ 分别表示子系统状态空间 H_a 和 H_b 上的恒等映射. 特别地, 对于量子态 $\rho \in \mathcal{S}(H_a \otimes H_b)$,

$$\rho_b = \mathrm{Tr}_a(\rho) = (\mathrm{Tr} \otimes \mathbb{1}_b)\rho \quad \text{和} \quad \rho_a = \mathrm{Tr}_b(\rho) = (\mathbb{1}_a \otimes \mathrm{Tr})\rho \tag{1.8}$$

称为 ρ 的约化态. 设纯态 $|\psi\rangle = \sum\limits_{m,\mu} d_{m\mu}|m\rangle|\mu\rangle \in H_a \otimes H_b$, $\dim H_a \otimes H_b \leqslant +\infty$, 记 $D = \sum\limits_{m,\mu} d_{m\mu}|m\rangle\langle\mu|$, 则显然 $D \in \mathcal{C}(H_b, H_a)$ 且 $\|D\|_2^2 = \mathrm{Tr}(D^\dagger D) = 1$. $|\psi\rangle$ 的约化态则为

$$\begin{aligned}
\rho_a = \mathrm{Tr}_b(|\psi\rangle\langle\psi|) &= (\mathbb{1}_a \otimes \mathrm{Tr}) \left(\sum_{m,\mu,n,\nu} d_{m\mu}\overline{d_{n\nu}}|m\rangle\langle n| \otimes |\mu\rangle\langle\nu| \right) \\
&= \sum_{m,\mu,n,\nu} d_{m\mu}\overline{d_{n\nu}}\mathrm{Tr}(|\mu\rangle\langle\nu|)|m\rangle\langle n| = \sum_{m,n,\mu} d_{m\mu}\overline{d_{n\mu}}|m\rangle\langle n| \\
&= \sum_{m,n} \left(\sum_{\mu} d_{m\mu}\overline{d_{n\mu}} \right) |m\rangle\langle n| = DD^\dagger,
\end{aligned}$$

类似可得 $\rho_b = D^\dagger D$. 若 ρ 是混合态, 由于 ρ 是紧正算子, 因此有谱分解

$$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|, p_i \geqslant 0, \quad \sum_i p_i = 1.$$

记 $|\psi_i\rangle = \sum\limits_{m,\mu} d_{m\mu}^{(i)}|m\rangle|\mu\rangle$, $D_i = \sum\limits_{m,\mu} d_{m\mu}^{(i)}|m\rangle\langle\mu|$, 则

$$\rho_a = \sum_i p_i D_i D_i^\dagger, \quad \rho_b = \sum_i p_i D_i^\dagger D_i.$$

在量子力学中, 任何测量都必须通过测量仪器来实现, 由于会受到噪声的影响, 此时如果把所考虑系统看作子系统 A, 测量仪器或者其他影响测量的因素视为另一子系统 B, 整体构成一个复合系统, 则系统 A 的力学量平均值应通过求约化密度算子给出. 下面的结论将论证这一事实, 说明约化态恰好表示了子系统的状态.

定理 1.1 设 $\dim H_a \otimes H_b = +\infty$, 映射 $L : \mathcal{S}(H_a \otimes H_b) \to \mathcal{S}(H_a)$ 是偏迹运算 (即 $L(\rho) = \mathrm{Tr}_b(\rho) = \rho_a$ 对所有 $\rho \in \mathcal{S}(H_a \otimes H_b)$) 都成立当且仅当

$$\mathrm{Tr}(PL(\rho)) = \mathrm{Tr}((P \otimes I_b)\rho) \tag{1.9}$$

对所有 $\rho\in\mathcal{S}(H_a\otimes H_b)$ 及 H_a 上所有秩一投影 P 都成立.

注意, 定理中 L 是任意映射, 我们没有假设 L 是线性的. 下面先给出几个引理.

引理 1.2[430]　设 H 是复 Hilbert 空间, $\dim H=+\infty$. 若 $\{\rho,\rho_n\}\subset\mathcal{S}(H)$, 则 ρ_n 按弱算子拓扑收敛于 ρ 当且仅当 ρ_n 按迹范数拓扑收敛于 ρ.

引理 1.3[212]　设 H_i, $i=1,2,\cdots,k$ 是 Hilbert 空间, $\Phi=\sum\limits_{j=1}^{n}A_{1j}\otimes A_{2j}\otimes\cdots\otimes A_{kj}\in\mathcal{B}(H_1\otimes H_2\otimes\cdots\otimes H_k)$, $0\neq A_{ij}\in\mathcal{B}(H_j)$. 若存在某个 r, $1\leqslant r\leqslant k$, 满足 $\{A_{rj}\}_{j=1}^{n}$ 是一线性无关集, 则 Φ 是 Schatten-p 类算子当且仅当 A_{ij} 都是 Schatten-p 类算子.

引理 1.4　设$\rho\in\mathcal{S}(H_a\otimes H_b)$, $\{|i\rangle\}_{i=1}^{\infty}$ 是 H_a 的一组标准正交基, 则 ρ 可以表示为 $\rho=\sum\limits_{i,j}E_{ij}\otimes B_{ij}$, $E_{ij}=|i\rangle\langle j|$, B_{ij} 是 H_b 上的迹类算子, 级数按迹范数收敛.

证明　取 H_b 的一组标准正交基 $\{|k'\rangle\}_{k'=1}^{\infty}$. 若 $\rho\in\mathcal{S}(H_a\otimes H_b)$, 则

$$\rho=\sum_{i,j,k',l'}\rho_{ijk'l'}|i\rangle\langle j|\otimes|k'\rangle\langle l'|=\sum_{i,j}|i\rangle\langle j|\otimes\left(\sum_{k',l'}\rho_{ijk'l'}|k'\rangle\langle l'|\right).$$

记 $B_{ij}=\sum\limits_{k',l'}\rho_{ijk'l'}|k'\rangle\langle l'|$, $i,j=1,2,\cdots$, 有

$$\rho=\sum_{i,j}E_{ij}\otimes B_{ij}. \tag{1.10}$$

我们断言 B_{ij} 是 H_b 上的迹类算子, $i,j\in\mathbb{N}$, 且该级数按迹范数收敛. 令

$$P_n=\sum_{i=1}^{n}|i\rangle\langle i|,\quad \widetilde{P_n}=P_n\otimes I_b.$$

显然 $\widetilde{P_n}\to I=I_a\otimes I_b$ (按强算子拓扑). 定义

$$\rho_n=\frac{1}{\mathrm{Tr}(\widetilde{P_n}\rho\widetilde{P_n})}\widetilde{P_n}\rho\widetilde{P_n},$$

则 $\rho_n\in\mathcal{S}(H_a\otimes H_b)$ 且 ρ_n 按弱算子拓扑收敛于 ρ $(n\to\infty)$, 这是因为

$$\langle x|\rho_n|f\rangle=\frac{1}{\mathrm{Tr}(\widetilde{P_n}\rho\widetilde{P_n})}(\langle f|\widetilde{P_n}\rho\widetilde{P_n}|x\rangle)\to\langle f|\rho|x\rangle(n\to\infty),$$

对任意 $|x\rangle,|f\rangle\in H_a\otimes H_b$ 成立. 因此, 由引理 1.3, ρ_n 按迹范数收敛于 ρ. 对任给 $n\in\mathbb{N}$, 由于

$$\rho_n=\frac{1}{\mathrm{Tr}(\widetilde{P_n}\rho\widetilde{P_n})}\sum_{i,j=1}^{n}E_{ij}\otimes B_{ij}$$