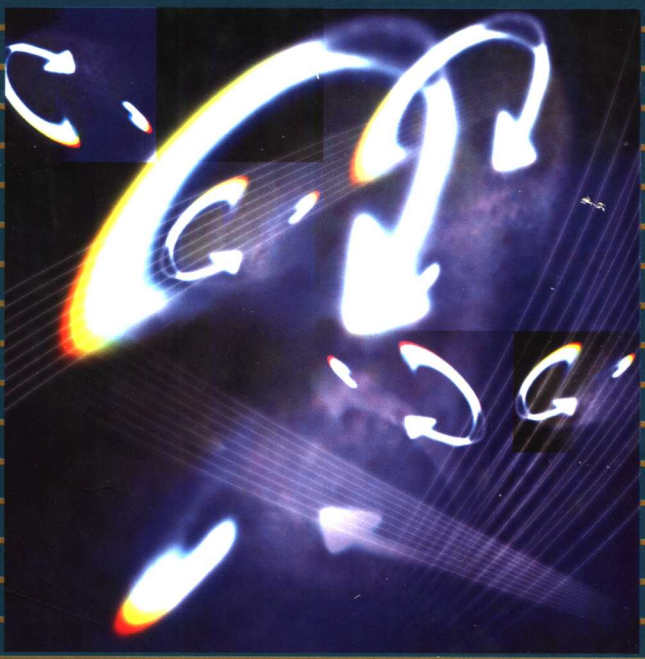
学 术 著 作 丛 书

量子通信和量子计算

李承祖 等编著



量子通信和量子计算

李承祖　黄明球
陈平形　梁林梅　编著

国防科技大学出版社
湖南·长沙

内 容 简 介

本书系统地介绍了量子通信和量子计算的物理原理和方法。内容包括经典信息论概要、量子信息学的量子力学基础、量子通信、量子计算、量子计算机的物理实现和消相干、量子纠错码、量子容错恢复和容错计算。

本书可用作量子信息学及相关专业研究生教材，亦可供相关专业教师及科研人员参考。

图书在版编目(CIP)数据

量子通信和量子计算/李承祖等编著.—长沙：国防科技大学出版社，2000.8

ISBN 7-81024-654-2

Ⅰ.量… Ⅱ.李… Ⅲ.①量子-理论-应用-通信②量子-计算 Ⅳ.①TN91②TB939

中国版本图书馆 CIP 数据核字(2000)第 33365 号

国防科技大学出版社出版发行

电话：(0731)4572640 邮政编码：410073

E-mail：gfkdcbs@public.cs.hn.cn

责任编辑：文 慧 责任校对：黄 煌

新华书店总店北京发行所经销

国防科技大学印刷厂印装

*

850×1168 1/32 印张：11.75 字数：295 千

2000 年 8 月第 1 版第 1 次印刷 印数：1－1000 册

*

定价：30.00 元

前　言

量子通信和量子计算(量子信息学)是最近几年迅速发展起来的新兴学科,由于它潜在的应用价值和重大的科学意义,正引起各方面越来越多的关注。根据著名科学家钱学森的建议,国防科技大学在1997年4月开始了该领域的研究。1998年秋,在应用物理系原子分子物理专业和计算机科学系计算机体系与系统结构专业为研究生开设了"量子通信和量子计算"课程。1999年春,国防科技大学量子信息技术研究中心为相关专业部分青年教师和研究生开设了关于这一内容的系列学术讲座。作者受命担任这些课程和讲座的主讲,迫使作者对这一领域有关专业知识以及大量文献资料进行认真钻研学习,选取讲授材料,组织讲稿。本书就是在这些讲稿基础上,经修改、补充而成的。

本书内容共分七章。第一章经典信息理论概要,介绍了信息、信息度量、互信息、Shannon编码定理等为理解量子信息学所必要的经典信息理论基础。这些内容对于过去很少涉足信息论的非通信专业人员学习量子信息学是必要的。第二章量子信息学的量子力学基础,从微观粒子波粒二象性以及不确定关系式出发,以公理化形式系统地表述了量子力学的基本原理,并介绍了密度算子、量子纠缠态等重要工具和概念。作者相信这一章内容对信息论、计算机专家了解量子信息学是绝对必要的。第三章量子通信,从量子态的基本性质出发,揭示了量子信息的特点,介绍了"稠密编码"、量子"隐形传态"、量子密钥分配、量子通信编码定理,最后还介绍了量子纠缠态度量研究情况。第四章量子计算,介绍了量子并行计算、随机数据库Grover搜索量子算法、分解大数质因子Shor

量子算法。第五章量子计算机的物理实现和消相干，介绍了量子通用逻辑门组，量子计算机线路网络模型，并从量子力学角度分析了量子计算机物理实现的困难。第六章量子纠错码，首先介绍了经典线性纠错码及代数基础、群的有关概念，然后介绍了 CSS 量子纠错码和一般稳定子码理论和方法。第七章量子容错恢复和容错计算，介绍了容错恢复和容错计算的概念和使用一般稳定子码的容错计算。全书内容前呼后应，形成一个有机整体，除去更深入地钻研一些问题需要进一步阅读更多文献资料外，阅读本书需要的概念、数学工具和理论基础，书中基本上可以自供自足。本书一定程度上可以满足不同领域工作的专家了解、学习量子信息学的需要。

由于量子信息学涉及到经典信息论、计算机科学、量子物理学的许多方面，其中还用到概率论、数论、群论等数学知识，是一个典型的多学科交叉。量子力学理论，像“纠缠”这种奇特的量子现象，曾困惑过几代人，并在 Einstein 和 Bohr 这些物理学巨人之间引起长期争论。量子信息学要求不仅理解这些现象，而且要解决许多技术问题，控制、操纵、利用这些现象做实际的量子通信和量子计算，难度很大。钱学森同志 1997 年 7 月就作者的一篇报告写给国防科技大学应用物理系的回信中曾指出：“我也知道，此任务难度不小，全校有关同志……要全力合作，各贡献出自己的才智才行。”作者希望借此书对我国量子信息科学研究工作贡献一点微薄之力。同时借此书出版之际，向钱学森同志对国防科技大学量子信息科学研究工作的支持、关心和指导表示衷心感谢。

白铭复教授、陈健华教授、田成林副教授和作者进行过多次有益的讨论；国防科技大学理学院曾淳院长最早为作者搜集了许多文献资料，其后对该课题的研究以及本书一直给予关心和支持；国防科技大学科研部领导也给了作者大力支持和帮助，作者向他们表示感谢。

量子信息学是一个迅速发展的领域，要概括出它的全貌，对于作者确实是十分困难的任务。加之本书成书时间仓促，作者学识、水平有限，书中错误、不当之处在所难免，诚恳地欢迎读者批评、指正。

作　者

2000年4月

引　言

随着信息技术进步，信息已经和物质、能量一起构成现代社会赖以生存和发展的三大基本要素。如果说物质是社会基础，能量使社会具有活力，那么信息则是促进社会进步的主要因素。随着现代社会变革和进步的加快，信息的作用越来越突出。这就是人们把当今社会称为信息社会的原因。

研究信息本身的理论是**信息论**(Information theory)。信息论研究信息的本质，信息的产生，信息存储和传输，信息编码、译码；传输信道对信息传输有效性、可靠性的影响；在噪声信道中如何保证信息传输质量等问题。虽然有人类活动就有信息获取、传输和利用，但作为一门定量科学，“信息论”则诞生于20世纪40年代。1948年，美国工程师C.E.Shannon发表了“通信的数学理论”的文章，给信息以定量的科学描述，标志着信息论作为一门科学的建立。50多年来，以Shannon理论为核心的经典信息理论经历了一个发展和成熟的过程，这个理论对通信技术和理论的发展起到了重要的推动作用。

几乎和Shannon信息论出现的同时，诞生了第一代电子计算机。计算机是信息处理的工具。随着计算机技术的进步，信息存储、显示、处理和利用发生了根本性的变化。信息在当代社会进步中的重大作用和广泛影响与计算机技术的进步有密不可分的联系。

20世纪科学史上的另一重大发现是**量子论**(quantum theory)。量子论揭示了经典物理学对物质世界的描述仅在宏观条件下才是正确的，微观世界遵循的是量子规律，世界本质上是量子的，经典

规律只是量子规律在宏观条件下的近似。微观粒子具有波粒二象性,它的运动状态、性质、描述方法、运动规律和经典物理根本不同。对结果的预测不再是 Laplace 决定论的,而是概率的、统计性的。量子力学就是我们描述微观粒子运动的一个理论框架和数学结构。量子力学的发现改变了我们对微观世界的描述方法,加深了我们对物质世界本质的理解。

从 20 世纪 20 年代量子力学诞生至今 70 多年来,量子力学理论取得了巨大的成功。这个理论不仅解释了原子、原子核结构、化学键、物体超导电性、固体结构、半导体性质、基本粒子产生和湮灭等许多重要物理问题,而且也促成了现代微电子技术、激光技术、新能源技术、新材料科学的出现和发展。尽管人们对量子力学理论的理解和解释还存在着这样或那样不同的看法,但它作为一个成功的物理理论,没有人怀疑过它的正确性。

在 20 世纪 80 年代以前,信息理论、计算机科学和量子力学作为不同的学科互相平行地发展,几乎无人注意到它们之间的交叉和联系。在过去的信息理论、计算机科学中,除去信息存储,信息传输和信息处理需要借助于物理手段进行外,这些科学本身似乎和物理学没有太多联系。经典信息论是 Shannon 等人把数学概率论应用于信息研究创造出来的,而计算机科学则在很大程度上是由 Turing, Church, Post 和 Gödel 等人依靠思辩和逻辑,凭借灵感和直觉创造出来的。最近 20 多年来,人们越来越清楚地认识到,信息论、计算机科学和物理学存在着深刻的、密切的联系。**信息,归根结底是编码在物理系统态中的东西,从物理角度看,信息源于物理态在时空中的变化,信息传输是编码物理态的传输,信息处理是被称为"计算机"的物理系统态的有控制演化,信息的提取则是对编码物理态的测量。**信息论、计算机科学和物理学的联系不仅表现在信息需要借助于物理手段存储、传输和处理,而且还表现在这些科学概念、原理都要受到基本物理规律的制约。当对编码信息

的态从经典物理理解过渡到量子物理理解时，由于量子态具有根本不同于经典物理态的性质，对经典物理为基础的信息论和计算机科学不可避免地要重新加以审视，于是产生了以量子力学为基础的**量子信息理论**(quantum information theory)或**量子信息学**。所谓量子信息学，实质上就是研究用量子态编码的信息科学。

现在量子信息学已成为内容丰富的新学科，已经建立了 Shannon 编码定理的量子推广。量子纠缠现象在通讯中的应用，创造出"绝对安全的密钥"、"稠密编码"、"隐形传态"等经典信息理论不可思议的奇迹；已经构造出"分解大数质因子"、"未加整理的数据库搜索"等问题的量子算法。利用理想中的量子计算机，可以实现大规模的并行计算，产生经典计算机不可比拟的信息处理功能等。在实验研究方面，已经成功地实现了局域网上的量子密钥分配，以及量子隐形传态。在量子逻辑门的物理实现方面已经找到了几个物理系统，并成功地实现了基本逻辑门运算。量子信息科学的研究不仅由于它的巨大科学意义和学术价值引起物理学家、信息科学专家的兴趣，而且由于它显示出的潜在应用价值，也引起各国政府、军事部门、金融银行业和企业厂商的重视。随着量子信息学理论和实验上不断获得新的突破，人们预言这一研究有可能在 21 世纪引起一场关于信息和通信技术的革命。

本书的目的就是系统地介绍量子信息理论的基本原理和量子通信和量子计算研究的主要成果以及实现技术研究进展情况，为有志于该项研究的读者打下必要的知识基础。

目　录

第二章　量子信息学的量子力学基础

第三章 量子通信

第四章 量子计算

第五章 量子计算机的物理实现和消相干

第六章 量子纠错码

第七章 量子容错、纠错和容错计算