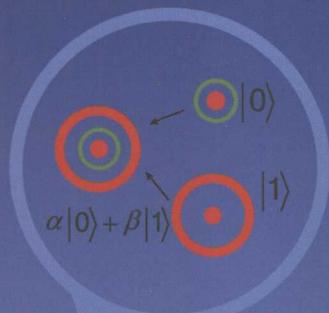
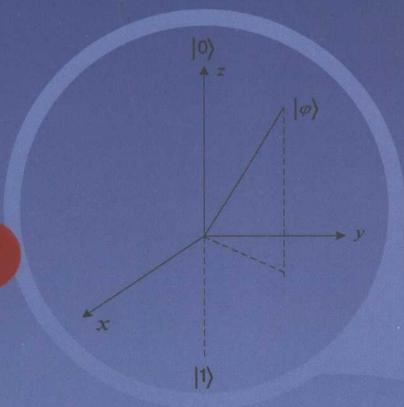




量子信息处理技术及 算法设计

周日贵 著



0101010101
0101010100
1110010101
010000101



科学出版社

014003505

0413.1
90

华东交通大学教材(专著)基金资助项目

量子信息处理技术及 算法设计

周日贵 著



0413.1
90

科学出版社

北京



北航

C1691273

014003202

内 容 简 介

本书通过对量子模式搜索、量子图像处理、量子神经计算及量子遗传算法 4 方面进行理论介绍及分析,并结合相应算法 MATLAB 仿真对量子信息处理技术进行了综合阐述。本书可读性好,具有交叉性、前沿性等特点。为了便于学习,书中给出了很多实例。

本书可供计算机科学、信息科学、智能信息处理和人工智能等相关专业的科研人员、高校教师、博士生和硕士生学习参考,同时对相关研究人员具有指导价值。

图书在版编目(CIP)数据

量子信息处理技术及算法设计/周日贵著. —北京:科学出版社, 2013
ISBN 978-7-03-038583-3

I. ①量… II. ①周… III. ①量子力学-信息技术②量子力学-算法设计
IV. ①0413.1

中国版本图书馆 CIP 数据核字(2013)第 215259 号

责任编辑:余 丁 王晓丽 / 责任校对:宋玲玲

责任印制:张 倩 / 封面设计:蓝 正

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>

新科印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2013 年 6 月第 一 版 开本: B5(720×1000)

2013 年 6 月第一次印刷 印张: 16 1/4

字数: 312 000

定价: 60.00 元

(如有印装质量问题,我社负责调换)

前 言

自 1946 年第一台电子计算机问世以来,其运算速度和存储器容量以难以想象的速度飞快提高。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 $0.1\mu\text{m}$,而这种尺度被认为已经达到了集成电路的极限。当电路的线宽小于 $0.1\mu\text{m}$ 时,将面临一个瓶颈问题,电路内运动的电子会出现量子效应,且量子效应会影响甚至完全破坏电路中芯片功能,原来的电路理论将不再适应,取而代之的是微观粒子的量子理论。利用量子理论设计的电子元件是量子元件,利用量子元件和量子算法设计的计算机称为量子计算机。量子力学对计算机技术发展具有决定性作用。

从计算之日开始,人们便不断寻求能方便运行和加速计算的工具。所以,计算和计算工具息息相关。从简单的计算工具如木棍、石头到算盘再到复杂的计算工具如电子管计算机、晶体管计算机到现在的电子计算机,人们不断地追求科技的进步。进入 21 世纪后,信息科学面临着新的挑战。计算机是否存在极限的运算速度,能否实现不可破译、不可窃听的保密通信等问题成为科学家们关注的重要课题。创建新一代高性能的、安全的计算工具和通信技术是当前研究的热点。近年的研究进展表明,应用量子信息的产生、载荷、传播和处理可以构造高性能的量子计算机。其具备的量子特性在信息领域中有着独特的功能,在提高运算速度、确保信息安全、增大信息容量和提高检测精度等方面可能突破现有的经典信息系统的极限。

量子,自被发现之日起便以不可思议的特性满足了众多研究者和实践者的要求。美国制定的研发量子芯片的“微型曼哈顿”计划,预示着未来、现有的密码体制将受到前所未有的挑战。现如今各国对量子技术都分外重视,中国科学院郭光灿院士认为“人类已经从对经典世界的认识,到对量子世界奥秘的认识,并到了开发量子世界的时代”。

量子计算的优越性主要体现在量子并行处理上,无论是量子并行计算还是量子模拟,都本质性地利用了量子相干性。失去了量子相干性,量子计算的优越性将消失殆尽。但不幸的是,在实际系统中,量子相干性却很难保持,其指数衰减不可避免。量子相干性的丢失就会导致运算结果出错,这就是量子错误。而其他一些技术原因,如量子门操作中的误差等,也会导致量子错误。因此,现在研究人员面对的关键问题就变成在操作和量子存储都有可能出错的前提下,如何进行可靠的量子运算。

随着一些优秀的量子算法被人们陆续发现,量子计算机逐渐成为研究的热点。1994年美国计算机专家 Shor 提出大数的素因子分解算法特别引人注目。大数的素因子分解算法之所以重要是因为大数的素因子分解是经典计算机的难解问题,而这正是目前广泛使用的 RSA 公开密钥加密系统得以安全的先决条件。也就是说大数的因子分解是经典计算理论中的 NP 难题,然而 Shor 的量子算法把它转化为 P 类问题。美国科学家 Grover 在 1997 年提出“量子搜寻算法”,可以破译 DES 密码体系。这使得现行的电子密码系统无密可言。这给量子计算机研究注入了新的活力,世界各国政府纷纷组织科研力量进行量子计算机的研究,引发了风靡全球的量子计算机研究的热潮。

量子信息处理技术是利用量子体系的独特性质对计算、编码、信息处理和传输过程给予新的诠释,开发新的、更为高效的信息处理功能的一门学科,它是现代科学技术发展的必然结果。量子信息科学的研究为物理学、信息科学、材料科学乃至整个科学注入了新的生命力,同时对推动相关高新技术的发展以及人类社会的进步具有深远的意义。但不得不承认的是目前量子信息处理技术在国内外尚处于研究者个体探索的阶段,它在物理实现上还存在许多困难,而且缺乏足够的研究技术支持来解决现存的困境。但是具有诱人前景的量子信息有很多优点,可能对未来技术产生革命性的变化,甚至对国家安全、国防建设等都具有现实意义。因此,研究量子信息处理技术不仅具有重大的理论研究价值,还具有广阔的实际应用前景。本书对量子信息处理技术和算法设计作了一些研究,具体内容是:

第 1 章绪论主要介绍了量子力学的产生和发展以及存在的关键问题;介绍了量子计算机的发展背景、物理实现、研究现状和未来展望以及与经典计算机相比存在的优越性;介绍了量子计算的过程、应用及存在的几种量子算法。

第 2 章量子信息技术基本理论介绍了量子信息学的量子力学和量子计算基础,从希尔伯特空间到狄拉克符号以及线性矩阵,以公式化形式系统地表述了量子力学的基本原理,并介绍了量子比特、量子比特门等一些量子计算的基本知识。

第 3 章量子模式搜索算法根据单模式量子识别和多模式量子识别介绍了相应的模式搜索算法。在单模式搜索部分主要介绍了旋转迭代搜索算法、基于分布式查询搜索算法等单模式搜索算法;在多模式搜索部分主要介绍了高概率多模式搜索算法、部分多模式搜索算法和非线性的多模式算法等。

第 4 章量子图像处理根据量子态的各种属性,结合经典图像处理的像素性质,通过多种不同的表示方式对图像进行量子态存储即图像变换,主要分为灰度图像量子态表示、FRQI 量子态存储表示、基于电磁波映射和量子纠缠的量子图像表示。最后介绍了量子图像特征提取的应用。

第 5 章量子神经计算是量子计算和神经计算结合产生的,是新兴和前沿的学科之一,目前在全世界还处于研究者个体探索的阶段,发展还很不成熟。科学家

研究量子神经计算一方面设计新型的量子神经计算模型,另一方面研究模型的具体工作算法和实际应用,本章介绍了6种量子神经计算模型。

第6章量子遗传算法主要分析了遗传算法的主要特性、不足之处以及现有改进算法,进而介绍了几种新型量子遗传模型:BP神经网络量子改进遗传训练模型、子群并行优化的量子遗传模型以及基于模拟退火算法的量子混合遗传模型。

第7章MATLAB仿真主要介绍量子信息的MATLAB仿真,分为3个部分:第1部分是量子态及量子门的MATLAB表征;第2部分是基于MATLAB表征的基础上定义相关函数、M文件的实现以及其应用举例;第3部分是量子算法的MATLAB仿真,介绍Grover量子算法以及量子遗传算法的仿真。

量子信息学涉及经典信息论、计算机科学和量子物理学等诸多方面,其中还用到了数学知识,涉及面甚广,再加上该领域发展非常迅速,这使得本书不能将所有的论题都深度展开,请大家谅解。

参考文献列出书中引用的全部文献,同时向由于疏忽而未被引用的作者表示歉意。

国家科学技术学术著作出版基金、国家自然科学基金(61065002)委员会、华东交通大学教材(专著)基金为本书的出版和相关研究工作提供了资金支持。

感谢南京航空航天大学丁秋林教授一直对本书的研究工作给予支持、指导和帮助。感谢黎海生博士、李明翠讲师、刘遵雄博士和张恒博士等诸多本领域学者以及研究生吴茜、张满群、李彦成、沈陈懿、肖天儒、曹建、施洋、王惠安、夏小舟和王凤美等为本书提供相关素材。感谢自己的博士后合作导师中国科学技术大学和清华大学的潘建伟院士、四川师范大学庞朝阳教授对本书的大力支持。特别感谢华东交通大学信息工程学院支持帮助我的同仁,他们为本书的研究工作创造了良好的环境,并给予充分的时间保障,让本书的研究得以顺利进行。

特别强调的是,量子信息处理技术和算法研究尚未成熟,且是一个发展迅速的领域,要概括出它的全貌,对于作者来说确实是十分困难的任务,加之作者水平有限,不妥之处在所难免,殷切期待读者给予批评指正。

周日贵

2012年7月

目 录

前言

| | |
|----------------------------|----|
| 第 1 章 绪论 | 1 |
| 1.1 引言 | 1 |
| 1.2 量子力学 | 3 |
| 1.2.1 量子力学的产生和发展 | 3 |
| 1.2.2 量子力学的定义 | 5 |
| 1.2.3 量子力学的关键问题 | 7 |
| 1.3 量子力学的新应用——量子计算机 | 9 |
| 1.3.1 经典计算机过渡到量子计算机 | 9 |
| 1.3.2 量子计算机的基本原理 | 12 |
| 1.3.3 量子计算机的物理实现 | 14 |
| 1.3.4 量子计算机的优越性 | 16 |
| 1.3.5 量子计算机研究现状及未来展望 | 17 |
| 1.4 量子计算 | 20 |
| 1.4.1 量子计算过程 | 21 |
| 1.4.2 量子计算应用 | 21 |
| 1.4.3 量子算法 | 23 |
| 参考文献 | 25 |
| 第 2 章 量子信息技术基本理论 | 28 |
| 2.1 量子力学的数学基础 | 29 |
| 2.1.1 向量空间与希尔伯特空间 | 29 |
| 2.1.2 狄拉克符号 | 29 |
| 2.1.3 基与线性无关 | 29 |
| 2.1.4 线性算子与矩阵 | 30 |
| 2.1.5 内积、外积、张量积 | 30 |
| 2.2 量子计算基础 | 33 |
| 2.2.1 单量子比特 | 33 |
| 2.2.2 多量子比特 | 34 |
| 2.2.3 量子比特门 | 34 |
| 2.2.4 量子力学假设 | 38 |

| | | |
|------------|----------------------|----|
| 2.2.5 | 量子并行性 | 39 |
| 2.2.6 | 量子计算的优点 | 40 |
| 2.3 | 基本量子理论 | 40 |
| 2.3.1 | 量子态线性叠加原理 | 40 |
| 2.3.2 | 相干与坍缩 | 41 |
| 2.3.3 | 算符 | 41 |
| 2.3.4 | 干涉 | 42 |
| 2.3.5 | 纠缠 | 42 |
| 2.3.6 | 量子测量 | 44 |
| | 参考文献 | 44 |
| 第3章 | 量子模式搜索算法 | 46 |
| 3.1 | 随机数据库搜索的量子算法 | 46 |
| 3.1.1 | 基于黑箱的搜索 | 46 |
| 3.1.2 | Grover 搜索算法 | 47 |
| 3.1.3 | Grover 搜索算法的改进和推广 | 50 |
| 3.2 | 单模式量子搜索算法 | 52 |
| 3.2.1 | 旋转迭代单模式量子搜索算法 | 52 |
| 3.2.2 | 基于改进 Grover 的单模式搜索算法 | 55 |
| 3.2.3 | 分布式查询单模式搜索算法 | 56 |
| 3.3 | 多模式量子搜索算法 | 57 |
| 3.3.1 | 高概率多模式搜索算法 | 57 |
| 3.3.2 | 带冗余项的多模式搜索算法 | 61 |
| 3.3.3 | 部分多模式搜索算法 | 65 |
| 3.3.4 | 多模式层级部分搜索算法 | 68 |
| 3.3.5 | 多模式单次量子部分搜索 | 74 |
| 3.3.6 | 非线性的多模式量子搜索 | 75 |
| | 参考文献 | 81 |
| 第4章 | 量子图像处理 | 84 |
| 4.1 | 经典图像处理 | 84 |
| 4.1.1 | 图像 | 84 |
| 4.1.2 | 图像几何变换 | 86 |
| 4.1.3 | 图像增强与恢复 | 88 |
| 4.1.4 | 图像压缩 | 89 |
| 4.2 | 量子灰度图像存储及其变换 | 92 |
| 4.2.1 | 表达式描述 | 92 |

| | | |
|------------|----------------------|------------|
| 4.2.2 | 表达式证明 | 93 |
| 4.2.3 | 像素映射与量子灰度图像指针式存储 | 94 |
| 4.2.4 | 量子灰度图像存储 | 96 |
| 4.2.5 | 量子灰度图像变换 | 97 |
| 4.2.6 | 小结 | 101 |
| 4.3 | FRQI 量子图像表示及其变换 | 102 |
| 4.3.1 | 表达式描述 | 102 |
| 4.3.2 | 表达式证明及实现 | 103 |
| 4.3.3 | 基本颜色变换 | 105 |
| 4.3.4 | 基本几何变换 | 107 |
| 4.3.5 | FRQI 演化——MCRQI | 109 |
| 4.3.6 | 小结 | 112 |
| 4.4 | 基于电磁波映射的量子图像表示 | 112 |
| 4.4.1 | 图像颜色的引入 | 112 |
| 4.4.2 | Qubit Lattice 量子图像存储 | 113 |
| 4.4.3 | 量子图像恢复 | 114 |
| 4.4.4 | 小结 | 117 |
| 4.5 | 基于量子纠缠的量子图像表示 | 117 |
| 4.5.1 | 量子纠缠 | 118 |
| 4.5.2 | 量子图像存储 | 119 |
| 4.5.3 | 图像恢复 | 121 |
| 4.5.4 | 小结 | 122 |
| 4.6 | 基于量子傅里叶变换的模式特征提取算法 | 122 |
| 4.6.1 | 量子傅里叶变换算法 | 123 |
| 4.6.2 | 特征提取算法 | 123 |
| | 参考文献 | 125 |
| 第5章 | 量子神经计算 | 127 |
| 5.1 | 量子 M-P 和感知器计算模型 | 127 |
| 5.1.1 | 量子 M-P 神经计算模型 | 127 |
| 5.1.2 | 单层量子感知器模型 | 131 |
| 5.1.3 | 两种模型的比较 | 136 |
| 5.1.4 | 小结 | 137 |
| 5.2 | 带权值的量子神经计算模型 | 137 |
| 5.2.1 | 量子 Grover 算法 | 138 |
| 5.2.2 | 带权值的量子神经网络 | 139 |

| | | |
|--------------|--------------------|------------|
| 5.2.3 | QNC 应用 | 141 |
| 5.2.4 | 小结 | 142 |
| 5.3 | 无权值的量子神经计算模型 | 142 |
| 5.3.1 | 量子竞争神经计算模型 | 142 |
| 5.3.2 | 随时间演化的量子门计算模型 | 148 |
| 5.3.3 | 两种模型比较 | 152 |
| 5.3.4 | 小结 | 153 |
| 5.4 | 量子 Hopfield 神经计算模型 | 153 |
| 5.4.1 | QHNC 模型和工作原理 | 155 |
| 5.4.2 | QHNC 应用实例 | 157 |
| 5.4.3 | QHNC 仿真与图像识别 | 159 |
| 5.4.4 | 小结 | 160 |
| 5.5 | 基于神经元的量子计算模型 | 161 |
| 5.5.1 | 量子神经元计算模型 | 161 |
| 5.5.2 | 量子神经元模型的性质 | 162 |
| 5.5.3 | 最优量子神经元模型的确定 | 162 |
| 5.5.4 | 实例分析 | 163 |
| 5.5.5 | 最优量子神经元结构确定 | 166 |
| 5.5.6 | 性能分析 | 167 |
| 5.5.7 | 小结 | 168 |
| 5.6 | 基于二叉树的存储计算模型 | 168 |
| 5.6.1 | 存储计算的工作原理 | 168 |
| 5.6.2 | 实例分析 | 170 |
| | 参考文献 | 176 |
| 第 6 章 | 量子遗传算法 | 178 |
| 6.1 | 量子遗传算法概述 | 178 |
| 6.1.1 | 量子遗传算法的提出 | 178 |
| 6.1.2 | 量子遗传算法的国内外现状 | 179 |
| 6.2 | 量子遗传算法基本理论 | 179 |
| 6.2.1 | 量子遗传算法原理简介 | 180 |
| 6.2.2 | 量子遗传算法的主要特点 | 183 |
| 6.2.3 | 量子遗传算法的不足 | 184 |
| 6.3 | BP 神经网络的量子遗传训练模型 | 184 |
| 6.3.1 | BP 神经网络 | 185 |
| 6.3.2 | 量子遗传算法的改进 | 186 |

| | | |
|--------------|-------------------------|------------|
| 6.3.3 | BP 神经网络的量子进化 | 186 |
| 6.3.4 | 农作物虫情的神经网络预测仿真 | 189 |
| 6.4 | 子群并行优化的量子遗传模型 | 193 |
| 6.4.1 | 子群并行优化量子遗传算法 | 193 |
| 6.4.2 | 算法基本流程 | 195 |
| 6.4.3 | 仿真 | 196 |
| 6.5 | 基于模拟退火算法的量子混合遗传模型 | 199 |
| 6.5.1 | 模拟退火算法简介 | 200 |
| 6.5.2 | 实数编码的量子遗传算法 | 200 |
| 6.5.3 | 新型混合量子遗传算法 | 202 |
| 6.5.4 | 仿真 | 204 |
| | 参考文献 | 207 |
| 第 7 章 | MATLAB 仿真 | 209 |
| 7.1 | 矩阵定义及运算 | 209 |
| 7.1.1 | 量子位 | 209 |
| 7.1.2 | 多量子位 | 210 |
| 7.1.3 | 单比特量子门 | 211 |
| 7.1.4 | 多比特量子门 | 212 |
| 7.1.5 | 量子门阵列 | 212 |
| 7.1.6 | 量子门通用性 | 213 |
| 7.2 | 函数定义及 M 文件的实现 | 215 |
| 7.2.1 | 量子态的表征 | 215 |
| 7.2.2 | 矩阵自乘 n 次张量积 | 218 |
| 7.2.3 | 量子比特的 Bloch 球面表示 | 219 |
| 7.2.4 | 酉矩阵的验证 | 221 |
| 7.2.5 | 量子叠加态的验证 | 221 |
| 7.2.6 | Toffoli 门 | 223 |
| 7.2.7 | Fredkin 门 | 224 |
| 7.2.8 | 交换门 | 225 |
| 7.3 | 量子算法的 MATLAB 仿真实现 | 226 |
| 7.3.1 | Grover 量子算法 | 226 |
| 7.3.2 | 量子遗传算法 | 234 |
| | 参考文献 | 239 |

| | |
|-------------------------|------------------|
| 附录 1 希腊字母及其读法 | 241 |
| 附录 2 书中使用到的量子计算常用名词汉英对照 | 242 |
| 附录 3 书中字母缩写与全称对照 | 247 |
| ACI | 量子信息科学国际研究中心 |
| ADP | 量子计算模型 |
| AEI | 量子 |
| AGI | 量子计算与量子通信及其在量子计算 |
| AGS | 量子计算与量子通信 |
| AGU | 量子计算与量子通信 |
| AGV | 量子计算与量子通信 |
| AGW | 量子 |
| AGX | 量子 |
| AGY | 量子 |
| AGZ | 量子 |
| AG1 | 量子 |
| AG2 | 量子 |
| AG3 | 量子 |
| AG4 | 量子 |
| AG5 | 量子 |
| AG6 | 量子 |
| AG7 | 量子 |
| AG8 | 量子 |
| AG9 | 量子 |
| AG10 | 量子 |
| AG11 | 量子 |
| AG12 | 量子 |
| AG13 | 量子 |
| AG14 | 量子 |
| AG15 | 量子 |
| AG16 | 量子 |
| AG17 | 量子 |
| AG18 | 量子 |
| AG19 | 量子 |
| AG20 | 量子 |
| AG21 | 量子 |
| AG22 | 量子 |
| AG23 | 量子 |
| AG24 | 量子 |
| AG25 | 量子 |
| AG26 | 量子 |
| AG27 | 量子 |
| AG28 | 量子 |
| AG29 | 量子 |
| AG30 | 量子 |
| AG31 | 量子 |
| AG32 | 量子 |
| AG33 | 量子 |
| AG34 | 量子 |
| AG35 | 量子 |
| AG36 | 量子 |
| AG37 | 量子 |
| AG38 | 量子 |
| AG39 | 量子 |
| AG40 | 量子 |
| AG41 | 量子 |
| AG42 | 量子 |
| AG43 | 量子 |
| AG44 | 量子 |
| AG45 | 量子 |
| AG46 | 量子 |
| AG47 | 量子 |
| AG48 | 量子 |
| AG49 | 量子 |
| AG50 | 量子 |
| AG51 | 量子 |
| AG52 | 量子 |
| AG53 | 量子 |
| AG54 | 量子 |
| AG55 | 量子 |
| AG56 | 量子 |
| AG57 | 量子 |
| AG58 | 量子 |
| AG59 | 量子 |
| AG60 | 量子 |
| AG61 | 量子 |
| AG62 | 量子 |
| AG63 | 量子 |
| AG64 | 量子 |
| AG65 | 量子 |
| AG66 | 量子 |
| AG67 | 量子 |
| AG68 | 量子 |
| AG69 | 量子 |
| AG70 | 量子 |
| AG71 | 量子 |
| AG72 | 量子 |
| AG73 | 量子 |
| AG74 | 量子 |
| AG75 | 量子 |
| AG76 | 量子 |
| AG77 | 量子 |
| AG78 | 量子 |
| AG79 | 量子 |
| AG80 | 量子 |
| AG81 | 量子 |
| AG82 | 量子 |
| AG83 | 量子 |
| AG84 | 量子 |
| AG85 | 量子 |
| AG86 | 量子 |
| AG87 | 量子 |
| AG88 | 量子 |
| AG89 | 量子 |
| AG90 | 量子 |
| AG91 | 量子 |
| AG92 | 量子 |
| AG93 | 量子 |
| AG94 | 量子 |
| AG95 | 量子 |
| AG96 | 量子 |
| AG97 | 量子 |
| AG98 | 量子 |
| AG99 | 量子 |
| AG100 | 量子 |

第 1 章 绪 论

量子信息学是量子力学和信息科学相结合而产生的新的研究领域。量子信息学在许多方面有着经典信息学无法比拟的优势,比如在提高运算速度、确保信息安全、增大信息容量和提高检测精度等方面量子信息学有可能突破现有的经典信息系统的极限。近年来,量子信息学的理论和实验方面取得了惊人的进展。

1.1 引 言

在日常生活中,人们已经习惯了这样的概念:一个物体的性质,如它的大小、重量、颜色、温度、表面积以及运动,全都可以从一个物体到另一个物体以连续的方式变化。在各种形状、大小与颜色的物体之间并无显著的等级。然而,在原子范围内,情况是极不相同的。原子、粒子的性质,如它们的运动不具有确定的轨道或速度,它们的能量和自旋并不总是显示出类似的连续变化,而是常常相差一些离散的量。经典力学的一个假设是:物质的性质是可以连续变化的。当物理学家们发现这个观念在原子范围内失效时,不得不设计一种全新的力学体系——量子力学^[1]。

众所周知,进入 20 世纪后计算机技术大行其道,人类进入信息时代。目前,计算机芯片集成度每 18 个月翻一番,而事实上,当集成电路的线宽继续缩小,摩尔定律将会失效,科学家们看到传统的计算机结构必将有终结的一天,而且尽管计算机的运行速度与日俱增,但是有一些难题是计算机根本无法解决的,如大数的因式分解,理论上只要一个数足够大,就连最快的经典计算机也需连续运行几亿年。

20 世纪 70 年代,美国 IBM 公司的 Bennett 等开始研究信息处理电路未来的去向问题,他们指出,当计算机元件的尺寸变得非常小时,不得不面对一个严峻的事实:量子效应开始影响电子的正常运动,那时就不得不用量子力学来对它们进行描述^[2]。20 世纪 80 年代初期,一些物理学家证明一台计算机原则上可以以纯粹的量子力学的方式运行,美国物理学家 Feynman 在 1982 年提出量子计算的概念。在更早的时候,Benioff 在《The computer as a physical system》一文中证明了一个重要的定理^[3],从该定理得出的结论是,通过量子态的么正演化可以实现经典图灵机的计算功能。因此量子计算机从理论上是可行的,而且它的性能至少不低于经典计算机。由于量子态的么正演化只存在于理想的孤立系统中,因此在

实际中,量子系统不可避免地和周围环境发生相互作用,表现为量子计算中的噪声干扰,导致量子计算很容易出错。之后很长一段时间,这一研究领域渐趋冷清,因为科学家们不能找到实际的系统可供进行量子计算机的实验,而且尚不清楚量子计算机解决数学问题是否会比常规计算机快。所以量子计算一开始只停留在理论上可行的阶段。

进入 20 世纪 90 年代,实验技术和理论模型的进步为量子计算机的实现提供了可能。随后一些优秀的量子算法被陆续发现,量子计算机逐渐成为研究的热点。值得一提的是美国贝尔实验室的 Shor 于 1994 年提出了大数的素因子分解算法并证明运用量子计算机竟然能有效地进行大数的因式分解。这意味着以大数因式分解算法为依据的电子银行、网络等领域的 RSA 公开密钥密码体系在量子计算机面前不堪一击。随后 Grover 提出量子搜寻算法,可以破译 DES(data encryption standard)密码体系^[2,4]。于是各国政府纷纷投入大量的资金和科研力量进行量子计算机的研究,引发了量子计算机研究的热潮^[5]。如今这一领域已经形成一门新型学科——量子信息学。

首先,什么是量子信息。量子信息属于交叉学科,它是近年来量子力学与信息科学相结合的新型产物。通常量子信息一词有两种不同的解释,广义上讲,它指的是与利用量子力学进行信息处理有关的所有操作方式的概括,包括量子计算、量子图像处理 and 量子遗传算法等;狭义上讲,它指的是对量子信息处理基本任务的研究,与经典信息论相对应。本书为了给大家一个系统的完整的关于量子信息的思想发展脉络,在这里采用的是广义的量子信息论解释,包含了上面提到的量子计算、量子图像处理和量子遗传算法等^[6]。

其次,为什么研究量子信息。经典计算机受到量子效应的干扰及能耗问题的限制,其发展受到很大的阻碍。研究量子信息的最初目的和意义在于突破现有经典信息系统的极限,辅助经典信息系统完成复杂的任务,旨在提高信息速度、确保信息安全、增大信息容量和提高检测精度^[6]。郭光灿教授最早在我国提倡量子信息的研究。我国科技部随后将量子信息的研究确立为“973”计划项目作重点研究。

量子信息的研究如当年的核理论研究一样。一方面,量子信息可以给人类带来诸多方面的进展,如革命性地提高计算速度,改变存储信息的单元,实现绝对保密通信等;另一方面,量子信息的研究也具有很大的破坏性。因为它的研究可以破译密码,以此来窃取他国的军事机密,扰乱他国的金融系统,彻底击毁一个国家。基于以上原因的考虑,各国在很大程度上,都不敢疏忽此项研究。我国将量子信息的研究确立为“973”计划项目作重点研究也是为了在将来的国际竞争中可以占主动地位。所以,量子信息的研究在现在看来已经不仅是科学自主发展的结果,在其发展过程中已经不可避免地加入了国家的意志和政治的目的。各国在量子信息方面的投资可以说是不惜血本。目前,美国、奥地利、英国、日本及我国处

于量子信息研究的领先地位。

1.2 量子力学

量子力学是研究微观粒子的运动规律的物理学分支学科,它主要研究原子、分子、凝聚态物质以及原子核和基本粒子的结构、性质的基础理论。它与相对论一起构成了现代物理学的理论基础。量子力学不仅是近代物理学的基础理论之一,还在化学等有关学科和许多近代技术中得到了广泛的应用。

1.2.1 量子力学的产生和发展

量子力学是在旧量子论的基础上发展起来的。旧量子论对经典物理理论加以某种人为的修正或附加条件以便解释微观领域中的一些现象。由于旧量子论解释不能令人满意,在寻找微观领域的规律时,研究者从不同的道路建立了量子力学。

在19世纪中叶,物理学家开始研究热辐射问题,由于各种物体辐射能量按波长的分布不仅与物体的温度有关,还与物体表面材料的性质有关,为了简化问题的处理,德国物理学家基尔霍夫提出用绝对黑体作为研究热辐射的理想化对象^[7]。1893年,德国物理学家维恩根据实验数据,得出了以他名字命名的维恩位移定律^[8]。这个定律表明,随着黑体温度的升高,对应着它所发射的光线的最大亮度的波长将变短,即向光谱的紫色区移动。虽然维恩位移公式所表述的规律在短波部分与实验曲线符合得比较好,但在长波部分却低于实验值^[8]。

1900年,英国物理学家瑞利从经典理论推导出一个与维恩公式不同的黑体辐射公式,这个公式的主体部分在长波段与实验吻合较好,但在短波段却是发散的。瑞利当时为了克服这一缺陷,人为地设置了一个负指数项以消除这个效应。1900年10月,普朗克获悉了瑞利的结果,他采用数学上的内插法,从维恩公式和瑞利公式得出了一个新的能量分布公式。这个公式与实验结果符合得非常好。但令人不解的是,这个公式却不能从经典理论中推导出来,即经典的连续能量概念和他的公式是格格不入的,以致被称为“纯粹是一些不相关的量的偶然结合”的经验公式^[9]。普朗克为了寻求隐藏在这个公式后面的物理意义,进行了艰苦的理论研究,提出辐射量子假说,假定电磁场和物质交换能量是以间断的形式(量子)实现的,量子的大小同辐射频率成正比,比例常数称为普朗克常数,从而得出黑体辐射能量分布公式,成功地解释了黑体辐射现象,并提出了量子概念^[8]。

1905年,爱因斯坦在《物理学年鉴》上发表了一篇题为“关于光的产生和转化的一个启发性观点”的论文,其中涉及光电效应问题^[9]。他在这篇论文中成功地运用普朗克的量子概念解决了包括光电效应在内的一系列光的产生与转化问题,

而且首次提出了光既有波动性,又有粒子性的观点。爱因斯坦认为,光的能量并不是连续分布的,而是由一些能量子组成的。当一个光量子与电子相碰撞时,会把它的全部能量转化为电子的动能,而只是当电子获得的动能大于它所在金属原子束缚它的能量时,它才能以一定动能离开金属表面,形成光电子^[9]。其后,他又提出固体的振动能量也是量子化的,从而解释了低温下固体比热问题。

爱因斯坦提出光电子理论以后,量子理论引起了越来越多物理学家的重视,并得到了广泛的传播。不仅许多欧洲一流的物理学家和化学家接受量子的概念,还吸引了大批年轻的科学工作者投身于解开量子之谜和把量子理论应用于更多领域的研究。1913年,丹麦物理学家玻尔为解决卢瑟福原子行星模型的不稳定(按经典理论,原子中电子绕原子核作圆周运动要辐射能量,导致轨道半径缩小直到跌落进原子核,与正电荷中和),提出定态假设:原子中的电子并不像行星一样可在任意经典力学的轨道上运转,稳定轨道的作用量 $\oint p dq$ 必须为 h 的整数倍(角动量量子化),即 $\oint p dq = nh$, n 称为量子数^[8]。玻尔又提出原子发光过程不是经典辐射,是电子在不同的稳定轨道态之间的不连续的跃迁过程,光的频率由轨道态之间的能量差 $\Delta E = h\nu$ 确定,即频率法则^[8]。这样,玻尔原子理论以它简单明晰的图像解释了氢原子分立光谱线,并以电子轨道态直观地解释了化学元素周期表,导致了72号元素铅的发现。从普朗克的量子假说到玻尔的原子结构理论,量子概念已经从一个仅说明与辐射问题有关的形式上的假说,发展成为说明微观现象本质的必不可少的概念。因此,玻尔原子结构理论的建立,在量子论发展史上具有里程碑的重要意义^[8]。

1916年,美国物理学家密立根发表了光电效应实验结果,验证了爱因斯坦的光量子说^[10]。

在认识到光具有波粒二象性之后,为了解释一些经典理论无法解释的现象,1923年4月美国物理学家康普顿发表了X射线被电子散射所引起的频率变小现象,即康普顿效应。按经典波动理论,静止物体对波的散射不会改变频率。而按爱因斯坦光量子说这是两个“粒子”碰撞的结果^[10]。光量子在碰撞时不仅将能量也将动量传递给了电子,使光量子说得到了实验的证明^[10]。

光不但是电磁波,而且是一种具有能量动量的粒子。1924年,美籍奥地利物理学家泡利发表了“不相容原理”:原子中不能有两个电子同时处于同一量子态。这一原理解释了原子中电子的壳层结构。这个原理对所有实体物质的基本粒子(通常称为费米子,如质子、中子、夸克等)都适用,构成了量子统计力学——费米统计的基点。为解释光谱线的精细结构与反常塞曼效应,泡利建议对于原子中的电子轨道态,除了已有的与经典力学量(能量、角动量及其分量)对应的3个量子数之外应引进第4个量子数。这个量子数后来称为“自旋”,是表述基本粒子一种内在性质的物理量。

1924年,法国物理学家德布罗意提出了表达波粒二象性的爱因斯坦-德布罗意关系: $E=h\nu$, $p=h/\lambda$,将表征粒子性的物理量能量、动量与表征波性的频率、波长通过一个常数 h 相等^[10]。

1925年,玻恩、约当和海森堡抛弃了玻尔的电子轨道概念及其有关的古典运动学的量,发表了矩阵力学理论,认为观察者不能同时确定某时刻电子在空间的位置,也不能在轨道上跟踪它^[10]。

1926年,物理学家薛定谔提出了描述物质波连续时空演化的偏微分方程——薛定谔方程,把德布罗意的相位理论大大向前推进,建立了量子力学的另一个数学描述——波动力学,找到了一个量子体系的物质波的运动方程^[10]。后来物理学家将矩阵力学与波动力学统一起来,统称量子力学。

其后不久,薛定谔还证明了波动力学和矩阵力学的数学等价性;与此同时,玻恩也做了大量工作,解释了波函数的意义。而冯·诺依曼和狄拉克总结出了正则量子化方案,该方案能够把描述古典力学的基本方程改造成量子力学方程。量子力学新思想与波动力学相结合,建立起了完整的量子力学的理论体系^[10]。

玻恩等提出的量子力学形式可以称为代数形式。薛定谔提出的是局域形式(微分形式)。后来,费米还提出过量子力学的整体形式(积分形式)。

尽管迄今为止所有的实验结果都支持量子力学,但不是量子力学所有的基础性问题都能很好地解决。这其中最为大家所熟知的就是爱因斯坦和玻尔之间的争论。爱因斯坦始终认为现有量子力学只是一个统计理论,不足以描述统计系统中的单个系统,但是玻尔却认为现行的量子力学理论已经完备地描述了单个系统^[10,11]。这一争论的影响极其深远。这其中包括贝尔不等式的出现和实验验证^[12,13]。

量子力学在低速、微观的现象范围内具有普遍适用的意义。它是现代物理学基础之一,在现代科学技术中的表面物理、半导体物理、凝聚态物理、粒子物理、低温超导物理、量子化学以及分子生物学等学科的发展中,都有重要的理论意义。量子力学的产生和发展标志着人类认识自然实现了从宏观世界向微观世界的重大飞跃。

1.2.2 量子力学的定义

量子力学是研究微观粒子(如电子、原子、分子等)运动规律的理论。原子核和固体的性质以及其他微观现象,目前已基本上能从以量子力学为基础的现代理论中得到说明。现在量子力学不仅是物理学中的基础理论之一,还在化学和许多近代技术中得到了广泛的应用。

20世纪末到21世纪初,物理学的研究领域从宏观世界逐渐深入到微观世界;许多新的实验结果用经典理论已不能得到解释。大量的实验事实和量子论的发