量子计算和量子信息(一)

——量子计算部分

Quantum Computation and Quantum Information

Michael A. Nielsen
Isaac L. Chuang 著

赵千川 译

清华大学出版社

量子计算和量子信息(一)

——量子计算部分

Quantum Computation and Quantum Information

Michael A. Nielsen
Isaac L. Chuang 著

赵千川 译

清华大学出版社
北 京

内 容 简 介

本书是剑桥大学出版社出版的 Michael A. Nielsen 和 Isaac L. Chuang 合著的 Quantum Computation and Quantum Information 的量子计算部分的中译本.

量子计算与量子信息是涉及物理学、计算机科学和数学等多学科的综合性交叉研究领域. 本书首先介绍基础知识,然后着重介绍量子计算的主要研究成果,包括量子线路、量子 Fourier 变换及其应用、量子搜索算法和量子计算机的物理实现.

本书完整系统地介绍了量子计算与量子信息的最新成果和基本知识. 本书内容深入浅出,层次分明,参考文献丰富. 它既可作一般有兴趣的读者了解该领域的入门读物,也可用作大专院校的教材,或供大学高年级学生和研究生自学使用,对相关领域的研究人员也有很大的参考价值.

北京市版权局著作权合同登记号 图字:01-2001-4170

图书在版编目(CIP)数据

量子计算和量子信息(一)——量子计算部分/尼尔森,庄著;赵千川译.—北京:清华大学出版社,2003
书名原文:Quantum Computation and Quantum Information
ISBN 7-302-07289-2

Ⅰ.量… Ⅱ.①尼… ②庄… ③赵… Ⅲ.①量子力学—光通信 ②第五代计算机
Ⅳ.①TN929.1 ②TP387

中国版本图书馆 CIP 数据核字(2003)第 084993 号

出 版 者:清华大学出版社 **地 址**:北京清华大学学研大厦
http://www.tup.com.cn **邮 编**:100084
社 总 机:010-62770175 **客户服务**:010-62776969
组稿编辑:王一玲
文稿编辑:邹开颜
封面设计:常雪影
版式设计:刘祎淼
印 装 者:北京国马印刷厂
发 行 者:新华书店总店北京发行所
开 本:175×245 **印张**:26 **字数**:497 千字
版 次:2004 年 1 月第 1 版 2004 年 1 月第 1 次印刷
书 号:ISBN 7-302-07289-2/O·321
印 数:1~3000
定 价:45.00 元

译者序

量子计算与量子信息的研究可以追溯到几十年前，但真正引起广泛关注的是20世纪90年代中期.这期间发现了Shor量子因子分解算法和Grover量子搜索算法，这两类算法展示了量子计算从根本上超越经典计算机计算能力和在信息处理方面的巨大潜力. 与此同时，量子计算机和量子信息处理装置在物理实现的研究，成为继并行计算机、生物计算机等之后的非串行计算体系的又一热点.

量子计算与量子信息对人类社会最具影响也最为惊人的发现之一是，量子计算机能够迅速破解广泛采用的RSA密码系统. 掌握量子计算能力的制高点已成为关系信息安全的重要课题，不少国家已纷纷开始启动和资助相关的研究项目.

国外不少大学也已开设了有关课程. 译者2000年访问的美国Carnegie Mellon大学，他们在计算机系和物理系的研究生中开设了量子计算机课程. 所采用的教材正是剑桥大学出版社出版的Michael A. Nielsen和Isaac L. Chuang的英文版原著Quantum Computation and Quantum Information，本书是该著作量子计算部分的中译本.

原著共12章，分三个部分，分别介绍基础知识以及量子计算和量子信息. 由于篇幅宏大，为方便读者和照顾不同背景读者的需要，原著将内容安排为两个相对独立的主题：第一和第二部分一起构成学习量子计算的相对完整的材料；第一和第三部分构成量子信息相对完整的内容. 中译本继承原著者的思想，分为量子计算和量子信息两册单独出版，供读者根据需要选择. 本书限于量子计算内容(原著的第1～7章). 量子信息对应原著的第8～12章共5章内容，将单独出版.

本书在写作上定位为教材，因此照顾到广大读者在背景知识上的差异，尽可能以浅显和自成体系的方式叙述主要研究思路，力图深入浅出. 在细节的处理上较好地保持了严谨性和启发性的折衷. 特别是在一般专业读者较为生疏的量子力学方面，大胆地采用了基于线性代数的公理化体系，大大简化了学习主题的途径. 这与我国物理专业量子力学教学改革中的类似尝试不谋而合.

译者在翻译过程中可喜地看到，我国研究工作者也已经开始了相关领域的研究，并已取得了一些成果，如已有论文集和总结国内外研究成果的学术专著出版. 应该说量子计算与量子信息的研究还远没有成熟，该领域的研究充满着令人兴奋的挑战性课题. 译者衷心希望本书的出版能为量子计算与量子信息方面知识在我国的传播起到一定推动作用.

赵千川
2003 年 8 月于
清华大学

前 言

本书介绍量子计算和量子信息领域的主要思想和方法. 由于这个学科领域的迅速发展和其交叉学科性质，初学者对该领域最重要的方法和成果获得全面了解并不容易.

因而本书有两方面的目的. 首先介绍计算机科学、数学和物理方面必要的背景知识，读者需要具有三个学科中至少一个学科的相当于研究生入学水平；其中最重要的是要有一定的数学修养和希望了解量子计算与量子信息的愿望. 本书的第二个目的是详尽叙述量子计算与量子信息的核心成果. 通过深入学习，读者能够掌握这个令人激动的领域的基本工具和成果. 这可作为读者一般教育的一部分，或作为他独立从事量子计算与量子信息研究的准备.

本书结构

本书的基本框架如图 1 所示，共分为三个部分. 叙述的基本原则是从具体到抽象. 先讲量子计算后讲量子信息；先讲特殊的量子纠错码后讲量子信息论的一般结果；先讲例子后讲一般理论.

第一部分概述量子计算与量子信息领域的主要思想和成果，并介绍量子计算与量子信息所必需的计算机科学、数学和物理背景知识. 第 1 章是介绍性的，介绍该领域的发展历史和基本概念，着重介绍了历史上的若干重要的未解决问题(open problem). 这部分读者即使不具备计算机科学或物理学背景，也可以读懂. 第 2 章和第 3 章给出了更深入、详细的背景知识，分别详尽叙述量子力学和计算机科学的基本概念. 读者可根据个人的背景，重点阅读第一部分的某些章节，后面必要时可返回来阅读，来获得所需的量子力学和计算机科学知识.

第二部分详尽叙述量子计算. 第 4 章描述量子计算所需基本元素，给出更复杂应用中要用到的基本运算. 第 5 章、第 6 章描述两个已知的量子算法：量子 Fourier 变换和量子搜索算法. 第 5 章还解释量子 Fourier 变换如何用于解因子分解(factoring)和离散对数(discrete logarithm)问题，以及这些结果对密码系统的重要性. 第 7 章以已在实验室获得成功的几个实现为例，来阐述量

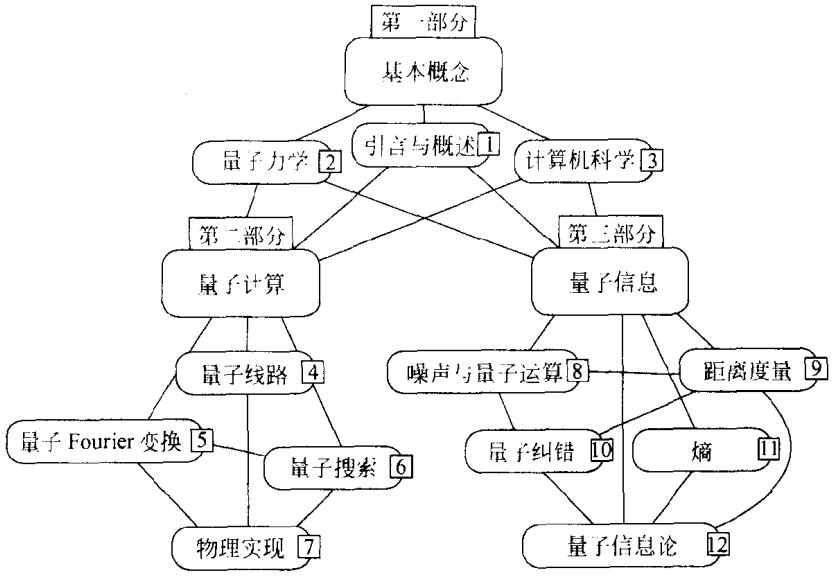


图 1　本书的结构

子计算机好的物理实现的一般原则.

第三部分有关量子信息:即如何用量子状态表示和传送信息,如何对付经典信息和量子信息的损失.第 8 章描述了用来理解现实世界量子信息处理的量子噪声性质和对理解量子噪声非常有用的量子运算形式化.第 9 章描述精确量化两个量子信息相似程度的距离度量.第 10 章讲量子纠错码,量子纠错码可用来使量子计算避免受到噪声的影响.这章的一个重要结果是阈值定理.阈值定理表明,在真实的噪声模型中,噪声原则上不对量子计算构成严重妨碍.第 11 章引入基础信息论的概念——熵,并给出经典和量子信息论中熵的许多性质.最后,第 12 章讨论量子状态和量子信道的信息承载属性,详尽描述这类系统传送经典信息和量子信息以及机密信息时具有的许多特殊性质.

本书配有大量练习和问题.练习贯穿在文中,为巩固对基本内容的理解而设,除个别情况,很容易在几分钟内完成这些练习.问题则安排在每章后边,用于补充一些由于正文篇幅限制,而未给出的有趣的新材料.问题常由几部分构成,目的是对特定的思路作一定深度的阐述.有几个问题在本书付印时尚未解决,这在叙述时作了说明.每章以整章主要结果的概要结束,并以"历史和进一步阅读的材料"为一节给出整章的主要思路、参考文献和推荐的阅读材料.

本书正文之前有目录、名词和记号.

本书正文之后包括五个附录和一个参考文献.

附录 A 复习初等概率论的一些基本概念、记号和结论.我们假设读者熟悉这

部分内容，包括进来的目的只是便于参考. 同样为方便读者，附录 B 复习群论的基本概念. 附录 C 包含量子计算的一个重要结论 Solovay-Kitaev 定理的证明，该定理表明量子门的有限集合可以用来快速逼近任意的量子门. 附录 D 复习理解量子因子分解和离散对数算法以及 RSA 密码系统所必需的数论知识. RSA 密码系统在下册的附录中介绍. 附录 E 包括量子计算与量子信息中最重要的定理之一 Lieb 定理的证明，该定理是重要的熵不等式（如著名的次可加不等式）的雏形. 因为 Solovay-Kitaev 定理和 Lieb 定理的证明较长，所以需要独立于正文给出.

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.

量子计算和量子信息领域发展非常迅速，这使得我们对所有的论题无法按照希望的深度展开. 但三个方面需特别提及. 第一个主题是纠缠（entanglement）测量，如书中所解释的，纠缠现象是量子隐形传态（teleportation）、快速量子算法和量子纠错等效应中的关键要素，简言之，是量子计算与量子信息的利器. 纠缠作为一种新的物理资源，寻求、驾驭它的规律和用途正成为一个兴起的研究方向. 我们认为尽管这方面的研究极富吸引力，但还没有达到像本书其他主题那样完整的程度，所以我们在第 12 章仅给出一个简述. 同样，考虑到极富吸引力的分布式量子计算（有时称量子通信复杂性）的研究非常活跃，为避免书未出版而内容过时，所以没有涉及. 量子信息处理机的实现也已成为一个有趣和成果丰富的方向，我们仅用一章的篇幅介绍，但物理实现有很多的内容，这涉及物理、化学和工程中更多的领域，因而不得不割爱.

如何使用本书

本书可用作多种用途，可以作为各类课程的基础教材，从用于讲授量子计算与量子信息的短期专题基础讲座到涉及整个领域的全年的正式课程. 只想对量子计算与量子信息稍作了解的读者可以自学；想进入研究前沿的读者也可采用本书. 本书的目的之一还在于作为该领域的一本参考书，特别希望它对初次接触这个领域的研究人员有价值.

致自学读者

本书考虑到自学读者的需要，文中准备了大量的练习，可用来理解正文内容，并进行自我测试. 目录和每章后边的提要可以帮助读者很快决定哪些章节需要透彻学习. 图 1 所示的关系图可帮助读者决定阅读的顺序.

致教师

本书覆盖了很宽范围的主题，可以作为多种课程的基础课本.

一个学期的量子计算课程可以根据学生的背景选择：第 1 到第 3 章部分内容、第 4 章量子线路、第 5 章、第 6 章量子算法的全部、第 7 章物理实现的一部分、第 8 到第 10 章特别是第 10 章关于量子纠错的全部内容.

一学期的量子信息课程也可以根据学生的背景选择：第 1 到第 3 章部分内容、第 8 到第 10 章关于量子纠错、第 11 章量子熵和第 12 章量子信息论.

一学年课程可以覆盖整本书的内容，还可以加增从部分章节的“历史和进一步阅读”中选择的额外阅读材料. 量子计算与量子信息领域本身还可为学生提供很好的研究题目.

除了用于量子计算与量子信息课程，我们还希望本书的内容作为物理系学生的量子力学专业的引论. 传统的量子力学课的引论非常强调偏微分方程的数学工具，我们认为这常常阻碍学生对基本思想的把握. 量子计算与量子信息为理解量子力学的基本概念和特殊现象提供了绝好的思想实验场所. 这样的课程可以集中于第 2 章量子力学引论、第 4 章量子线路的基本内容、第 5 章、第 6 章量子算法的一部分、第 7 章量子计算物理实现、然后根据兴趣选择本书第三部分的内容.

致学生

我们尽量使本书内容自成体系. 主要例外是我们偶尔会略去一些需要读者自己弄明白的论述，这些地方留作练习，当然我们假设读者愿意尝试解决书中所有的练习. 几乎所有练习都可在几分钟之内解决，如果读者对许多练习遇到很多困难，也许应该回到前面去掌握一些关键的概念.

进一步阅读的材料

如前所述，每章最后有一节“历史和进一步阅读的材料”，还有一些内容包括很广的参考文献. Preskill[Pre98b] 关于量子计算与量子信息的讲义与本书的角度有些不同. 关于专题的好的综述文章有（按在本书中出现的先后）：Aharonov 关于量子计算的综述[Aha99b]，Kitave 关于算法和纠错的综述[Kit97b]，Mosca 关于量子算法的学位论文[Mos99]，Fuch 关于量子信息中可区分性和距离测度的学位论文[Fuc96]，Gottesman 关于量子纠错的学位论文[Got97]，Preskill[Pre97] 关于量子纠错的综述，Nielsen 关于量子信息论的学位论文[Nie98] 和 Bennett 与 Shor[BS98]、Bennett 与 Divinceno 关于量子信息论的综述[BD00]. 其他有价值的参考资料包括 Gruska 的书[Gru99] 和 Lo、Spiller 和 Popescu 编辑的综述文集[LSP98].

更正

任何大篇幅的文本总有一些错误和疏忽，本书也不例外. 如果你发现任何错误或有任何关于本书的评论，请通过电子邮件发给：qci@squint. org. 本书英文版的更正信息可在以下网址找到：http://www. squint. org/qci/.

名词和记号

量子计算与量子信息中一些名词和记号有两个以上含义，这里收集了许多本书经常使用的条目及其在本书中的约定，以避免混淆.

线性代数与量子力学

除特别声明，所有向量空间均假定为有限维. 许多情况下该限制是不必要的，或者可以通过其他技巧去掉，不过作这样的全局性限制，可以使表达更易理解，也不会分散读者对运用结果的注意力.

半正定算子 A 满足对任意 $|\psi\rangle$，$\langle\psi|A|\psi\rangle\geqslant 0$. 正定算子 A 满足对任意 $|\psi\rangle\neq 0$，$\langle\psi|A|\psi\rangle>0$. 算子的支集定义为正交于其核的向量空间. Hermite 算子即为由非零特征值的特征向量所张成的向量空间.

记号 U（或 V）一般用于表示酉算子或酉矩阵. H 通常用来表示 Hadamard 门，有时也表示量子系统的 Hamilton 函数.

向量有时写作列的形式，如

$$\begin{bmatrix}1\\2\end{bmatrix} \tag{1}$$

有时写成便于阅读的形式(1,2)，后一种形式应理解为列向量的简写. 对于用作量子比特（或称量子位，qubit）的双态量子系统，常将状态 $|0\rangle$ 等同于向量 (1,0)，状态 $|1\rangle$ 等同于(0,1). 这里采用 Pauli sigma 矩阵的传统定义（参见下面的“常用的量子门和线路的符号”). 注意，习惯上 Pauli sigma z 矩阵为 $\sigma_z|0\rangle=|0\rangle$，$\sigma_z|1\rangle=-|1\rangle$，这与某些物理学家（通常不是计算机科学家或数学家）的直观期待相反. 这个不一致来源于 σ_z 的本征态 $+1$ 常被物理学家等同于激发态，因而很多人很自然地将其等同于 $|1\rangle$，而不是像本书中等同于 $|0\rangle$. 我们这样做是为了保持线性代数矩阵元素指标的一致性，也就是让 σ_z 的第一列自然地表示 σ_z 在 $|0\rangle$ 上的作用，第二列表示 σ_z 在 $|1\rangle$ 上的作用，这个做法在量子计算与量子信息领域内是通行的. 除了 σ_x，σ_y 和 σ_z 这些 Pauli sigma 矩阵的传统记号外，用 σ_1，σ_2，σ_3 来表示这三个矩阵也很方便. 我们用 σ_0 表示 2×2 单位阵. 不过最常用的记号还是用 I，X，Y 和 Z 分别表示 σ_0，σ_1，σ_2 和 σ_3.

信息论和概率

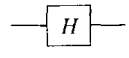
按照信息论的习惯，除非特别说明，对数总是取以 2 为底. 我们用 $\log(x)$ 表示以 2 为底的对数，在个别情况下用到 $\ln(x)$ 表示自然对数. **概率分布**指满足 $p_x \geqslant 0$ 和 $\sum_x p_x = 1$ 的有限实数集合 p_x. 半正定算子 A 相对于半正定算子 B 的**相对熵**定义为 $S(A \parallel B) \equiv \mathrm{tr}(A\log A) - \mathrm{tr}(A\log B)$.

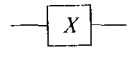
杂项

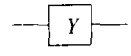
$\oplus$ 记模 2 的加法. 全书中 z 念作“zed”.

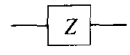
常用量子门和线路的符号

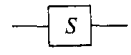
引入设计量子线路常用的表示酉变换的一些方框符号，为方便读者，收集如下：酉变换的行和列从左到右、从上到下标为 $00\cdots0, 00\cdots1$ 到 $11\cdots1$，最下方的线是重要性最小的线. 注意 $e^{i\pi/4}$ 是 i 的平方根，故 $\pi/8$ 门是相位门(phase gate)的平方根. 相位门本身是 Pauli-Z 门的平方根.

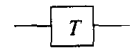
Hadamard 门  $\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$

Pauli-X 门  $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$

Pauli-Y 门  $\begin{bmatrix}0 & -\mathrm{i}\\ \mathrm{i} & 0\end{bmatrix}$

Pauli-Z 门  $\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$

相位门  $\begin{bmatrix}1 & 0\\ 0 & \mathrm{i}\end{bmatrix}$

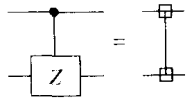
$\frac{\pi}{8}$ 门  $\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$

受控非门  $\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$

交换门

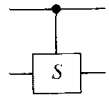
$$\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}$$

受控 Z 门



$$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix}$$

受控相位门



$$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&i\end{bmatrix}$$

Toffoli 门

$$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$$

Fredkin(受控交换) 门

$$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\end{bmatrix}$$

测量运算

投影到$|0\rangle$和$|1\rangle$上

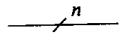
量子比特

承载单量子比特的线(时间为先左后右)

经典比特

承载单经典比特的线

n 量子比特



承载 n 量子比特的线

CONTENTS

目 录

第二部分 量 子 计 算