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

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。

赵千川，河北唐县人，清华大学自动化系智能与网络化系统研究中心副教授，主要研究离散事件动态系统(DEDS)理论及其在制造、通信等领域的应用。1987年考入清华大学自动化系，1996年获得控制理论与应用专业工学博士学位，并留校任教。2000年3月至4月得到国家留学基金资助，赴美国Carnegie Mellon大学从事访问研究。曾获2000年度“何潘清荫”优秀论文奖，该奖为DEDS领域对华人的最高奖。

ISBN 7-302-07289-2



9 787302 072898 >

定价：45.00元

0413
8
:1

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

北方工业大学图书馆
00544625

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.

Michael A. Nielsen, Isaac L. Chuang
Quantum Computation and Quantum Information
© Cambridge University Press 2000
First Published 2000
All Rights Reserved.
For sale in Main land China only.

本书翻译版由剑桥大学出版社授权清华大学出版社在中国境内独家出版、发行.
未经出版者书面许可,不得以任何方式复制或抄袭本书的任何部分.

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(…)-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 081993 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

本书如有在文字不清、漏印以及缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。联系电话:(010)62770175-3103 或(010)62795704

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

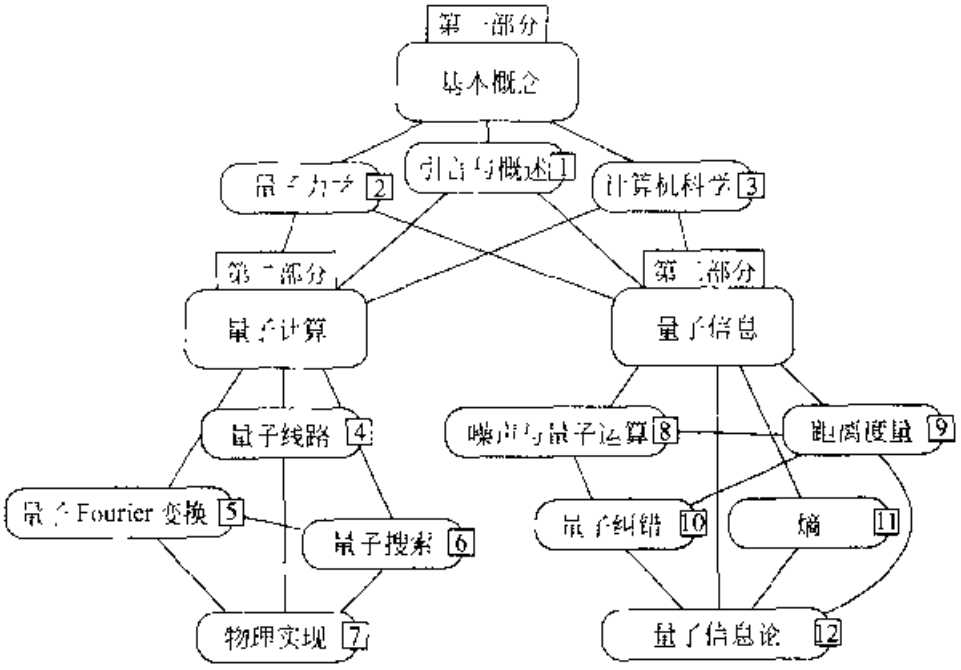


图 1　本书的结构

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

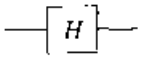
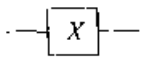
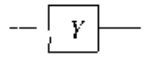
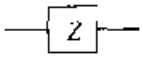
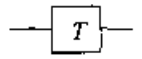
按照信息论的习惯，除非特别说明，对数总是取以 2 为底. 我们用 $\log(x)$ 表示以 2 为底的对数，在个别情况下用到 $\ln(x)$ 表示自然对数. **概率分布**指满足 $p_i \geqslant 0$ 和 $\sum_i p_i = 1$ 的有限实数集合 p_i，半正定算子 A 相对于半正定算子 B 的**相对熵**定义为 $S(A \| B) \equiv \mathrm{tr}(A\log A) - \mathrm{tr}(A\log B)$.

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.

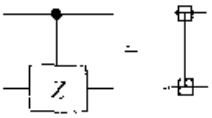
Hadamard 门		$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Pauli X 门		$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
Pauli-Y 门		$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$
Pauli-Z 门		$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
相位门		$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$
$\frac{\pi}{8}$ 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



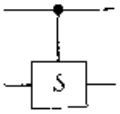
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

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

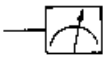


$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Fredkin(受控交换)门

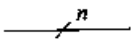


$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

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

译者序 …… 1
前言 …… 3
名词和记号 …… 9

第一部分 基本概念

第1章 引言与概述 …… 3
1.1 全貌 …… 1
1.1.1 量子计算与量子信息的历史 …… 4
1.1.2 未来发展方向 …… 12
1.2 量子比特 …… 13
1.2.1 多量子比特 …… 16
1.3 量子计算 …… 17
1.3.1 单量子比特门 …… 17
1.3.2 多量子比特门 …… 20
1.3.3 除计算基以外的基的测量 …… 21
1.3.4 量子线路 …… 22
1.3.5 量子比特复制线路? …… 23
1.3.6 例子:Bell 态 …… 24
1.3.7 例子:量子隐形传态 …… 25
1.4 量子算法 …… 27
1.4.1 量子计算机上的经典计算 …… 28
1.4.2 量子并行性 …… 29
1.4.3 Deutsch 算法 …… 31
1.4.4 Deutsch Jozsa 算法 …… 32
1.4.5 量子算法的总结 …… 34
1.5 实验量子信息处理 …… 40
1.5.1 Stern-Gerlach 实验 …… 40
1.5.2 实际量子信息处理的前景 …… 43
1.6 量子信息 …… 47

1.6.1 量子信息论：例子问题 …… 48
1.6.2 更一般背景下的量子信息 …… 53

第 2 章 量子力学引论 …… 56
2.1 线性代数 …… 57
2.1.1 基与线性无关 …… 58
2.1.2 线性算子与矩阵 …… 59
2.1.3 Pauli 阵 …… 60
2.1.4 内积 …… 61
2.1.5 特征向量和特征值 …… 64
2.1.6 伴随与 Hermite 算子 …… 65
2.1.7 张量积 …… 68
2.1.8 算子函数 …… 70
2.1.9 对易式和反对易式 …… 71
2.1.10 极式分解和奇异值分解 …… 73
2.2 量子力学假设 …… 74
2.2.1 状态空间 …… 74
2.2.2 演化 …… 75
2.2.3 量子测量 …… 78
2.2.4 区分量子状态 …… 80
2.2.5 投影测量 …… 81
2.2.6 POVM 测量 …… 83
2.2.7 相位 …… 86
2.2.8 复合系统 …… 87
2.2.9 量子力学：总览 …… 89
2.3 应用：超密编码 …… 90
2.4 密度算子 …… 91
2.4.1 量子状态的系综 …… 91
2.4.2 密度算子的一般性质 …… 93
2.4.3 约化密度算子 …… 97
2.5 Schmidt 分解和纯化 …… 101
2.6 EPR 和 Bell 不等式 …… 103

第 3 章 计算机科学简介 …… 111
3.1 计算的模型 …… 112

3.1.1 Turing 机 …… 113
3.1.2 线路 …… 120
3.2 计算问题的分析 …… 124
3.2.1 如何量化计算资源 …… 125
3.2.2 计算复杂性 …… 126
3.2.3 判定问题和复杂性 P 类和 NP 类 …… 129
3.2.4 更多的复杂性类 …… 137
3.2.5 能量与计算 …… 140
3.3 对计算科学的思考 …… 148

第二部分 量 子 计 算

第 4 章 量子线路 …… 157
4.1 量子算法 …… 158
4.2 单量子比特运算 …… 159
4.3 受控运算 …… 163
4.4 测量 …… 170
4.5 通用量子门 …… 173
4.5.1 两级酉门(two-level unitary gate)是通用的 …… 173
4.5.2 单量子比特门和受控非门是通用的 …… 175
4.5.3 通用运算的一个离散集合 …… 178
4.5.4 近似任意酉门一般是难的 …… 182
4.5.5 量子计算复杂性 …… 184
4.6 计算的量子线路模型的总结 …… 185
4.7 量子系统的仿真 …… 187
4.7.1 仿真原理 …… 188
4.7.2 量子仿真算法 …… 189
4.7.3 一个说明性的例子 …… 192
4.7.4 量子仿真的展望 …… 193

第 5 章 量子 Fourier 变换及其应用 …… 198
5.1 量子 Fourier 变换 …… 199
5.2 相位估计 …… 203
5.2.1 性能和要求 …… 205
5.3 应用：求阶和因子问题 …… 207
5.3.1 应用：求阶 …… 208

5.3.2 应用：因子分解 …… 214
5.4 量子 Fourier 变换的一般应用 …… 217
5.4.1 求周期问题 …… 217
5.4.2 离散对数问题 …… 219
5.4.3 隐含子群问题 …… 221
5.4.4 其他量子算法 …… 223

第 6 章 量子搜索算法 …… 228
6.1 量子搜索算法 …… 228
6.1.1 oracle …… 228
6.1.2 过程 …… 230
6.1.3 几何可视化 …… 231
6.1.4 性能 …… 234
6.2 作为量子仿真的量子搜索 …… 236
6.3 量子计数 …… 240
6.4 NP 完全问题解的加速 …… 243
6.5 非结构化数据库的量子搜索 …… 244
6.6 搜索算法的最优性 …… 248
6.7 黑箱算法的极限 …… 250

第 7 章 量子计算机：物理实现 …… 256
7.1 指导性原则 …… 257
7.2 量子计算的条件 …… 258
7.2.1 量子信息的表示 …… 258
7.2.2 酉变换的性能 …… 260
7.2.3 基准初态的制备 …… 260
7.2.4 输出结果的测量 …… 261
7.3 谐振子量子计算机 …… 262
7.3.1 物理装置 …… 262
7.3.2 Hamilton 量 …… 262
7.3.3 量子计算 …… 264
7.3.4 不足 …… 265
7.4 光子量子计算机 …… 266
7.4.1 物理装置 …… 266

7.4.2 量子计算 …… 268
7.4.3 不足 …… 274
7.5 光学共振腔量子电动力学 …… 275
7.5.1 物理装置 …… 275
7.5.2 Hamilton 量 …… 279
7.5.3 单光子单原子吸收与折射 …… 280
7.5.4 量子计算 …… 283
7.6 离子阱(ion trap) …… 286
7.6.1 物理装置 …… 287
7.6.2 Hamilton 量 …… 293
7.6.3 量子计算 …… 295
7.6.4 实验 …… 297
7.7 核磁共振 …… 300
7.7.1 物理装置 …… 301
7.7.2 Hamilton 量 …… 302
7.7.3 量子计算 …… 306
7.7.4 实验 …… 311
7.8 其他实现方案 …… 318

附录 A 概率论基础 …… 327

附录 B 群论 …… 329
B.1 基本定义 …… 329
B.1.1 生成元 …… 330
B.1.2 循环群 …… 330
B.1.3 陪集 …… 331
B.2 表示 …… 331
B.2.1 等价性与可约性 …… 331
B.2.2 正交性 …… 332
B.2.3 正规表示 …… 333
B.3 Fourier 变换 …… 333

附录 C Solovay-Kitaev 定理 …… 335

附录 D 数论 …… 343
D.1 基础知识 …… 343
D.2 模算术与 Euclid 算法 …… 344
D.3 因子问题向求阶问题的归约 …… 349
D.4 连分式 …… 351
附录 E 公钥密码术与 RSA 密码系统 …… 356
参考文献 …… 361

第一部分

基本概念

第 1 章

引言与概述

科学代表着一个时代最为大胆的思想. 她纯粹是人为的. 但我们相信，通过追寻梦想—发现—解释—梦想的不断循环，我们可以开拓一个个新领域，世界最终会变得越来越清晰，我们最终会了解宇宙的奥妙. 所有的奥妙都是彼此联系和有意义的.

——*Edward O. Wilson*

信息是物理的.

——*Rolf Landauer*

量子计算与量子信息的基本概念是什么？这些概念是怎么来的？有什么用途？本书如何讲述这些内容？本章通过给出量子计算与量子信息一个粗线条的全景来回答这些问题，目的是让读者对该领域的核心概念及发展过程有个基本了解，帮助读者决定如何阅读本书其他部分.

1.1 节讲述量子计算与量子信息的发展历史. 本章其他小节简介该领域中的几个基本概念：量子比特(1.2 节)，量子计算机、量子门和量子线路(1.3 节)，量子算法(1.4 节)，实验量子信息处理(1.5 节)和量子信息与通信(1.6 节).

沿着这条思路，通过本章讲授的基本数学知识，给出如量子隐形传态和某些简单的量子算法那样的说明和易于理解的内容. 内容是自成体系的，即使没有计算机科学或物理学知识的人也可读懂. 随着论述的展开，我们还指明了后面相对应的章节，由它提供更深入的讨论，而在后面章节中又可找到参考文献和建议的阅读材料.

如果阅读中发现有不太清楚的地方，不妨跳过. 有些地方我们不得不用到少量后面才会完整解释的技术术语，这些术语可以暂且简单地接受下来，等深入理解了全部术语后，读者可再返回来. 本章的重点在于该领域的全貌，细节留待后面章节阐述.

1.1 全 貌

量子计算与量子信息的研究对象是用量子力学系统能够完成的信息处理任务.看起来非常简单和自然,对不对?但正像许多简单而深刻的思想一样,人们想到用量子力学系统进行信息处理其实花了很长时间.要明白其中的原因,我们必须回溯历史,逐个考察为量子计算与量子信息提供基本概念的每个领域——量子力学、计算机科学、信息论和密码系统.当简要回顾这些领域历史的时候,为了对在量子计算与量子信息中已成为一体的不同的诸方面有一点感觉,我们需要先后采用物理学家、计算机科学家、信息论专家和密码系统专家的视角.

1.1.1 量子计算与量子信息的历史

20 世纪初叶,科学经历了一场出人意料的革命,物理学遇到了一系列危机.问题在于当时的物理学理论(现在称为经典物理学)作出一些荒唐预言,诸如存在包含无穷能量的"紫外灾"或电子必然旋转着进到原子核内部.起初这些问题是通过在经典物理学中附加特别的假设来解决,但随着人们对原子和辐射更好的了解,这些尝试性的解释越来越让人困惑.经过四分之一世纪的混乱,危机到 20 世纪 20 年代早期达到高潮,并导致量子力学这一现代理论的创立.量子力学一出现就成为科学不可缺少的一部分,并已有无数成功应用的例子,包括原子结构、恒星核聚变、超导体、DNA 结构和自然界基本粒子等的几乎所有方面.

什么是量子力学?量子力学是一个数学框架或一套构造物理学理论的规则,例如量子电动力学就是一套以惊人的精确度刻画原子和光的相互作用的物理理论.量子电动力学是在量子力学框架下建立的,不过它还包含量子力学未规定的一些特殊规则.量子力学与像量子电动力学那样的特殊物理理论之间的关系,很像计算机操作系统与特殊应用软件之间的关系——操作系统设置某些基本参数和运行模式,应用软件则完成具体任务.

量子力学的规则很简单,但即使是专家有时也会感到违反直观.量子计算与量子信息的先驱长期存在着使量子力学更好地被理解的愿望.量子力学最著名的批判者 Einstein,直到去世都不能接受他帮助发明的这个理论.几代物理学家一直在为使量子力学作出的预言更令人满意而奋斗.量子计算与量子信息的一个目标就是增进我们对量子力学直观上的把握,使它的预言让人更明白.

例如在 20 世纪 80 年代早期,人们感兴趣的一个问题是,能否通过量子效应进行超光速的信号传递,这按照 Einstein 相对论绝对不可能.解决这一问题的关键在于能否克隆未知量子状态,即复制量子状态.如果克隆是可能的,那么就有可能借

助量子效应进行超光速的信号传递.尽管克隆对经典信息(想想这本书上的信息是从哪里来的!)而言太容易了,但是在量子力学的一般意义下不可能.这条20世纪80年代早期发现的不可克隆定理是量子计算与量子信息的早期成果之一.从此对不可克隆定理有了许多改进,我们现在已掌握了了解量子克隆设备(必然是不完美)能力的工具.这些工具反过来已用于理解量子力学的其他方面.

对量子计算与量子信息的发展做出过贡献的相关历史论据还可追溯到20世纪70年代对单量子系统的完全能控性的研究.在那之前,量子力学应用的典型做法是对包含大量量子力学系统的批量样本的总体控制,但单个量子力学系统无法单独访问.例如超导现象有很好的量子力学解释,但由于超导体涉及导电金属的巨大样本(相对原子尺度而言),所以只能探测到其量子性质的几个方面,而不能访问构成超导体的单量子系统.虽然粒子加速器可以让我们有限度地访问单量子系统,但是几乎无法对其实施控制.

从20世纪70年代起,对单量子系统的控制有了发展.如有了捕捉单个原子的"原子阱",可使原子与其环境分离并对原子行为的许多方面进行非常精密的探测;扫描隧道显微镜可被用于移动单个原子和按要求排列原子;还出现了可以运送单电子的电子设备.

这一切试图完全控制单量子系统的努力目的何在?撇开技术原因,从纯粹科学的角度看,主要的原因是研究人员有一种预感,科学上最深刻的见解往往出现在获得探索自然新领域的一种方法的时刻.例如20世纪的30年代到40年代射电天文学的发明导致一系列重大发现,包括银河系的中心、脉冲星、类星体等;低温物理的惊人成就也是在人们找到降低各种系统温度的方法后达成的.同样,通过完全控制单量子系统,我们正在探索自然的未知领域,希望发现新的和意外的现象.我们在这些方向上刚迈出第一步,就已经在这个领域有了几项令人惊喜的发现.完全控制单量子系统,以及扩展到更复杂的系统后,我们又会有什么发现?

量子计算与量子信息的研究很自然地适合这样一项计划.它为试图更好地操作单量子系统的人们提供了一系列有价值的挑战性课题,也刺激了新的实验技术的发展,还指出了实验研究最有意义的方向.反过来,控制单量子系统对于把强大的量子力学工具运用到量子计算与量子信息研究起着根本作用.

尽管人们有这样强烈的兴趣,建造量子信息处理系统的努力到目前为止只是取得初步的成功.在几个量子比特上进行几十步操作的小型量子计算机代表着量子计算的最高水平.用于长距离保密通信的量子密码术(quantum cryptography)的实验原型也已出现,并且在某些实际应用的水平上或许会被采用.然而,制造解决实际问题的大规模量子信息处理装置的技术,仍将是物理学家和工程师未来面临的巨大挑战.

让我们把注意力从量子力学转到20世纪另一项伟大的智慧成就:计算机科

学. 计算机科学的起源可以追溯很久远的历史，例如汗默拉比(Hammurabi，大约公元前 1750 年)的楔形字板显示巴比伦人(Babylonian)有相当复杂的算法思想，有些思想看来可以追溯到更早的年代.

伟大的数学家 Alan Turing 在 1936 年发表的一篇令人瞩目的论文宣告了现代计算机科学的形成. Turing 以一种抽象的方式详细描述了我们现在所说的可编程计算机，也就是以他的名字命名的称之为 Turing 机的计算模型. Turing 证明了存在一个通用 Turing 机可以模拟任何其他 Turing 机；进而，他宣称通用 Turing 机完全刻画了算法手段所能完成的所有任务，即任何可以由硬件(如现代计算机)执行的算法都有通用 Turing 机上的等价算法完成完全相同的任务. 这个称为 Church-Turing 论题的论断断言了在某一物理设备上可完成的算法和数学上严格的通用 Turing 机概念的等价性. 这个论题的广泛接受为计算机科学丰富的理论的发展奠定了基础.

Turing 的论文发表不久，建成了第一台电子计算机. John von Neumann 为采用实际元件实现通用 Turing 机的全部功能，设计了一个简单的理论模型. 到 1947 年，当 John Bardeen、Walter Brattain 和 Will Shockley 发明了晶体管后，硬件的发展才真正起飞，从那时起，计算机硬件的能力以惊人的速度成长，以致 1965 年 Gordon Moore 把这种成长概括为 Moore 律，即计算机的能力以固定的速率成长，大约每两年增加一倍.

令人吃惊的是，从 20 世纪 60 年代开始，Moore 律在几十年时间里都近似成立，然而，大多数观察家预期这将在 21 世纪的前 20 年内结束. 制造计算机的传统方法在解决规模上的困难时开始显得力不从心，当电子器件越做越小的时候，它的功能开始受到量子效应的干扰.

Moore 律最终失效问题的一个可能解决办法是采用不同的计算模式. 量子计算理论就是这类模式的一种，量子计算基于量子力学而非经典物理学的思想进行计算. 有趣的是，虽然传统计算机可以模拟(simluate)量子计算机，但似乎不可能以一种有效的方式去模拟. 量子计算机从速度上对经典计算机有本质的超越，这种速度上的优越性太重要了，以致许多研究者相信在经典计算机和量子计算机的能力之间存在着无法跨越的鸿沟.

量子计算机的“有效”和“非有效”模拟指什么？早在量子计算机出现之前，回答这个问题需要的关键概念就已经被定义了. 特别是计算复杂性理论从数学上精确定义了“有效”和“非有效”算法的概念. 粗略地说，有效算法解决问题需要的时间，是问题规模的多项式；相反，非有效算法需要超多项式(典型情况是指数)时间. 20 世纪 60 年代末到 70 年代初，人们注意到通过 Turing 机模拟其他计算模型，某个计算模型可以有效解决的问题在 Turing 机上也可以有效解决，看来 Turing 机作为计算模型的功能不逊于任何别的计算模型. 这个观点概括为加

强的 Church-Turing 论题：任何算法过程都可以用 Turing 机进行有效模拟.

强 Church-Turing 论题的加强之处在于“有效”一词. 如果这一论题成立，就意味着无论用什么机器运行算法，这个机器都可以用标准的 Turing 机进行有效模拟. 这个加强很重要，因为这意味着要分析一项计算任务是否可以有效完成，可以限制在 Turing 机计算模型上进行.

对强 Church Turing 论题的一个挑战来自模拟计算(analog computation)领域. Turing 的年代，许多不同的研究小组注意到某些模拟计算机可以有效解决一些被认为在 Turing 机无法有效求解的问题. 表面上看模拟计算机否定了强 Church-Turing 论题，不幸的是，对模拟计算机，在考虑噪声的现实情形下，其计算能力在所有已知的例子上都会消失，它们无法有效解决 Turing 机所不能有效解决的问题. 这个教训——即评价计算模型的效率时，必须考虑现实噪声的影响——是量子计算与量子信息研究初期面临的最大挑战之一. 这个挑战随量子纠错码和容错量子计算理论的发展而得到成功解决. 因为与模拟计算不同，量子计算原则上可以容许有限的噪声而保持计算上的优越性.

对强 Church-Turing 论题的第一个重大挑战出现在 20 世纪 70 年代中期. 当时 Robert Solovay 和 Volker Strassen 证明通过随机化算法可以测试一个整数是否为素数，也就是说，随机性是 Solovay-Strassen 测试算法的一个实质部分. 该算法并不确定一个整数是否一定是素数或合数，相反，该算法确定一个数是素数或合数的可能性. 对 Solovay-Strassen 测试算法进行几次重复，就可以几乎肯定一个数是素数或合数. 特别有趣的是，Solovay-Strassen 测试算法提出的时候没有已知的有效确定型测试算法，于是，好像带有随机数发生器的计算机可以有效进行计算任务，而此计算任务在经典的确定型 Turing 机上无法有效进行. 这个发现激励人们寻找其他随机算法，这方面已取得很漂亮的结果，并成为一个活跃的研究方向.

随机化算法形成了对强 Church-Turing 论题的挑战，暗示存在着在确定型 Turing 机上无法有效求解的有效可解问题. 这个挑战可以通过对强 Church-Turing 论题稍做修改解决：任何算法过程都可以用概率 Turing 机进行有效模拟.

强 Church-Turing 论题的这种就事论事的修改令人不安. 将来难道一定不会有另外一种计算模型能有效求解 Turing 计算模型无法求解的问题吗？有什么途径使我们找到一种保证能有效模拟其他任何计算模型的计算模型？

在这个问题的启发下，1985 年 David Deutsch 提出是否可以用物理学定律推导出任何更强的 Church-Turing 论题的问题. Deutsch 没有用特定假设的方法，他试图用物理学理论来为 Church-Turing 论题建立和当今物理理论可信程度相当的基础，特别地，他试图定义一种能够有效模拟任意物理系统的计算装置. 由于量子

力学是物理学的最终规律，Deutsch 很自然地考虑在量子力学原理下的计算装置. 这些装置，仿照了 49 年前 Turing 定义的机器，最终导出了本书讲的现代量子计算机的概念.

到本书写作的时候，还不清楚 Deutsch 的通用量子计算机的概念是否足以有效模拟任意的物理系统. 证明或否定这个猜想是量子计算与量子信息研究的一个重要的未解决的问题. 量子场理论的某些效应或者甚至是基于弦论的更奇特效应，量子引力或者其他物理理论，都有可能为我们提供比 Deutsch 的通用量子计算机更强大的计算模型，只是现在，我们还不知道.

Deutsch 的量子计算机模型确实向强 Church-Turing 论题提出挑战. Deutsch 曾问道，量子计算机是否可以有效解决经典计算机，甚至是概率 Turing 机不能有效解决的计算问题，然后他举出一个简单的例子，来说明量子计算机确实可能从计算机能力上超过那些经典计算机.

随后十年内许多人努力改进 Deutsch 令人瞩目的初步结果，这些努力到 1994 年 Peter Shor 展示两个极其重要的问题——寻找整数的素因子问题和解决所谓离散对数问题——可以用量子计算机有效解决时，达到顶点. 这方面研究受到广泛关注的原因是，人们仍相信这两个问题在经典计算机上没有有效解法. Shor 的结果是量子计算机比 Turing 机，甚至概率 Turing 机更为强大的有力证据. 量子计算机功能强大的进一步的证据出现在 1995 年当 Lov Grover 证明另一个重要问题——在没有结构的搜索空间上进行搜索的问题——在量子计算机上可以被加速时. 虽然 Grover 算法没有达到 Shor 算法那样明显的加速，但搜索方法的广泛适用性引起人们对 Grover 算法相当的关注.

大约在 Shor 和 Grover 算法发现的同时，许多人致力于发展 Richard Feynman 在 1982 年建议的一个想法. Feynman 指出似乎在经典计算机上模拟量子力学系统存在本质困难，并建议在量子力学原理的基础上构造计算机以克服那些困难. 1990 年几个研究小组使这个思想具体化，证明在经典计算机上没有已知有效模拟的系统用量子计算机有效模拟是可能的. 量子计算机未来的一个主要的应用似乎是用来模拟那些在经典计算机上难以模拟的量子力学系统，这对科学和技术领域有深远意义.

量子计算机比经典计算机更快解决的问题还有哪些？简要的回答是我们不知道. 找到好的量子算法看起来是困难的，悲观主义者也许会认为除已发现的应用外，量子计算机并没任何其他好处. 设计量子计算机算法困难的原因是，设计者面临经典计算机所没有的两方面难题. 首先，人的直觉植根于经典世界，如果借助于直觉构造算法，则想到的只能是经典思想. 为设计好的量子算法，我们必须至少部分地"关闭"经典直觉，而利用量子效应去达到期望的算法目的. 其次，设计出纯粹的量子力学算法并不一定真正有意义，算法必须超过所有已知的经典算法！ 因此，

人们或许可以找到采用纯粹量子力学效应的算法，但由于已经有了可匹敌的经典算法而无法引起广泛兴趣. 这两方面问题的组合使得构造新的量子力学算法是未来的挑战.

一般而言，我们可能会问是否可归纳出量子计算机与经典计算机的计算能力的差别. 如果果真如此，什么使量子计算机比经典计算机更强大？哪类问题用量子计算机可以有效解决，与经典计算机可有效求解问题相比怎样？量子计算与量子信息中一件最令人激动的事情是，我们对这些问题的答案知之甚少！更好地理解这些问题是未来的巨大挑战.

到了量子计算的前沿后，再回到对量子计算与量子信息做出贡献的另一方面的思想：信息论. 1940 年，人们探索计算机科学的同时，通信在进行另一场革命. 1948 年 Claude Shannon 发表了现代信息和通信理论奠基性的引人瞩目的两篇论文.

Shannon 迈出的关键一步也许是在数学上定义了信息的概念. 数学的许多分支在基本定义的选择上具有相当的灵活性. 试着凭直观思考一下下面的问题：怎样从数学的角度定义信源？几种不同的答案都有着广泛的用途，但 Shannon 的定义看来明显地具有更丰富的内容，因为该定义能更好地理解，引发了深刻的结果并建立了层次丰富的理论. 这个理论准确反映了现实通信问题.

Shannon 所关注的是与信息通过信道传送有关的两个关键问题. 第一，通过信道传送信息需要哪些资源？例如，电话公司需要知道一个固定的电话电缆能可靠传送多少信息. 第二，在信道上可以保护信息避免噪声的干扰吗？

Shannon 通过证明信息论的基本定理回答了这些问题. 首先，Shannon 的无噪声信道编码定理，定量给出了用于存储从信源发出信息所需要的物理资源. Shannon 的第二个基本定理，带噪声信道编码定理，定量给出了有噪声的信道能可靠传送信息的量. 为在有噪声的情况下传送信息，Shannon 证明纠错码可用来保护要发送的信息，带噪声信道编码定理给出了纠错码提供保护的一个上限，不幸的是，Shannon 定理并没有给出实际能够达到这个极限的一组纠错码. 从 Shannon 的论文发表到现在，研究人员一直在不断推出更好类型的纠错码试图逼近 Shannon 定理设定的极限. 复杂的纠错码理论为使用者提供了多种选择. 这些码用途广泛，如应用在光盘播放器、计算机调制解调器、卫星通信系统等.

量子信息论有类似的发展过程. 1995 年，Ben Schumacher 证明了与 Shannon 无噪声编码定理类似的结果，并定义了“量子比特”作为切实的物理资源，但还没有针对量子信息的对应于 Shannon 带噪声信道编码定理的结果. 与经典对应物相应，出现了已经提到的量子纠错码使量子计算机在出现噪声的情形下能有效计算，也允许在带噪声的量子信道上进行可靠通信.

事实上，已证明在研究和理解量子纠错码上，纠错码的经典思想起着极其重要

的作用. 1996 年，两个独立的研究小组，Robert Calderbank、Peter Shor 和 Andrew Steane，发现了用他们缩写名字命名的重要的 CSS 类量子码，这项工作被包含在由 Robert Calderbank、Eric Rains、Peter Shor、Neil Sloane 和 Daniel Gottesman 独立发现的镇定码(stabilizer code)中. 由于建立在经典线性码的基本思想基础上，这些发现者大大加快了对量子纠错码及其在量子计算与量子信息中的应用的理解.

研究量子纠错码理论的目的是保护量子状态不受噪声干扰. 在量子信道上传送普通的经典信息会怎样？能够做到多么有效？这方面有几项惊人的发现. 1992 年 Charles Bennett 和 Stephen Wiesner 解释了如何只传送一比特量子比特，从发送方到接收方就达到传送两比特经典信息的目的. 这个结果称为超密编码(superdense coding).

更有趣的结果在分布式量子计算方面. 设想你有两台联网的计算机来解决一个特定问题，为求解问题需要多少通信量？最近的结果显示为求解某些问题时，量子计算机需要比联网经典计算机用指数性更少的通信量！不幸的是，这些问题在实际中不是特别重要，而且受到一些技术上的限制. 对量子计算与量子信息将来的一个主要挑战是，寻找现实中重要，而且分布式量子计算求解相对经典计算有实质优越性的问题.

让我们回到正规的信息论. 信息论始于对单个信道的研究. 实际应用中我们通常不止遇到一个信道，而是许多信道构成的网络. 网络化信息论的主题是研究信道网络的信息承载性质，这已成为一个内容丰富而复杂的课题.

与之对照，网络化量子信息论的研究还非常初步，即使是对量子信道网络的信息承载能力我们也是几乎一无所知. 过去几年里得出了一些相当引人瞩目的基本结果，但还没有针对量子信道的统一的网络化量子信息理论. 网络化量子信息论的一个例子就足以让人相信这样一套原理的重要性. 设想我们试图通过一个带噪声的量子信道，从 Alice 向 Bob 传送量子信息，如果信道的量子信息容量为 0，就不可能从 Alice 向 Bob 可靠地传送任何信息. 再设想我们有同步操作的该信道的两个拷贝，很显然(也可以严格检验)这样的信道传送量子信息的容量仍然为 0. 但是，如果我们将其中一个信道反向，如图 1.1 所示，某种情况下，我们能够获得从 Alice 到 Bob 的非 0 信息传送容量！这种违反直观的性质说明量子信息的奇异性. 更好地理解量子信道网络的信息承载能力是量子计算与量子信息的一个主要的未解决的问题.

让我们最后一次转换领域，来看古老的密码术中的科学和技巧. 广义而言，密码术是一个涉及互相不一定信任的两方或多方的通信或计算问题，最熟知的密码术问题就是保密通信，假设两个方面希望通信秘密进行. 例如，你想把信用卡号码告诉商家来买东西，但不希望任何有恶意的第三方截取你的信用卡号码. 实际过程是采用密码协议. 本书后面会详细描述密码协议的工作过程. 现在弄清一些简单的

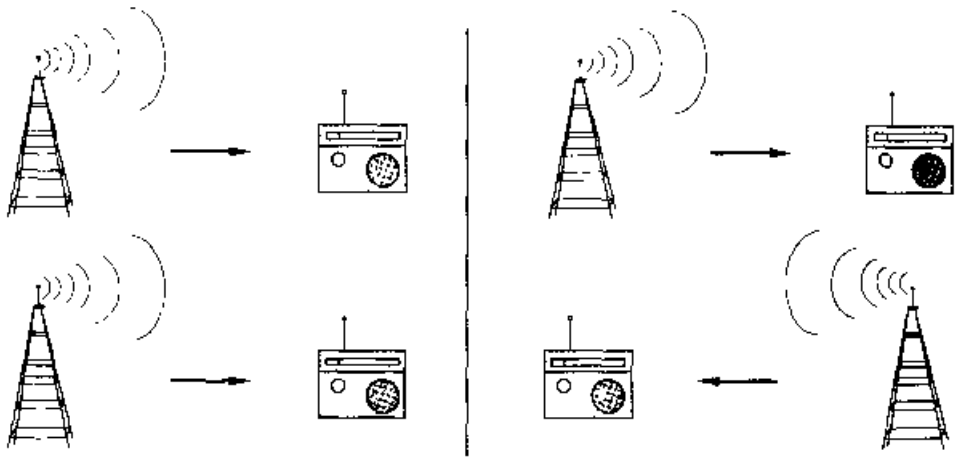


图 1.1　从经典角度看，两个噪声很大的零容量信道并排运转，联合的信道发送信息的容量为零．若一个信道反向，不奇怪，发送信息的容量仍为零．而从量子力学角度上，掉转一个零容量信道真的可以让我们发送信息！

区别就可以了．最大的区别是私钥密码系统(private key cryptosystem)和公钥密码系统(public key cryptosystem)．

私钥密码系统工作原理是通信双方 Alice 和 Bob 共享一个只有他们知道的私钥，密钥的准确形式在这里并不重要——不妨认为是 0 和 1 的串，要点是 Alice 用这个密钥将希望传送给 Bob 的信息进行加密．Alice 将加密信息发给 Bob，Bob 要恢复原始信息．Alice 加密消息的具体方式依赖于私钥，因此为了恢复原始消息，Bob 需要知道私钥，以便取消 Alice 施加的变换．

不幸的是，私钥密码系统在许多情况下存在严重的问题，最基本的问题是如何分配密钥？在许多意义上，密钥的分配和原始的保密通信问题难度相同——恶意的第三方可能在密钥分配时监听，然后用截获的密钥来解密传送的某些信息．

量子计算与量子信息最早的发现之一是量子力学可以用于密钥分配，使 Alice 和 Bob 的秘密不会受威胁．这个过程称为量子密码或量子密钥分配，基本思想是利用观测一般会干扰被观测系统的量子力学原理．于是，当 Alice 和 Bob 要传送密钥的时候，若有人监听，监听者就因对 Alice 和 Bob 用来进行密钥确定的信道带来干扰而被发现．Alice 和 Bob 可以丢弃有监听者出现时建立的密钥位，并重新确定密钥．20 世纪 60 年代后期 StephenWiesner 首次提出量子密码的概念，但不幸的是没有被发表．1984 年，Charles Bennett 和 Gills Brassard 在 Wiesner 早期工作的基础上，提出了利用量子力学在 Alice 和 Bob 之间分配密钥而不可能被威胁的协议．从那时起，出现了无数的量子密码协议，并有了实验原型．在写本书时，实验原型已接近适用于有限规模的实际应用的阶段．

密码系统的第二个主要类型是公钥密码系统．公钥密码系统不依赖预先共享一个密钥的 Alice 和 Bob．相反，Bob 只是公布一个“公钥”，让所有人都可以得到，

Alice 用这个密钥把送给 Bob 的消息加密. 有趣的是,第三方不可能用 Bob 的公钥解密! 严格讲,我们不能说不可能,而应说加密变换取得非常巧妙,以致仅根据公钥来逆向(invert)解密极其困难(虽然不是完全不可能). 为了使逆向过程简单,Bob 有一个与公钥配对的私钥,用这两个密钥 Bob 可以很容易地进行解密. 这个私钥只有 Bob 知道,故在别人不太可能具有只用公钥就能解密的前提下,Bob 可以相信,只有他能阅读 Alice 传来的内容. 公钥密码系统通过让 Alice 和 Bob 不需要在通信之前共享私钥来解决密钥分配问题.

值得注意的是,20 世纪 70 年代中期,在 Whitefield Diffie、Martin Hellman 和 Ralph Merkle 等人分别独立对公钥密码系统领域提出变革以前,公钥系统并没有得到广泛的使用. 稍后,Ronald Rivest、Adi Shamir 和 Leonard Adleman 研制出 RSA 密码系统,这是直到本书写作时,最广泛被采用的公钥密码系统. RSA 被认为在安全性和实用性之间取得了微妙的平衡. 1997 年人们得知这些思想——公钥密码系统、Diffie-Hellman 密码系统和 RSA 密码系统——实际上是 20 世纪 60 年代末 70 年代初英国情报机构 GCHQ 的研究人员发明的.

公钥密码系统的安全性的关键在于,仅利用公钥进行解密是困难的. 例如,对 RSA 来说,逆向解密过程是一个与分解因数密切相关的问题,对 RSA 的安全性的假设建立在用经典计算机分解因数是困难的这个信念之上. 然而,Shor 的在量子计算机上分解因数的快速算法可以用于破解 RSA! 类似地,如果知道一个解离散对数问题的快速算法——比如 Shor 的针对离散对数问题的量子算法,有些其他公钥密码系统就会被破解. 量子计算机在攻破密码系统密码上的这项应用,引发了对量子计算与量子信息的研究的很大兴趣.

我们一直在回顾量子计算与量子信息研究的发展历史. 当然随着该领域的发展和成熟,已产生它自己的子研究领域,它们的历史基本上包含在量子计算和量子信息的历史当中.

最引人瞩目的或许是对量子纠缠现象(quantum entanglement)的研究. 纠缠现象是量子力学独特的资源,在量子计算与量子信息的大多数有意义的应用上起着关键作用,相当于经典世界青铜器时代中铁的地位. 近年来,人们为更深入理解纠缠现象付出巨大的努力. 纠缠现象已被视为一种基本的自然资源,其重要性可以和能量、信息、熵以及任何其他基本资源相比. 尽管还没有纠缠现象的完整理论,但在理解这一量子力学奇特性质方面已取得一些进展. 许多研究者期待对纠缠现象性质的进一步研究会带来推动量子计算与量子信息新应用的见解.

1.1.2 未来发展方向

我们已回顾了量子计算与量子信息研究的历史和现状. 未来会怎样? 量子计算与量子信息会带给科学、技术和人类什么? 量子计算与量子信息给产生它的计

算机科学、信息论和物理学诸领域带来什么好处？量子计算与量子信息有哪些关键问题没有解决？在展开细节之前，我们对这些全局性问题作简要的评注.

量子计算与量子信息教我们以物理的方式思考计算，我们发现这种做法能为信息处理和通信带来许多新的令人鼓舞的动力，计算机科学家和信息论专家有了一个值得探索的新的内容丰富的模型. 的确，从广义上说，我们学到的任何物理理论，不仅仅是量子力学，都可以作为信息处理和通信的基础. 这种探索的结果，也许有一天会导致发明远超过当今计算和通信系统能力的信息处理装置，并带来对整个社会正面和负面的影响.

量子计算与量子信息必然向物理学家提出很多挑战，但长远看它为物理学本身做出何种贡献却有些微妙. 我们相信就像我们学会用物理的方式思考计算一样，我们也能够学会以计算的方式思考物理学. 虽然物理学主要集中于弄清基本物体和简单系统，自然界的很多有趣方面只会出现在事物变大和变复杂的情形中. 化学和工程在一定程度上处理这样的复杂性，但绝大多数情况用的是特定的手法. 量子计算与量子信息传达的一个信息是，新的工具可以用来跨越微小和相对复杂的事物之间鸿沟：计算和算法为构造和理解这类系统提供了系统化的手段. 应用这些领域的思想已经开始为物理学带来新见解，我们希望这个方向未来将发展成一个理解物理学所有分支的富有成果的方向.

本节考察了量子计算与量子信息背后的一些关键思想和研究动机，本章的其他小节将对这些思想和动机作更具技术性但仍容易理解的介绍，以期带读者鸟瞰这个领域的现状.

1.2　量子比特

比特(bit)是经典计算和经典信息的基本概念. 量子计算与量子信息建立在类似的概念量子比特(quantum bit 或 qubit)的基础上. 本节我们比照经典比特介绍单量子比特和多量子比特的属性.

何谓量子比特？我们将量子比特描述为具有特定属性的数学对象. 也许你会说："等等，我想量子比特是物理对象."像比特一样，量子比特诚然是用实际物理系统来实现的，并且在 1.5 节和第 7 章，我们还会详尽指出，抽象数学观点和实际系统之间是如何联系的. 但是，本书的大部分内容中，量子比特的确是被当作数学对象来对待. 把量子比特当作抽象对象的美妙之处在于，这给了我们建立一个不依赖特定系统实现的一般量子计算与量子信息理论的自由.

那么什么是量子比特呢？就像经典比特有一个状态——或 0 或 1——量子比特也有一个状态，量子比特的两个可能状态是 $|0\rangle$ 和 $|1\rangle$. 像你会猜到的它们分别对应经典比特的状态 0 和 1. 记号"$|\rangle$"称为 Dirac 记号，我们会常碰到，它在量子力学

中表示状态. 比特和量子比特的区别在于，量子比特的状态可以落在$|0\rangle$和$|1\rangle$之外，量子比特可以是状态的线性组合，常称为叠加态(superpostition). 例

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.1}$$

其中α和β是复数，尽管许多时候把它们当作实数也不会有太大问题. 换句话说，量子比特的状态是二维复向量空间中的向量. 特殊的$|0\rangle$和$|1\rangle$状态称为计算基态(computational basis state)，是构成这个向量空间的一组正交基.

我们可以通过检查一个比特，来确定它是处在0状态还是1状态. 例如，计算机每次从内存取内容时，都要做这件事. 但值得特别注意的是，我们不能通过检查量子比特来确定它的量子状态，也就是得到α和β的值. 相反，量子力学告诉我们，只能得到关于量子状态的有限信息. 在测量量子比特时，我们得到0的概率为$|\alpha|^2$，得到1的概率为$|\beta|^2$. 当然$|\alpha|^2+|\beta|^2=1$，因为概率总和一定是1. 从几何意义上看，是要求量子比特的状态归一化到长度1. 因此，一般而言，量子比特的状态是二维复向量空间中的单位向量.

量子比特的不可观测状态和我们能够进行观测的差别在量子计算与量子信息研究中处于中心位置. 在我们建立的现实世界的大多数抽象模型当中，抽象和真实模型之间存在直接的对应关系，就像建筑师蓝图和最终的建筑物对应那样. 没有这种直接的对应关系，使得从直观上解释量子系统的行为变得困难. 不过好在存在一种间接对应关系，因为量子比特的状态可以被处理和变换，按照状态的不同属性，产生可区分的测量结果，因此，这些量子态具有真实的、实验可验证的效应. 这些效应对量子计算与量子信息的功能是非常重要的.

量子比特处于叠加态的可能性与我们理解身边物理世界的常识相矛盾. 经典比特像一枚硬币：要么正面要么反面向上. 不均匀的硬币或许靠边缘的平衡，处于某个中间状态，但在理想情况下不被考虑. 与之相反，量子比特可以处在$|0\rangle$和$|1\rangle$之间的连续状态中——直到它被观测. 这里再次提醒一下，当量子比特被观测时，只能得到非"0"即"1"的测量结果——每个结果有一定的概率. 例如，量子比特可以处子状态

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{1.2}$$

经过测量，有50%($|1/\sqrt{2}|^2$)的可能得到0，50%的可能得到1. 我们经常会用到这个状态. 这个状态有时记作$|+\rangle$.

尽管这么奇特，量子比特的存在确实是真实的，它们的存在和行为被大量实验(见1.5节和第7章的讨论)所证实，并且有许多不同的物理系统，可以用来实现量子比特. 为具体起见，列出某些实现的方法也许有帮助：比如光子的两种不同的极化(polarization)；又如在均匀电磁场中核自旋的取向；再如图1.2所示的围绕单个原子的电子的两种状态. 在原子模型中，电子可能处在基态，也可能处在激发态，分

别用$|0\rangle$和$|1\rangle$表示. 用光照射该原子，如果能量合适，并且时间足够长，可以使电子在$|0\rangle$和$|1\rangle$状态之间移动. 但更有趣的现象是，缩短光照时间，并始处在$|0\rangle$的电子可以移到从 $0\rangle$到$|1\rangle$的中途，即进入$|+\rangle$状态.

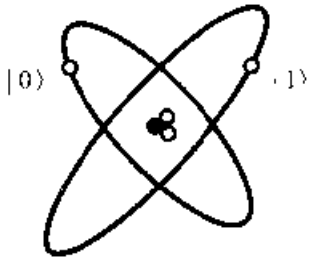


图 1.2　用原子中电子的两个能级表示的量子比特.

很自然，叠加态的可能含义或解释和量子系统观测的内在概率性质引起了很大关注，但本书基本上不考虑这些内容. 我们的目的是给出具有预见性的数学和概念上的图像.

量子比特的一个有用的图像是如下的几何表示. 因为 $\alpha|^2+|\beta|^2=1$，等式(1.1)可改写为

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right) \tag{1.3}$$

其中 θ,φ,γ 都是实数. 第 2 章会看到括号外的 $e^{i\gamma}$ 可以略去，因为它不具有任何可观测的效应，因此我们可以写出有效的形式为

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{1.4}$$

数 θ 和 φ 定义了三维单位球面上的一个点，如图 1.3 所示. 这个球面常称为 Bloch 球面. 它是使单个量子比特状态可视化的有效办法，也是量子计算与量子信息思想的极好试验台. 本章后面要讲的单个量子比特的许多操作都是在 Bloch 球面的画面中描绘的. 不过，切记这种直观的想象是有局限的，因为尚不知道如何将 Bloch 球面简单地推广到多量子比特情形.

一个量子比特包含多少信息？看似荒谬，单位球面上有无穷多点，因而原则上可以把 Shakespeare 全部著作存在 θ 的无限二进制展开当中. 然而，鉴于量子比特被观测的行为，这个结论实际上是一种误导. 回想一下，量子比特的观测结果只会得到 0 或 1，进而，测量改变量子比特的状态，从$|0\rangle$和$|1\rangle$的叠加态坍缩(collapsing)到与测量结果相容的特定状态. 例如，如果$|+\rangle$的测量结果是 0，那么量子比特的测后状态就是$|0\rangle$. 为什么会发生这类坍缩？没有人知道. 如第 2 章所讨论的，这种行为是量子力学的基本原理之一. 与我们的论题相关的是量子比特的一次测量只得到有关量子比特的状态的一比特信息，这就解决了上述的佯谬. 事实上只

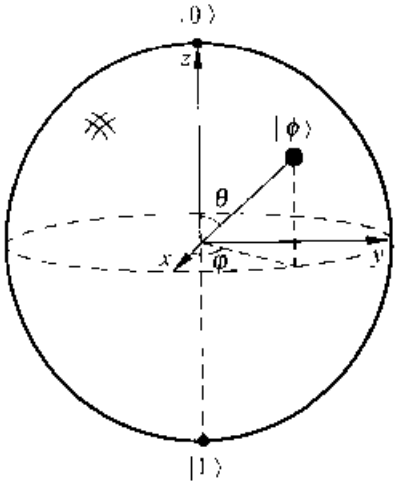


图 1.3　量子比特的 Bloch 球面表示.

有测量无穷多完全相同的量子比特才能确定等式(1.1)中的 α 和 β.

但更有趣的问题是:如果不进行测量,一个量子比特代表多少信息?这是个需要小心的问题.因为如果不能测量,如何量化信息呢?不管怎么说,这里包含重要的概念,因为量子比特组成的封闭量子系统在自然界中的演化,不进行任何测量,该系统显然的确保留着描述状态的连续变量的轨迹,例如 α 和 β.一定意义上说,在量子比特的状态里,自然界隐藏了大量隐含信息.更有趣的是,我们很快会看到这些额外信息随量子比特个数的增加而指数上升.弄清隐含的量子信息是本书许多部分试图要解决的问题,是使量子力学成为信息处理强大工具的核心.

1.2.1 多量子比特

Hilbert 空间很大.

——*Carlton Caves*

假设有两个量子比特.对两个经典比特而言,共有四种可能状态:00,01,10 和 11.相应地,一个双量子比特有四个基态,记作$|00\rangle$,$|01\rangle$,$|10\rangle$,$|11\rangle$.一对量子比特也可以处于这四个基态的叠加,因而双量子比特的量子状态包含相应基态的复系数,有时称为幅度(概率幅 amplitude).这样描述双量子比特的状态向量为

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{1.5}$$

类似于单量子比特情形,测量结果 x(=00,01,10 或 11)出现的概率是$|\alpha_x|^2$,测量后,量子比特处于$|x\rangle$状态.概率之和为 1 的归一化条件可表示为

$$\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1$$

其中$\{0,1\}^2$ 意味着长度为 2,每个字母从 0 和 1 中任取的符号串的集合.对于一个双量子比特系统,可以只测量其中一个量子比特,如第一个.你可能会猜到结果:单独测量第一个量子比特,得到 0 的概率为$|\alpha_{00}|^2+|\alpha_{01}|^2$,而测量后的状态为

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2+|\alpha_{01}|^2}} \tag{1.6}$$

注意,测后状态被因子$\sqrt{|\alpha_{00}|^2+|\alpha_{01}|^2}$重新归一化后,仍满足归一化条件,正像我们对一个标准的量子比特状态所期待的那样.

Bell 态或 EPR 对是一个重要的双量子态,

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{1.7}$$

这个不起眼的状态和量子计算与量子信息中许多惊人的发现有关.它是量子隐形传态和超密编码的关键要素,还是其他许多有趣量子状态的原型,这将在 1.3.7 小节和 2.3 节分别介绍.Bell 态的性质是当测量第一量子比特时,以 1/2 概率得到 0,

进入测后状态$|\varphi'\rangle=|00\rangle$；以 1/2 概率得到 1，进入测后状态$|\varphi'\rangle=|11\rangle$. 结果是，对第二量子比特的测量总得到与第一量子比特一样的结果，也就是说，测量结果是相关的. 其实，可以对 Bell 态进行其他方式的测量，先在第一或第二量子比特上施加某种操作，而第一、第二比特之间测量结果上的有趣相关性仍然存在. 自从 Einstein、Podolsky 和 Rosen 的著名论文首次指出诸如 Bell 态的奇怪性质，这类相关性成为大量研究的主题. EPR 的见解被 John Bell 继承并发扬光大，他证明了一个惊人的结论：Bell 态的测量相关性比经典系统可能存在的相关性都要强. 这些结论首次宣告量子力学具有超越经典世界的信息处理能力，它们将在 2.6 节介绍.

更一般地，可以考虑 n 量子比特系统. 这个系统的基态形如$|x_1x_2\cdots x_n\rangle$，并且量子状态由 2^n 个幅度所确定. $n=500$ 时，这数就已超过整个宇宙原子的估算总数！在任何传统计算机上存储所有这些复数都是不可想象的. Hilbert 空间的确是个巨大的空间. 然而可以肯定，即使对包含几百个原子的系统，大自然也需要处理如此大量的数据，看起来为计算系统的演化，大自然需要在手边放 2^{500} 张看不见的草稿纸. 我们非常希望能够利用如此巨大的计算潜力，但怎样把量子力学过程看作计算呢？

1.3　量子计算

量子状态的变化可以用量子计算的语言来描述. 类似于经典计算机是由包含连线和逻辑门的线路建造的，量子计算机是由包含连线和基本量子门排列起来、形成的处理量子信息的量子线路建造的. 本节介绍简单的量子门，并举几个线路的例子来说明它们的应用，其中包括一个量子隐形传态的线路.

1.3.1　单量子比特门

经典计算机线路由连线和逻辑门构成. 连线用于在线路间传送信息，而逻辑门负责处理信息，把信息从一种形式转换为另一种. 例如，考虑一个经典单比特逻辑门. 惟一的不平凡成员是非门，非门的操作由真值表定义，其中 0→1，1→0，即将 0，1 状态交换.

可以类似地定义量子比特的量子非门(NOT gate)吗？设想我们有某个过程来把状态$|0\rangle$和$|1\rangle$交换，那这个过程显然是量子非门的好的候选对象. 但如果没有关于量子门性质的进一步知识，在$|0\rangle$和$|1\rangle$状态上定义门的作用无法确定$|0\rangle$和$|1\rangle$之间的叠加态会发生什么. 实际上，量子非门的作用是线性的，即把状态

$$\alpha|0\rangle+\beta|1\rangle \tag{1.8}$$

变到$|0\rangle$和$|1\rangle$状态角色互换的新状态，

$$\alpha|1\rangle+\beta|0\rangle \tag{1.9}$$

量子非门的作用是线性而不是非线性的原因很有趣，且答案并不显然. 事实上，这一线性行为是量子力学的一般属性，也非常符合经验，更甚之，非线性行为会导致许多佯谬，如时间旅行、超光速通信、违反热力学第二定律等. 本书后面的章节还会深入阐述这一点，现在暂且接受下来.

基于线性性质，量子非门可以方便地用矩阵形式表示. 定义一个 X 矩阵来表示非门如下：

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{1.10}$$

（用记号 X 表示非门是由于历史的原因）若把量子态 $\alpha|0\rangle+\beta|1\rangle$ 写成向量形式

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{1.11}$$

其中上面一项对应 $|0\rangle$ 的幅度，而下面一项对应 $|1\rangle$ 的幅度，那么量子非门的输出就是

$$X\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \tag{1.12}$$

注意非门的作用是把 $|0\rangle$ 状态变成矩阵 X 的第一列所对应的状态，把 $|1\rangle$ 状态变成矩阵 X 第二列所对应的状态.

因此单量子比特的量子门可以由 2×2 矩阵给出. 对用作量子门的矩阵有什么限制呢？有限制. 回忆归一化条件，要求量子状态 $\alpha|0\rangle+\beta|1\rangle$ 满足 $|\alpha|^2+|\beta|^2=1$，这对于量子门作用后得到状态 $|\psi'\rangle=\alpha'|0\rangle+\beta'|1\rangle$ 也是适用的. 实际上表示单量子比特门的相应矩阵 U 要满足的条件是酉性（unitary），即 $U^\dagger U=I$，其中 $U^\dagger$ 是 U 的共轭转置（由取 U 的转置和复共轭得到），I 是 2×2 的单位阵. 例如，对非门很容易验证 $X^\dagger X=I$.

令人惊奇的是，酉性限制是对量子门的惟一限制，每个酉矩阵都定义一个有效的量子门. 一个有趣的推论是：和只有一种不平凡单比特门——非门——的经典情形不同，有很多的不平凡单比特量子门. 我们在后面会用到的两个是 Z 门

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{1.13}$$

它保持 $|0\rangle$ 不变，而翻转 $|1\rangle$ 的符号变成 $-|1\rangle$，和 Hadamard 门

$$H \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{1.14}$$

这个门有时被视为非门的平方根. 它把 $|0\rangle$ 变到 $|0\rangle$ 至 $|1\rangle$ 的中间状态 $(|0\rangle+|1\rangle)/\sqrt{2}$，而把 $|1\rangle$ 变到同样是 $|0\rangle$ 至 $|1\rangle$ 的中间状态 $(|0\rangle-|1\rangle)/\sqrt{2}$. 不过需要注意，$H^2$ 不是非门，经过简单计算可得出 $H^2=I$，因此两次应用 H 到一个状态等于什么都没做.

Hadamard 门是最有用的量子门之一，有必要在 Bloch 球面上把它的作用显示出来. 在这个图画中，单量子比特门对应于球面上的旋转和反射. Hardamard 操作如图 1.4 所示，恰好是先绕 y 轴旋转 90°，再绕 x 轴旋转 180°. 图 1.5 给出了一些重要的单量子比特门，并与经典情形对照.

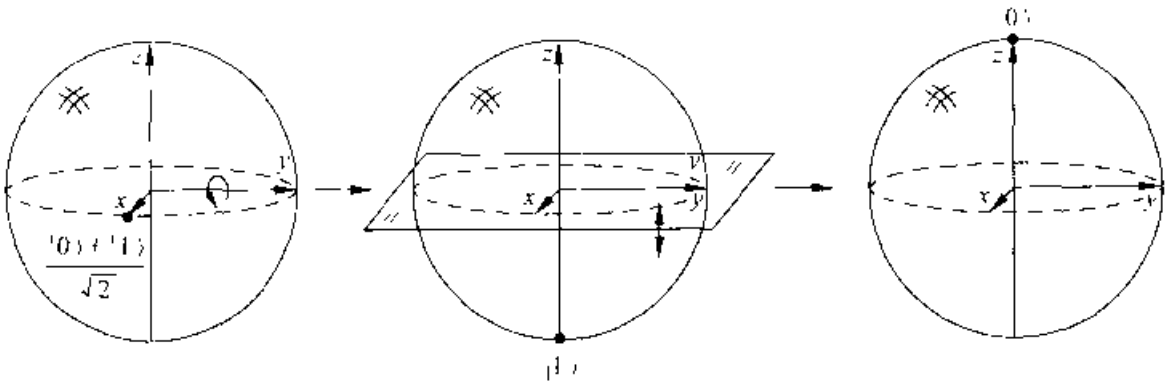


图 1.4　Hadamard 门在 Bloch 球面上的显示，作用于输入状态 $(|0\rangle+|1\rangle)/\sqrt{2}$ 上.

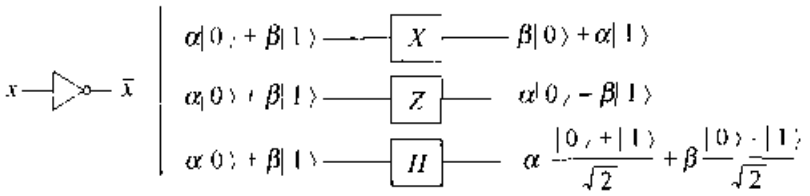


图 1.5　单比特(左)和量子比特(右)逻辑门. 其中 $\bar{x}$ 是 x 的逻辑非.

因为存在无穷多个 2×2 酉矩阵，所以量子比特门的种类也是无限的. 不过，整个集合的属性可以从小得多的集合得到. 例如，如盒子 1.1 所述，一个任意单量子比特酉门都可以分解成一个旋转

$$\begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix} \tag{1.15}$$

和一个可理解为绕 z 轴旋转的门(将在后面介绍)，

$$\begin{bmatrix} e^{i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix} \tag{1.16}$$

再加上一个(全局)相移 ——形如 $e^{i\alpha}$ 的常系数的乘积. 这些门还可以进一步分解，我们不需要考虑任意的 α，β 和 γ，但可用 α，β 和 γ 的某些特殊的固定值任意逼近这些门. 在这种意义下，任意的单量子比特门可以基于量子门的一个有限集合来构造. 更一般地，任意数量的量子比特上的任何量子计算，可以从称为对量子计算具有通用性的(universal)一组有限个门产生出来. 为获得这样的通用集合，我们首先

要引入涉及多量子比特的量子门.

盒子 1.1 单量子比特操作的分解

在 4.2 节我们证明任意的 2×2 酉矩阵可分解为

$$U = e^{i\alpha}\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}\begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}\begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix} \tag{1.17}$$

其中 α,β,γ 和 δ 是实数. 注意,第二个矩阵是普通的旋转,第一和最后一个矩阵可以理解为在不同平面内的旋转. 该分解可对任意单个量子比特逻辑门的操作进行精确描述.

1.3.2 多量子比特门

现在把单量子比特推广到多量子比特. 图 1.6 画了五个重要的经典多比特门:与(AND)、或(OR)、异或(XOR)(互斥或)、与非(NAND)和或非(NOR)门. 一个重要的理论结果是,比特上的任意函数可以仅用与非门的复合来计算,因而与非门称为一个通用门. 与之对照,异或门即使加上非门都不具有通用性. 弄清这一点的一个办法是,注意应用异或门不改变比特奇偶性(parity)的事实. 作为推论,任何只包含非和异或门的电路,如果输入 x 和 y 具有相同的奇偶性,输出也将具有同样的奇偶性,从而排除了电路的通用性.

多量子比特量子逻辑门的原型是受控非(controlled-NOT 或 CNOT)门. 这个门有两个输入量子比特,分别是控制量子比特和目标量子比特. 受控非门的线路如图 1.6 右上方所示,上面的线表示控制量子比特,下面的线表示目标量子比特.

该门的作用描述如下. 若控制量子比特置为 0,则目标量子比特将保持不变. 若控制量子比特置为 1,目标量子比特将翻转. 用方程形式表示有

$$|00\rangle \to |00\rangle,\ |01\rangle \to |01\rangle,\ |10\rangle \to |11\rangle,\ |11\rangle \to |10\rangle \tag{1.18}$$

另一描述受控非门的方法是将其视为经典异或门的推广,因为该门的作用可总结为 $|A,B\rangle \to |A,B\oplus A\rangle$,其中$\oplus$是模 2 加法,而这正是异或运算所做的. 也就是说,控制量子比特和目标量子比特作异或运算,并将结果存在目标量子比特中.

受控非门还有一种矩阵表示方法,如图 1.6 的右下方所示. 容易验证 U_{CN} 的第一列表示对 $|00\rangle$ 的变换,对其他基态 $|01\rangle$,$|10\rangle$ 和 $|11\rangle$ 也类似. 像对单量子比特情形一样,保持概率特性的要求体现为 U_{CN} 是一酉矩阵,即 $U_{CN}^{\dagger}U_{CN}=I$.

我们提到,受控非门可视为一类推广的异或门. 其他经典门,如与非门和通常的异或门,能够在某种意义上以类似于量子非门表示经典非门的方式被视为酉门

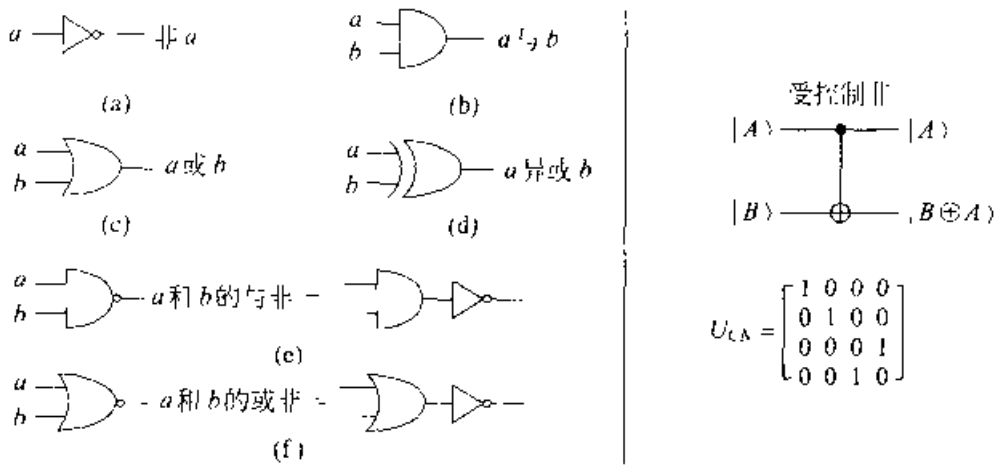


图 1.6　左边是一些标准的多比特门，而右边是多量子比特门的原型，即受控非门. 给出受控非门的矩阵表示，U_{CN}，分别依次针对状态 $|00\rangle$、$|01\rangle$、$|10\rangle$ 和 $|11\rangle$ 的幅度.

吗？实际上这不可能，原因是异或和与非门具有本质的不可逆性. 例如，已知异或门的输出 $A\oplus B$，并不能确定输入 A 和 B. 异或门的不可逆性带来信息的损失. 另一方面，酉量子门却总是可逆的，因为酉矩阵的逆还是酉矩阵，故一个量子门的作用总可以通过另一量子门翻转过来. 明白如何在这种可逆和不可逆意义下做经典逻辑运算，是懂得如何利用量子力学的功能来进行计算的关键步骤，我们将在 1.4.1 小节解释做可逆运算的基本思想.

当然，除受控非门外还有许多其他重要的量子门. 不过，出于以下著名的通用性结果：任意的多量子比特门都可由受控非门和单量子比特门复合而成，某种意义上说，受控非门和单量子比特门是所有其他门的原型. 该结论是与非门通用性的量子版本，其证明将在 4.5 节给出.

1.3.3　除计算基以外的基的测量

我们提到过对处于状态 $\alpha|0\rangle+\beta|1\rangle$ 的单量子比特进行测量，得到 0 和 1 结果的概率分别是 $|\alpha|^2$ 和 $|\beta|^2$，并进入 $|0\rangle$ 或 $|1\rangle$ 量子状态. 事实上，尽管从一次测量不足以恢复出 α 和 β，一定意义下，量子力学还是允许更为灵活的测量.

注意对量子比特而言，状态 $|0\rangle$ 和 $|1\rangle$ 只是基态的许多选择中的一种，另一可能的选择是 $|+\rangle\equiv(|0\rangle+|1\rangle)/\sqrt{2}$ 和 $|-\rangle\equiv(|0\rangle-|1\rangle)/\sqrt{2}$. 任意的状态 $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ 可以相对于状态 $|+\rangle$ 和 $|-\rangle$ 重新表示为

$$\begin{aligned}|\psi\rangle=\alpha|0\rangle+\beta|1\rangle&=\alpha\frac{|+\rangle+|-\rangle}{\sqrt{2}}+\beta\frac{|+\rangle-|-\rangle}{\sqrt{2}}\\&=\frac{\alpha+\beta}{\sqrt{2}}|+\rangle+\frac{\alpha-\beta}{\sqrt{2}}|-\rangle\end{aligned}\tag{1.19}$$

把$|+\rangle$和$|-\rangle$视为基底，并参照这组新基进行测量，确实是可能的. 很自然地，相对$|+\rangle$，$|-\rangle$基的测量以$|\alpha+\beta|^2/2$的概率导致“+”的结果，以$|\alpha-\beta|^2/2$的概率导致“−”的结果，测后状态分别为$|+\rangle$和$|-\rangle$.

更一般地，给定量子比特的任意基态$|a\rangle$和$|b\rangle$，可以把任意状态表为线性组合$\alpha|a\rangle+\beta|b\rangle$. 进而，若$|a\rangle$和$|b\rangle$状态是正交的，则可以相对基$|a\rangle$，$|b\rangle$进行测量，并以$|\alpha|^2$概率导致$a$，以$|\beta|^2$概率导致$b$. 正交性约束是保证概率条件$|\alpha|^2+|\beta|^2=1$所要求的. 同样道理，原则上多量子比特系统相对任意正交基的测量都是可能的，不过，仅是原则上可能，并不意味着进行这样的测量就是容易的. 我们后面还会回到如何进行相对任意基的有效测量问题.

有许多理由要求使用这种推广形式的量子测量，但最好的理由是：这种形式让我们能够解释观察到的实验结果，正如在 1.5.1 小节，我们对 Stern-Gerlach 实验的讨论一样. 下一章 2.2.3 小节将给出一个更复杂、但更方便(但本质上等价)的描述量子测量的框架.

1.3.4 量子线路

我们已经遇到一些简单的量子线路，现在来更仔细地考察量子线路的元件. 图 1.7 给出包含三个量子门的量子线路，线路的读法是从左到右. 每条线表示量子线路中的连线，连线不一定对应物理上的接线，而可能是对应一段时间或一个从空间的一处移动到另一处的物理粒子，如光子. 为方便起见，假定线路的输入状态是基态，通常是全$|0\rangle$组成的状态. 这个约定在量子计算与量子信息的文献中常常被打破，不过这种情况最好向读者声明.

图 1.7 中的线路完成一件简单而有用的任务——它对换两个量子比特的状态. 为明白该线路完成对换操作(swap operation)，需要注意这一连串门在计算基态$|a,b\rangle$上的一系列作用，

$$\begin{aligned} |a,b\rangle &\rightarrow |a,a\oplus b\rangle \\ &\rightarrow |a\oplus(a\oplus b),a\oplus b\rangle = |b,a\oplus b\rangle \\ &\rightarrow |b,(a\oplus b)\oplus b\rangle = |b,a\rangle \end{aligned} \tag{1.20}$$

其中所有的加法都是模 2 的. 于是，这个线路的作用就是互换两个量子比特的状态.

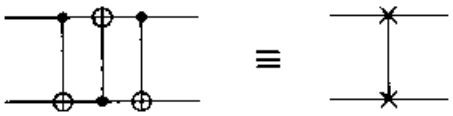


图 1.7 对换两个量子比特的线路和这个常用线路的等价框图符号.

一些经典线路特有的概念在量子线路中通常不出现. 首先，量子线路不允许出现回路，即从线路的一部分到另一部分的反馈，也就是说量子线路是无环的(acyclic). 其次，经典线路允许连线汇合，即所谓扇入操作(FANIN)，导致单连线

包括所有输入位的按位或(bitwise OR). 显然这个操作是不可逆的,因而也是非酉的,因此在量子线路中我们不允许出现扇入. 最后,相反的操作,扇出(FANOUT),即产生一比特的多个拷贝在量子线路中也是不允许的. 事实上量子力学禁止量子比特的复制,扇出操作是不可能的. 在下节尝试设计复制量子比特的线路时,我们将看到这样的例子.

后面我们还会引入新的量子门. 现在为方便起见,介绍和量子线路有关的另一个约定,如图 1.8 所示. 设 U 是作用在 n 量子比特上的任意酉矩阵,于是 U 可视为那些量子比特上的量子门. 作为受控非门的自然推广,可定义受控 U 门. 这样的门具有单一的控制量子比特,用带黑点的线表示,和 n 个目标量子比特,用标上 U 的盒子表示. 如果控制量子比特置于 0,目标量子比特将不受影响;如果控制量子比特置于 1,则门 U 作用到目标量子比特上. 受控 U 门的原始模型是受控非门,这里的 $U=X$,如图 1.9 所示.

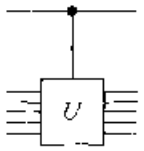


图 1.8　受控 U 门.

另一重要的操作是测量,用仪表符号来表示,如图 1.10 所示. 如前所述,这个操作把单量子比特的状态 $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ 变成概率意义下的经典比特 M(为与量子比特区分,画成双线),取 0 的概率为 $|\alpha|^2$,取 1 的概率为 $|\beta|^2$.

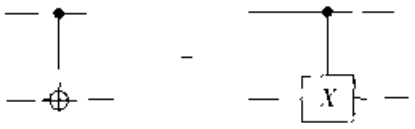


图 1.9　受控非门的两种表示.



图 1.10　表示测量的量子线路符号.

量子线路是所有量子过程的有用模型,包括但不限于计算、通信、量子噪声. 下面用几个简单例子说明这一点.

1.3.5　量子比特复制线路?

受控非门对说明量子信息的一个特有属性非常有用. 考虑复制经典比特的任务. 它可以用经典受控非门完成,如图 1.11 所示,将待复制的比特(处于未知状态 x)和初始化为 0 的中间缓存器比特输入到该门即可. 输出结果是两个比特,都处在相同的状态 x.

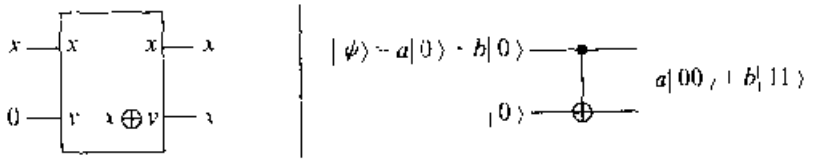


图 1.11　复制未知比特和量子比特的经典与量子线路.

设想我们要采用相同的办法，以受控非门来复制未知状态$|\psi\rangle=a|0\rangle+b|1\rangle$. 两个输入量子比特可写作

$$[a|0\rangle+b|1\rangle]|0\rangle=a|00\rangle+b|10\rangle \tag{1.21}$$

受控非门的作用是当第一量子比特为 1 时，把第二量子比特取反，结果就是$a|00\rangle+b|11\rangle$. 复制$|\psi\rangle$成功了吗？也即产生状态$|\psi\rangle|\psi\rangle$了吗？对于$|\psi\rangle=0$成$|\psi\rangle=1$的情形，该线路确实做到了，因为用量子线路来复制编码为$|0\rangle$和$|1\rangle$的经典信息是可能的. 然而，对一般状态$|\psi\rangle$

$$|\psi\rangle|\psi\rangle=a^2|00\rangle+ab|01\rangle+ab|10\rangle+b^2|11\rangle \tag{1.22}$$

与$a|00\rangle+b|11\rangle$比较，可以看到除非$ab=0$，复制线路不能复制输入的量子状态. 实际上，要制作未知量子状态的拷贝是不可能的. 这条量子比特不能被复制的性质，称为不可克隆(non-cloning)定理，是量子信息和经典信息的主要差别之一. 盒子 12.1 会更仔细讨论不可克隆定理，其证明非常简单，你可以去阅读这个证明.

基子量子比特以某种方式包含不能直接从测量得到的“隐含”信息的直观概念，还可以从另外的角度看图 1.11 线路的失败. 考虑测量$a|00\rangle+b|11\rangle$的一个量子比特会发生什么. 如前所述，我们以概率$|a|^2$和$|b|^2$得到 0 或 1，但一旦有一个量子比特被测量，另一个量子比特的状态就完全确定了，再也不会得到关于 a 和 b 的更多的信息了. 在这个意义上，原始量子比特$|\psi\rangle$承载的额外信息在第一次测量中就丢失了，且无法恢复. 但假如量子比特被复制了，那么另外一个量子比特的状态应该仍保留着部分的隐含信息. 因此，不可能建立拷贝.

1.3.6 例子：Bell 态

考虑一个稍复杂些的线路，在图 1.12 的线路中，一个 Hadamard 门后面连接一个受控非门，并按所给的表变换四个计算基态. 具体说来，设 Hadamard 门将输入$|00\rangle$变到$(|0\rangle+|1\rangle)|0\rangle/\sqrt{2}$，子是受控非门给出输出状态$(|00\rangle+|11\rangle)/\sqrt{2}$. 注意，进行方式是：首先 Hadamard 变换把上面的量子比特变为叠加态；然后该状态作为受控非门的控制输入，仅当控制为 1 时，目标量子比特被翻转. 输出状态

输入	输　出
$\|00\rangle$	$(\|00\rangle+\|11\rangle)/\sqrt{2}\equiv\|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle+\|10\rangle)/\sqrt{2}\equiv\|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle-\|11\rangle)/\sqrt{2}\equiv\|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle-\|10\rangle)/\sqrt{2}\equiv\|\beta_{11}\rangle$

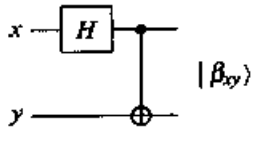


图 1.12 产生 Bell 态的量子线路以及输入输出量子“真值表”.

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{1.23}$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{1.24}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{1.25}$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{1.26}$$

称为 Bell 态，有时也称为 EPR 态或 EPR 对. 这是根据首次指出这些状态的奇特性质的学者 Bell 和 Einstein、Podolsky 与 Rosen 命名的. 状态的记号是 $|\beta_{00}\rangle$，$|\beta_{01}\rangle$，$|\beta_{10}\rangle$，$|\beta_{11}\rangle$. 可以用如下的公式记忆：

$$|\beta_{x,y}\rangle \equiv \frac{|0,y\rangle + (-1)^x |1,\bar{y}\rangle}{\sqrt{2}} \tag{1.27}$$

其中 $\bar{y}$ 是 y 的非.

1.3.7　例子：量子隐形传态

我们现在就用刚刚学到的技能来解释一个令人惊奇而非常有趣的现象——量子隐形传态. 量子隐形传态是在发送和接收方甚至没有量子通信信道连接的情况下，移动量子状态的一项技术.

下面是量子隐形传态的工作原理. Alice 和 Bob 很久以前相遇过，但现在住得很远，在一起时他们产生了一个 EPR 对，分开时每人带走 EPR 对中的一个量子比特，许多年后，Bob 躲起来. 设想 Alice 有一项使命，是要向 Bob 发送一个量子比特 $|\psi\rangle$，她不知道该量子比特的状态，而且只能给 Bob 发送经典信息. Alice 应该接受这项使命吗？

直观上看来，Alice 的情况很糟. 她不知道必须发给 Bob 的量子比特的状态 $|\psi\rangle$，而量子力学定律使她不能利用 $|\psi\rangle$ 仅有的一个拷贝去确定这个状态. 更糟糕的是，即便她知道状态 $|\psi\rangle$，描述它也需要无穷多的经典信息，因为 $|\psi\rangle$ 取值于一个连续空间. 如此看来，即使知道 $|\psi\rangle$，Alice 也要花无穷长时间向 Bob 描述这个状态. 情况看来对 Alice 不妙. 对 Alice 来说幸运的是，量子隐形传态提供了利用 EPR 对向 Bob 发送 $|\psi\rangle$ 的一条途经，仅仅比经典的通信多做一点点工作.

概括起来，解决步骤如下：Alice 让 $|\psi\rangle$ 和 EPR 对在她的那里的一半相互作用，并测量她拥有的两个量子比特，得到四个可能结果 00，01，10 和 11 中的一个；她把这个信息发给 Bob；根据 Alice 的经典消息，Bob 对他拥有的那一半 EPR 对进行四个操作中的一种. 令人吃惊的是，这样做他可以恢复原始的 $|\psi\rangle$.

图 1.13 的线路对量子隐形传态进行了更准确的描述. 要进行隐形传态的状态

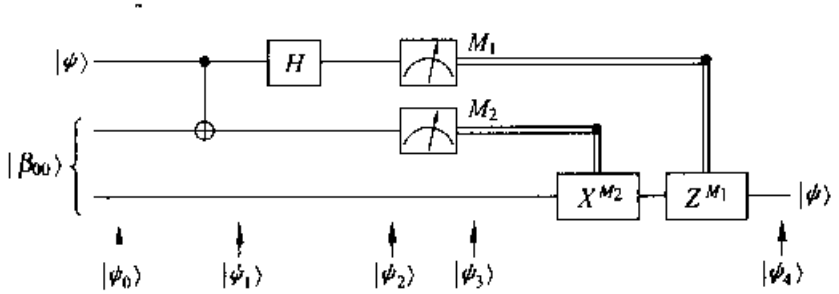


图 1.13 一个量子比特的隐形传态线路. 上方两根线表示 Alice 的系统,下方的线是 Bob 的系统. 仪表代表测量,双线表示它们承载经典比特(回忆单线表示量子比特).

是$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$,其中 α 和 β 是未知幅度. 输入线路的状态是$|\psi_0\rangle$,

$$|\psi_0\rangle = |\psi\rangle\,|\beta_{00}\rangle \tag{1.28}$$

$$=\frac{1}{\sqrt{2}}[\alpha\,|\,0\rangle\,(|\,00\rangle+|\,11\rangle)+\beta\,|\,1\rangle\,(|\,00\rangle+|\,11\rangle)] \tag{1.29}$$

其中约定前两个量子比特(左边)属于 Alice,而第三个量子比特属于 Bob. 如前所述,Alice 的第二个量子比特和 Bob 的量子比特是从同一个 EPR 状态来的. Alice 把她的量子比特送到一个受控非门,得到

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha\,|\,0\rangle\,(|\,00\rangle+|\,11\rangle)+\beta\,|\,1\rangle\,(|\,10\rangle+|\,01\rangle)] \tag{1.30}$$

接着她让第一量子比特通过一个 Hadamard 门,得到

$$|\psi_2\rangle = \frac{1}{2}[\alpha(|\,0\rangle+|\,1\rangle)(|\,00\rangle+|\,11\rangle)+\beta(|\,0\rangle-|\,1\rangle)(|\,10\rangle+|\,01\rangle)] \tag{1.31}$$

经过重新组项,这个状态可以重写为

$$|\psi_2\rangle = \frac{1}{2}[|\,00\rangle(\alpha\,|\,0\rangle+\beta\,|\,1\rangle)+|\,01\rangle(\alpha\,|\,1\rangle+\beta\,|\,0\rangle)$$

$$+|\,10\rangle(\alpha\,|\,0\rangle-\beta\,|\,1\rangle)+|\,11\rangle(\alpha\,|\,1\rangle-\beta\,|\,0\rangle)] \tag{1.32}$$

这个表达式自然地分为四项. 第一项状态$|00\rangle$中含有 Alice 的量子比特,状态 $\alpha|0\rangle+\beta|1\rangle$包含 Bob 的量子比特,也就是最初的状态$|\psi\rangle$. 如果 Alice 进行测量并得到$|00\rangle$,那么 Bob 的系统就处于状态$|\psi\rangle$. 类似地,从上面的表达式,我们可以在给定 Alice 测量结果的情况下,读出 Bob 的测后状态:

$$00 \mapsto |\psi_3(00)\rangle \equiv [\alpha\,|\,0\rangle+\beta\,|\,1\rangle] \tag{1.33}$$

$$01 \mapsto |\psi_2(01)\rangle \equiv [\alpha\,|\,1\rangle+\beta\,|\,0\rangle] \tag{1.34}$$

$$10 \mapsto |\psi_3(10)\rangle \equiv [\alpha\,|\,0\rangle-\beta\,|\,1\rangle] \tag{1.35}$$

$$11 \mapsto |\psi_2(11)\rangle \equiv [\alpha\,|\,1\rangle-\beta\,|\,0\rangle] \tag{1.36}$$

依赖于 Alice 的测量结果,Bob 的量子比特将落到这四个可能状态之一. 当然,要

知道在哪个状态，Bob 必须知道 Alice 的测量结果，我们将在后面说明，正是这个事实使量子隐形传态传送信息的速率不能超过光速. 一旦 Bob 得知测量的结果，Bob 就可以调整他的状态，采用适当的量子门恢复 $|\psi\rangle$. 例如，测量结果是 00，Bob 不需要做什么；如果是 01，Bob 可以应用 X 门来恢复；如果是 10，Bob 可以用 Z 门；如果是 11，Bob 可以先应用 X 再应用 Z 门来恢复；总之，Bob 需要应用变换 $Z^{M_1}X^{M_2}$ 到他的量子比特上(注意在线路图上时间从左到右，但在矩阵乘积项中在右边的先乘)，就能恢复状态 $|\psi\rangle$.

量子隐形传态有很多有趣的特性，我们后面会提到一些. 现在对其中几个方面进行评述. 首先，隐形传态不是让我们传送量子状态信息的速率超过光速了吗？这一点相当奇特，因为相对论蕴涵着，如果存在超光速信息传递，则可以把信息发回过去. 幸运的是，量子隐形传态没有带来超光速通信，因为完成隐形传态，Alice 必须通过经典信道把她的测量结果传给 Bob. 2.4.3 节将看到如果没有经典信道，隐形传态根本不传送任何信息. 经典信道受到光速的限制，因此量子隐形传态不能超过光速完成，这样就解决了这个佯谬.

第二个关于隐形传态的谜是：它看上去生成了要传状态的一个备份，从而明显地违背了 1.3.5 节讨论的不可克隆定理. 这只是一种错觉，因为隐形传态过程之后，只有目标量子比特处于状态 $|\psi\rangle$，而原始的数据比特依赖于第一量子比特测量结果，消失在 $|0\rangle$ 或 $|1\rangle$ 的基态中.

我们从量子隐形传态学到了什么？很多！它绝不仅仅是可以实施在量子状态上的优雅技巧. 量子隐形传态强调量子力学不同资源之间的互换性，显示出一个共享的 EPR 对加上两个经典比特的通信构成一个至少等于单量子比特通信的资源. 量子计算与量子信息的研究揭示出大量的资源互换方法，其中许多建立在量子隐形传态的基础之上. 特别地，在第 10 章，我们将解释隐形传态如何用于构造抗噪声量子门，在第 12 章我们将指出隐形传态与量子纠错码的性质紧密相关. 尽管与其他主题有这些联系，实事求是地说人类才刚开始明白为什么量子隐形传态在量子力学中是可能的. 后面的章节我们会努力通过阐述一些见解来让读者真正有所理解.

1.4　量子算法

量子线路可以进行哪些类型的计算？这类计算与用经典逻辑电路可做的计算相比如何？能找到量子计算机比经典计算机完成得好的任务吗？本节考虑这些问题，解释如何在量子计算机上做经典计算，给出量子计算机优于经典计算机的一些问题的例子，并总结已知的量子算法.

1.4.1 量子计算机上的经典计算

能用量子线路模拟经典逻辑线路吗？不奇怪，答案是肯定的，若答案是否定的，就太奇怪了.因为物理学家相信我们周围的世界，包括经典逻辑线路，最终都可以用量子力学进行解释.如前指出，量子线路不能用于经典线路的直接模拟，这是因为酉量子逻辑门具有内在可逆性，而许多经典逻辑门，如与非门，本质上是不可逆的.

采用一种称为 Toffoli 门的可逆门，任何经典线路都可以用等价的，仅包含可逆元件的线路代替. Toffoli 门有 3 个输入比特和 3 个输出比特，如图 1.14 所示.两个控制比特不受 Toffoli 门作用的影响，第三个比特是目标比特，在控制比特都置 1 时翻转，否则不变.注意连续应用两次 Toffoli 门到一组比特，相当于$(a,b,c)\to(a,b,c\oplus ab)\to(a,b,c)$，因此 Toffoli 门是可逆门，因为它有逆，逆是它本身.

输入			输出		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

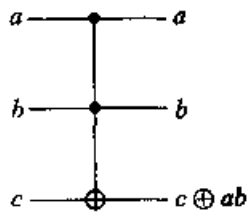


图 1.14 Toffoli 门的真值表和线路表示.

如图 1.15 所示，Toffoli 门可用来模拟与非门，还可以实现扇出，这如图 1.16 所示.有了这两个操作就可以模拟经典线路所有其他元件，因此任意的经典线路都可以被等价的可逆线路模拟.

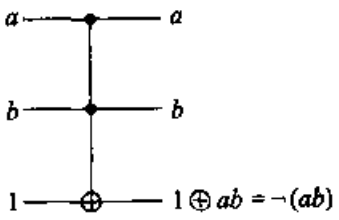


图 1.15 采用 Toffoli 门实现与非门的经典线路.上边两比特表示与非门的输入，第三比特设置为标准状态 1，有时称为附属状态.与非门的输出在第三比特.

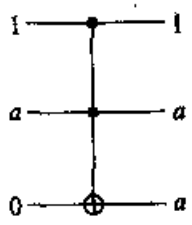


图 1.16 用 Toffoli 门实现的扇出，第二比特是扇出的输入（另外两个比特代表附属状态），扇出的输出出现在第二和第三比特.

Toffoli 门虽以经典门形式出现，却也可作为量子逻辑门实现. 由定义，Toffoli 门的量子逻辑实现只是按经典 Toffoli 门同样的方式置换基态. 例如量子 Toffoli 门作用到状态$|110\rangle$上就翻转第三量子比特，因为前两量子比特均被置位(set)，就进入状态$|111\rangle$. 虽然繁琐，但不难写出这个变换的 8×8 矩阵 U，并可具体证明 U 是酉矩阵，从而 Toffoli 门是合法的量子门. 量子 Toffoli 门可以像经典 Toffoli 门那样用于模拟不可逆逻辑门，并保证量子计算机可以进行任何经典(确定性)计算机能够完成的计算.

如果经典计算机是不确定的，即它具有产生被用于计算的随机比特的能力，情况会怎么样？不奇怪，量子计算机很容易模拟它. 为了完成这种模拟，只要使随机的均匀硬币产生投掷就足够了. 而这可以通过制备一个处于状态$|0\rangle$的量子比特，送到一个 Hadamard 门产生出$(|0\rangle+|1\rangle)/\sqrt{2}$，再进行状态测量来完成，结果是$|0\rangle$和$|1\rangle$各有 50%概率. 这就为量子计算机提供了有效模拟不确定的经典计算机的能力.

当然，如果模拟经典计算机是量子计算机仅有的特点，那么探索量子效应的努力就没什么必要. 量子计算的好处在于采用量子比特和量子门，可以计算功能更强大的函数. 在下面的几节里我们要借助 Deutsch-Jozsa 算法解释这是如何实现的，它是我们的第一个比任何经典算法求解问题都更快的量子算法的例子.

1.4.2　量子并行性

量子并行性是许多量子算法的一个基本特征，简言之，量子并行性使量子计算机可以同时计算函数 $f(x)$在许多不同的 x 处的值. 本节将阐述量子并行性的原理及其某些局限性.

设 $f(x):\{0,1\}\to\{0,1\}$是具有一比特定义域和值域的函数. 在量子计算机上计算该函数的一个简便办法是，考虑初态为$|x,y\rangle$的双量子比特的量子计算机. 通过适当的逻辑门序列可以把这个状态变换为$|x,y\oplus f(x)\rangle$，这里$\oplus$表示模 2 加，第一个寄存器称为数据寄存器，第二个称为目标寄存器，映射$|x,y\rangle\to|x,y\oplus f(x)\rangle$叫做 U_f，容易证明它是酉的. 若 $y=0$，则第二个量子比特的终了状态就是 $f(x)$值(在 3.2.5 节中，我们说明所给定的计算 $f(x)$的一个经典线路是一个效率相当的量子线路，它在量子计算机上计算变换 U_f. 这里我们可以把它看做一个黑箱(black box)).

考虑图 1.17 的线路，把 U_f 加到计算基以外的一个输入. 数据寄存器中是叠加态$(|0\rangle+|1\rangle)/\sqrt{2}$，这可由 Hadamard 门作用到$|0\rangle$上得到. 于是应用 U_f 得到状态

$$\frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}} \tag{1.37}$$

这是一个值得注意的状态，不同的项同时包含 $f(0)$和 $f(1)$，看起来似乎同时对 x 的两个值计算了 $f(x)$. 与经典的并行不同，那里多重 $f(x)$电路同时运行，而这里，利用量子计算机处于不同状态的叠加态的能力，单个 $f(x)$线路用来同时计算多个 x 的函数值.

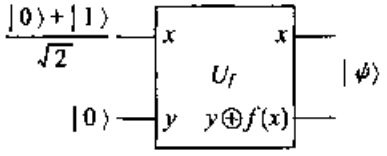


图 1.17 同时计算 $f(0)$和 $f(1)$的量子线路. U_f 是把输入$|x,y\rangle$变成 $|x,y\oplus f(x)\rangle$.

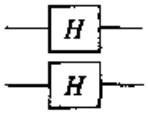


图 1.18 双量子比特上的 Hadamard 变换 $H^{\otimes 2}$.

利用 Hadamard 变换，有时又称为 Walsh-Hadamard 变换，这个过程很容易推广到任意数目的量子比特上的函数. 该变换就是 n 个 Hadamard 门同时作用到 n 个量子比特上. 例如图 1.18 是 $n=2$，初态全为$|0\rangle$的情况，输出是

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)=\frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2} \tag{1.38}$$

我们以 $H^{\otimes 2}$表示两个 Hadamard 门的并行作用，“$\otimes$”读作“张量积”. 更一般地，n 重量子比特上的 Hadamard 变换从全$|0\rangle$出发，得到

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle \tag{1.39}$$

其中求和是对 x 的所有可能取值，并用 $H^{\otimes n}$表示这个作用. 可见，Hadamard 变换产生了所有计算基态的平衡叠加(equal superposition)，而且，它的效率非常高，仅用 n 个门就产生了 2^n 个状态的叠加.

可以采用下述方法进行 n 比特输入 x 和单比特输出 $f(x)$函数的量子并行计算. 制备 $n+1$ 量子比特的状态$|0\rangle^{\otimes n}|0\rangle$，对前 n 位应用 Hadamard 变换，并连接实现 U_f 的量子线路. 这就产生状态

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|f(x)\rangle \tag{1.40}$$

在某种意义上，表面上似乎只进行一次 f 计算，量于并行性却使 f 的所有可能值同时被计算出来. 然而，这种并行性并不是直接就有用. 对单量子比特，测量状态得到$|0,f(0)\rangle$或$|1,f(1)\rangle$ 中的一个，一般而言，测量状态 $\sum_x |x,f(x)\rangle$ 也类似地只给出对某个单个 x 的 $f(x)$值. 经典计算机当然很容易可以做到这一点！为了真正有用，量子计算要求的不仅仅是量子并行性；它要求比从叠加态 $\sum_x |x,f(x)\rangle$ 中得到一个 $f(x)$值更高的信息抽取能力. 下两节我们会通过例子看这是如何实现的.

1.4.3　Deutsch 算法

图 1.17 的线路稍加修改，就可以用 Deutsch 算法的实现来说明量子线路如何超越经典线路(我们实际是用了原始算法的改进和简化版本，参考本章末"历史和进一步阅读的材料"). Deutsch 算法把量子并行性和量子力学中称为干涉(interference)的性质结合了起来. 像以前一样，我们用 Hadamard 门把第一量子比特变为叠加态$(|0\rangle+|1\rangle)/\sqrt{2}$，但现在使用施加于状态$|1\rangle$的 Hadamard 门把第二量子比特 y 变为叠加态$(|0\rangle-|1\rangle)/\sqrt{2}$. 在如图 1.19 所示的线路中，让我们随着状态看，会发生些什么.

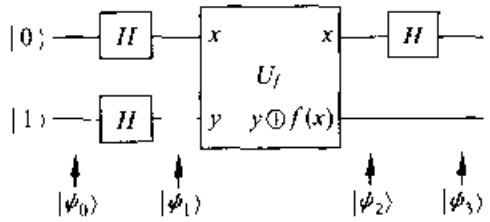


图 1.19　实现 Deutsch 算法的量子线路.

输入状态

$$|\psi_0\rangle = |01\rangle \tag{1.41}$$

通过两个 Hadamard 门后，给出

$$|\psi_1\rangle = \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \tag{1.42}$$

很容易看到，如果应用 U_f 到状态$|x\rangle(|0\rangle-|1\rangle)/\sqrt{2}$上，就可得状态$(-1)^{f(x)}\times|x\rangle(|0\rangle-|1\rangle)/\sqrt{2}$. 于是把 U_f 应用到$|\psi_1\rangle$上，就出现两种可能情形之一：

$$|\psi_2\rangle = \begin{cases} \pm\left[\dfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & f(0)=f(1) \\ \pm\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & f(0)\neq f(1) \end{cases} \tag{1.43}$$

最后的 Hadamard 门作用在第一量子比特上，导致

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & f(0)=f(1) \\ \pm|1\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & f(0)\neq f(1) \end{cases} \tag{1.44}$$

注意到当 $f(0)=f(1)$时，$f(0)\oplus f(1)$为 0，其他情况为 1，可以重写该结果为

$$|\psi_3\rangle = \pm|f(0)\oplus f(1)\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \tag{1.45}$$

这样，通过测量第一量子比特，我们可以确定 $f(0)\oplus f(1)$. 这非常有意义：量子线路可以让我们仅用对 $f(x)$的一次计算，就能够确定 $f(x)$的全局性质，即 $f(0)\oplus f(1)$. 这个过程比所有可能的经典设备都要快，因为经典设备至少要两次计算.

这个例子使量子并行性与经典随机化算法的差别凸显出来，简单地说，可以认为状态$|0\rangle|f(0)\rangle+|1\rangle|f(1)\rangle$非常接近于以$\frac{1}{2}$概率算 $f(0)$、以$\frac{1}{2}$概率算 $f(1)$的经典概率计算机. 差别在于经典计算机上这两种选择总是互相排斥的，而在量子计算机上，两种选择却可能通过相互干涉，而给出函数 $f(x)$的某些全局性质，具体方法是像在 Deutsch 算法中那样，利用如 Hadamard 门那样的装置，对不同选择进行重新组合. 许多量子算法设计的本质在于，精心选择函数和最终变换，以便有效地确定有关函数的有用全局信息，而经典计算机上无法快速得到.

1.4.4 Deutsch-Jozsa 算法

Deutsch 算法是一般量子算法的简单例子，称为 Deutsch-Jozsa 算法. 作为应用，就是 Deutsch 问题，可以被描述为如下的游戏. 阿姆斯特丹的 Alice，在从 0 到 2^n-1 的数中选择一个数 x，通过信把它邮寄给波士顿的 Bob. Bob 计算出某个函数值 $f(x)$，不是 0 就是 1，并把它寄回给 Alice. Bob 保证只用两类函数之一：要么 $f(x)$对所有的 x 是常数；要么 $f(x)$是平衡的(balanced)，即恰好有所有可能的 x 的一半使函数取 1，另一半使函数取 0. Alice 的目的是用尽可能少的通信，确定出 Bob 用的是常数还是平衡函数. 她能做到多快?

经典情形下，Alice 一封信只能发给 Bob 一个 x 值. 最坏情况下，Alice 至少要问 Bob $2^n/2+1$ 次，因她可能在收到 $2^n/2$ 个 0 后收到一个 1，使她得知 Bob 的函数是平衡的，所以最好的确定性经典算法需要 $2^n/2+1$ 次询问. 注意每封信中，Alice 发给 Bob n 比特信息，在此例中用物理上的距离来人为估计计算 $f(x)$的费用，但这在一般问题中是不必要的，一般问题中 $f(x)$可能是本质上难以计算的.

如果 Alice 和 Bob 可以交换量子比特，而不是经典比特，而且如果 Bob 同意使用酉变换 U_f 来计算 $f(x)$，那么 Alice 通过和 Bob 的一次通信就可以达到目的. 算法如下.

类似于 Deutsch 算法，Alice 用一个 n 量子比特的寄存器存储她的查询输入，用一个单量子比特寄存器给 Bob 存储答案. 开始时她把查询和答案寄存器置子一个叠加态，Bob 用量子并行性计算 $f(x)$，把结果放在答案寄存器中，Alice 接着用 Hadamard 变换干涉查询寄存器的状态，再通过适当的测量，决定 f 是平衡函数还是常数.

算法的具体步骤描绘在图 1.20 中. 我们考察一下线路中的状态，输入状态类似于式(1.41)为

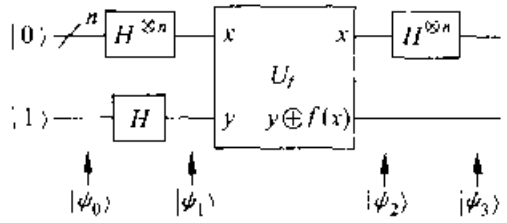


图 1.20　实现一般 Deutsch-Jozsa 算法的量子线路.类似于工程上通用的符号,带有/的线表示穿过此线的一组 n 量子比特.

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle \tag{1.46}$$

但这里的查询寄存器描述了全都处于$|0\rangle$状态的 n 量子比特的状态.经过查询寄存器上的 Hadamrad 变换和答案寄存器上的 Hadamrad 门,得到

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^n}\frac{|x\rangle}{\sqrt{2^n}}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \tag{1.47}$$

查询寄存器现在处于所有值的叠加,而答案寄存器是 0 和 1 的一个平衡叠加.接下来,使用 U_f: $|x,y\rangle \to |x,y\oplus f(x)\rangle$,进行函数 f 的计算(由 Bob 进行),给出

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}}{\sqrt{2^n}}|x\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \tag{1.48}$$

Alice 现在拥有一组量子比特,Bob 的函数计算结果被保存在量子比特叠加态的幅度中,她利用查询寄存器上的 Hadamrad 变换,来干涉叠加态中的项.为确定 Hadamrad 变换的结果,可以先算出 Hadamrad 变换在一个状态 $|x\rangle$ 上的效应.分别考察 $x=0$ 和 $x=1$ 的情况,可以看到,对单量子比特而言,有 $H|x\rangle = \sum_z (-1)^{xz}|z\rangle/\sqrt{2}$.于是

$$H^{\otimes n}|x_1,\cdots,x_n\rangle = \frac{\sum_{z_1,\cdots,z_n}(-1)^{x_1z_1+\cdots+x_nz_n}|z_1,\cdots,z_n\rangle}{\sqrt{2^n}} \tag{1.49}$$

写成非常有用的更紧凑形式

$$H^{\otimes n}|x\rangle = \frac{\sum_z (-1)^{x\cdot z}|z\rangle}{\sqrt{2^n}} \tag{1.50}$$

其中 $x\cdot z$ 是 x 和 z 的模 2 按位内积.利用此式和式(1.48),我们可以计算$|\psi_3\rangle$,

$$|\psi_3\rangle = \sum_z\sum_x \frac{(-1)^{x\cdot z+f(x)}}{2^n}|z\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \tag{1.51}$$

Alice 开始查看查询寄存器,注意状态$|0\rangle^{\otimes n}$的幅度是 $\sum_x (-1)^{f(x)}/2^n$.考察两种可能的情况——f 是常数和 f 是平衡函数——以辨别所出现的结果.f 是常数,$f(x)$得常数值,$|0\rangle^{\otimes n}$的幅度是+1 或−1,因为$|\psi_3\rangle$具有单位长度,故所有其他幅度必

须是0，且测量会使查询寄存器的全部量子比特都成为0. f 是平衡函数，对 $|0\rangle^{\otimes n}$ 的正负幅度贡献抵消，幅度为0，查询寄存器的至少一位的测量结果为非零. 归纳起来，如果 Alice 测量是全0.则函数是常数；否则函数是平衡的. Deutsch-Jozsa 算法可总结如下.

算法 Deutsch-Jozsa

输入 (1) 对 $x\in\{0,\cdots,2^n-1\}$ 和 $f(x)\in\{0,1\}$ 进行变换 $|x\rangle|y\rangle\rightarrow|x\rangle|y\oplus f(x)\rangle$ 的黑箱 U_f，已知 $f(x)$ 或者对所有的 x 是常数或者是平衡的，即恰好对于所有可能的 x 的一半取1，另一半取0.

输出 当且仅当 f 是常数，为0

运行时间 计算 U_f 一次，总是成功的.

过程

(1) $|0\rangle^{\otimes n}|1\rangle$ // 状态初始化

(2) $\rightarrow\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$ // 用 Hadamard 门产生叠加

(3) $\rightarrow\frac{1}{\sqrt{2^n}}\sum_x(-1)^{f(x)}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$ // 用 U_f 计算函数 f

(4) $\rightarrow\sum_z\sum_x\frac{(-1)^{x\cdot z+f(x)}}{2^n}|z\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$ // 进行 Hadamard 变换

(5) $\rightarrow z$ // 测量最终输出 z

我们说明了量子计算机用函数 f 的一次计算就能解决 Deutsch 问题，而与此相比，经典计算需要计算 $2^n/2+1$ 次. 这给人留下很深的印象，不过有几点重要的提醒. 首先 Deutsch 问题不是一个具有实质重要性的问题，它没有已知的应用. 其次，某种角度上，经典和量子算法很难比较，因为计算函数值的方法差别很大. 最后，如果 Alice 可以使用概率经典计算机，那么让 Bob 对随机选择的一些 x 计算函数值 $f(x)$，Alice 可以很快以非常高的概率确定 f 是常数还是平衡函数，这种概率模型比我们考虑的确定性模型也许更现实. 尽管有这些提醒，Deutsch-Jozsa 算法仍包含着孕育更加影响深远的量子算法的种子，它对试图理解运算背后的规律很有启发性.

练习 1.1(概率经典算法) 假设问题不是确定性地区分常数和平衡函数，而是以误差 $\varepsilon<1/2$ 的概率区分，那么问题的最佳经典算法的性能如何？

1.4.5 量子算法的总结

Deutsch-Jozsa 算法暗示着，量子计算机解决一些计算问题的效率有可能远远超过经典计算机，不幸的是，那个问题几乎没有什么实际意义. 是否存在用量子算

法可以更有效地获得解的更有意义的问题？这类算法背后的基本原理是什么？量子计算机计算能力的极限是什么？

广而言之，有三类优于已知经典算法的量子算法. 第一，基于 Fourier 变换的量子版本的一类量子算法，Fourier 变换在经典算法中也广泛应用，Deutsch-Jozsa 算法是这类算法的例子，Shor 的因子分解算法和离散对数算法也是这样. 第二类算法是量子搜索算法. 第三类算法是量子仿真，用量子计算机模拟量子系统. 下面简述这些算法，并综述关于量子计算机计算能力的已知或推测的结果.

1. 基于 Fourier 变换的量子算法

离散 Fourier 变换通常被视为 N 元复数集合 $x_0,\cdots,x_{N-1}$ 到复数集合 $y_0,\cdots,y_{N-1}$ 的变换，定义如下：

$$y_k \equiv \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi ijk/N} x_j \tag{1.52}$$

当然，这个变换在科学的许多分支中有无数的应用，因为 Fourier 变换后的问题常比原问题更容易得到解答.

Fourier 变换非常有用，实际上已形成了超出定义式(1.52)的一套优美的 Fourier 变换理论. 这个一般理论涉及来源于有限群特征的一些技巧和思想，在这里我们不打算讨论. 重要的是用于 Deutsch-Jozsa 算法的 Hadamard 变换是一类广义 Fourier 变换的特例，而且，许多其他重要的量子算法也涉及某种类型的 Fourier 变换.

已知的最重要的量子算法，即 Shor 的快速因子分解算法和离散对数算法，是基于式(1.52)定义的 Fourier 变换算法的两个例子. 式(1.52)就所呈现的形式而言，并没有太多的量子力学味道. 然而，设想一下，通过量子比特在计算基 $|j\rangle(0\leqslant j\leqslant 2^n-1)$ 上的作用，定义一个 n 量子比特上的线性变换 U

$$|j\rangle \rightarrow \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n}|k\rangle \tag{1.53}$$

可以验证该变换是酉的，而且事实上它还可以用量子线路实现. 进而，如果写出它在叠加态上的作用

$$\sum_{j=0}^{2^n-1} x_j|j\rangle \rightarrow \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}\left[\sum_{j=0}^{2^n-1} e^{2\pi ijk/2^n} x_j\right]|k\rangle = \sum_{k=0}^{2^n-1} y_k|k\rangle \tag{1.54}$$

可以看到，它是对应于 Fourier 变换式(1.52)$N=2^n$ 的一种向量形式.

Fourier 变换的快速性如何？在经典情形，快速 Fourier 变换花大约 $N\log(N)=n2^n$ 步来完成 $N=2^n$ 个数的 Fourier 变换. 在量子计算机上，Fourier 变换可以用约 $\log^2(N)=n^2$ 步完成，指数量级节省了计算步数！第 5 章会给出相应的量子线路.

这个结果似乎显示，量子计算机可以非常迅速地计算 2^n 个复数的向量的

Fourier 变换，这对很大范围的应用将极为有用，然而，事实并非完全如此. Fourier 变换是在“隐含”于量子状态幅度的信息上进行的，这些信息无法从测量中直接得到. 问题在于，如果测量输出状态，将使每个量子比特都坍缩到$|0\rangle$或$|1\rangle$状态，我们就无法直接知道变换的结果 y_k. 这个例子触及设计量子算法之谜的核心. 一方面，我们能以远比经典计算机有效的方式，在 n 量子比特的 2^n 个幅度上进行某项计算，但另一方面，采用直接的方法无法利用这样的计算结果. 为利用量子计算的能力需要用更聪明的办法.

幸运的是，确实有可能利用量于 Fourier 变换来有效求解若干被认为经典计算机无法有效求解的问题. 这些问题包括 Deutsch 问题、Shor 的离散对数和因子分解算法、Kitaev 发现的 Abel 稳定子问题的一种解决方法和对隐含子群问题的推广使这个方向的研究达到高潮. 隐含子群问题是：设 f 是从有限生成群 G 到有限集合 X 的函数，f 在子群 K 的陪集上是常数，而且在每个陪集上取值不同. 给定量子黑箱进行酉变换 $U|g\rangle|h\rangle=|g\rangle|h\oplus f(g)\rangle$，其中 $g\in G, h\in X$，$\oplus$是在 X 上适当选择的二元运算，找出 K 的一个生成集.

Deutsch-Jozsa 算法、Shor 算法以及指数加速的量子算法均可被视为该算法的特殊情况. 量于 Fourier 变换及其应用将在第 5 章阐述.

2. 量子搜索算法

量子搜索算法是完全不同类型的算法，其基本原理由 Grover 发现. 量子搜索算法解决如下问题：给定大小为 N 的搜索空间，没有关于它结构信息的先验知识，希望找到这个搜索空间中的满足已知性质的一个元素. 要找到一个满足条件的元素需要多久？经典情形，这个问题需要大概 N 次操作，但量子搜索算法可以用大概$\sqrt{N}$次操作解决.

量子搜索算法只提供了二次加速，不如基子量子 Fourier 变换的算法的指数加速令人印象深刻. 然而，量子搜索算法仍有很大意义，因为搜索方面的知识的应用比量于 Fourier 变换解决的问题更广，而且采用量子搜索算法对很宽范围的问题都可能有用. 量子搜索算法及其应用将在第 6 章阐述.

3. 量子仿真

对于量子计算机擅长，而经典计算机却难于完成的任务的一个明显的选择问题是模拟自然发生的量子力学系统. 经典计算机模拟一般量子系统遇到困难的原因与它们难于模拟量子计算机大致相同，描述量子系统需要的复数个数往往随系统规模的增大呈指数性，而不是线性增长. 像经典系统那样，一般地，存储具有 n 个不同元素的系统的量于状态需要大概 c^n 比特经典计算机的内存，这里 c 是依赖于被模拟系统细节和模拟精度的常数.

与之对照，量子计算机可以用 kn 量子比特进行模拟，k 也是依赖于被模拟系

统细节的常数，这使量子计算机可以有效模拟被认为在经典计算机上不能模拟的量子力学系统. 一个重要的提醒是，即使量子计算机可以比经典计算机远为有效地模拟许多量子系统，这并不意味着快速模拟能得到关于量子系统的期望信息. 测量时，一个 kn 量子比特的模拟将坍缩为一个确定状态，只给出 kn 比特的信息，在波函数(wavefunction)中的 c^n 比特的隐含信息不能全部访问. 因此，量子仿真的一个关键步骤是，研究有效抽取期望答案的系统化方法，但如何去做还不完全清楚.

尽管有这个提醒，量子仿真看来将是量子计算机的一项重要应用. 量子系统仿真在许多领域都很重要，特别是在量子化学中. 由于经典计算机在计算能力上的限制，使得它很难精确模拟哪怕是中等规模的分子，更不用说在许多重要生物学系统中出现的超大分子了. 因此获得这类系统的更快和更精确的仿真，有利于促进量子现象扮演重要角色的其他领域的发展.

将来我们也许会发现，自然界的物理现象不能在量子计算机上得到有效模拟，这绝对不是坏消息，而是太妙了！至少它会激励我们扩展计算模型来包含新的现象，并增加我们计算模型的能力，来超过现有的量子计算模型. 有趣的新的物理效应也很可能与任何此类现象有关.

量子仿真的另一应用是作为获得其他量子算法的灵感的一般途径，例如 6.2 节中，我们会解释量子搜索算法如何被视为一个量子模拟问题的解. 通过以这种方式看问题，理解量子搜索算法的产生要容易得多.

最后，量子模拟也为 Moore 定律提供了一个有趣和乐观的量子推论. 回想 Moore 定律是说，经典计算机的计算能力将以固定成本，约每两年增加一倍. 然而，设想我们在经典计算机上模拟量子系统，要增加单个量子比特(和更大的系统)到被模拟的系统中，这需要经典计算机上存储量子系统状态的内存增加一倍或更多，同时模拟动态系统需要相同或更多的时间. 基此，就有 Moore 律的量子推论，即如果能够每两年向量子计算机增加一个量子比特，量子计算机将保持与经典计算机相同的步伐. 对这个推论倒不必太认真，因为量子计算超过经典计算的程度，即使存在，准确性质也尚不清楚. 不过，这个概念有助于解释为什么我们对量子计算机感兴趣，并且也许有朝一日，它们至少在某些应用上能超过最强大的经典计算机.

4. 量子计算的能力

量子计算的能力强大到何种程度？这种能力的来源是什么？尽管诸如因子分解那样的例子，让人猜测量子计算机很有可能比经典计算机更强大，但这些问题的答案仍不得而知. 从任何可用量子计算机有效求解的问题在经典计算机上也可能求解的角度看，仍存在量子计算机并不比经典计算机更强大的可能性；另一方面，人们也可能最终证明量子计算机远比经典计算机强大. 下面综述一下关于量子计算能力的已知事实.

计算复杂性理论对包括经典和量子计算问题的各种计算问题的难度进行了分类.为弄清量子计算机的计算能力,我们先来考察一些计算复杂性的一般概念,最基本的是复杂类(complexity class)概念.一个复杂类被认为是计算问题的一个集合,这些问题在求解所需计算资源上具有共性.

最重要的两个复杂类分别称为 P 和 NP 类.粗略地说,P 类在经典计算机上可以快速求解,NP 的解可以在经典计算机上迅速检验.为明确 P 和 NP 的区别,考虑求整数 n 的素因子的问题.到目前为止,还不知道在经典计算机上求解此问题的快速方法,这暗示它不在 P 类中.另一方面,如果某人告诉你 p 是 n 的因子,你可以通过用 p 去除 n,来很快检查其正确性,于是这问题属于 NP 类.

很清楚 P 类是 NP 类的子集,因为能求解意味着必然能检验可能的解.尚不清楚是否存在不属 P 类的 NP 问题.理论计算机科学中最重要的未解决的问题也许就是确定这两个类是否不同:

$$P \neq NP \tag{1.55}$$

大多数研究者相信 NP 包含不属于 P 的问题,特别地,NP 类中有一个重要的子类——NP 完全(NP-complete)问题类.NP 完全类的重要性在于两个方面:首先,已知有成千上万的问题,包括许多非常重要的问题,是 NP 完全的;其次,任何一个给定的 NP 完全问题,在某种意义下,至少和所有其他 NP 问题"一样难".更精确地,求解特定 NP 完全问题的算法只要增加一点附加资源,就可用来求解 NP 类中任何其他问题.特别地,如果 $P \neq NP$,那么没有任何 NP 完全问题可以在经典计算机上有效求解.

尚不清楚量子计算机是否可以快速求解 NP 类的所有问题,尽管它们可以解决一些问题,像因子分解问题,很多人认为这个问题属于 NP 而不属于 P(注意,还不知道因子分解问题是否为 NP 完全,否则我们就知道如何用量子计算机有效求解所有 NP 问题了).倘若可以用量子计算机有效求解所有 NP 问题,那当然非常令人激动.有一个在这个方向上所知道的有趣的反面结论,排除了用量子并行性的简单变化来解所有 NP 问题的可能性.确切地说,量子计算机上解 NP 问题的一个办法是利用某种形式的量子并行机制来并行搜索问题的所有可能解.在 6.6 节,会看到不存在基于这种搜索手段的方法能对所有 NP 问题给出有效解答.这种方法不成功虽然令人失望,但它并不排除在 NP 问题中存在更深层的结构,使得用量子计算机能够快速求解它们.

P 类和 NP 类只是已定义的诸多复杂类中的两个,另一重要的复杂类是 PSPACE 类.粗略地说,PSPACE 类包括在空间尺寸方面使用很少的资源(即计算机"小")可以求解,而时间上未必短(计算可以"长")的那些问题.人们相信

PSPACE 类严格超过 P 和 NP 类，尽管这也是未被证明的. 最后，BPP 类是如果在对问题的求解中允许有限的误差概率(如 1/4)，用多项式时间随机算法可以求解的问题类. BPP 类被广泛认为甚至比 P 类更适合作为用经典计算机能够有效求解的问题类. 我们集中注意力在 P 类而不是 BPP 类的原因是，人们对 P 类的研究更为深入，不过在 BPP 类问题中会有许多与 P 相似的思路和结论.

量子复杂类情形怎样？我们可以定义 BQP 类为，当允许有限的误差概率时，量子计算机可以有效求解的所有计算问题的类(严格讲，这使 BQP 类更像经典的 BPP 复杂类而不是 P 类，不过我们暂且忽略这个细微的差别，把它视为 P 的类似物). 目前尚不知 BQP 类与 P、NP 和 PSPACE 类的准确关系. 所知的是量子计算机可以有效求解所有 P 类问题，但不存在 PSPACE 类以外的问题可以用量子计算机有效求解. 因此 BQP 类处在 P 类与 PSPACE 类之间的某个位置，如图 1.21 所示. 一个重要的推论是，如果证明量子计算机的能力严格强于经典计算机，那么 P 类就能不等于 PSPACE 类. 许多计算机科学家试图证明后面这个结论，却都未成功，这暗示证明量子计算机比经典计算机更强大的命题也许是不平凡的，尽管有许多证据支持这个命题.

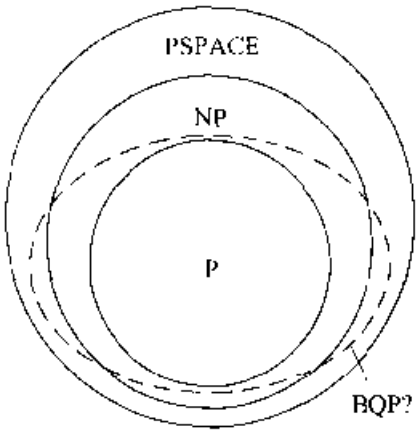


图 1.21　经典和量子复杂类的关系. 量子计算机可以快速求解任何 P 类问题，且已知不能迅速求解 PSPACE 类以外的问题. 量子计算机应该在 P 类和 PSPACE 类之间的什么位置尚不清楚. 部分原因是我们甚至不知道 PSPACE 类是否比 P 类大.

我们现在不再继续探讨量子计算能力的极限，等到对快速量子算法的基本原理更好了解以后再讨论. 快速量子算法的基本原理是本书第二部分花很多篇幅阐述的主题. 现在能够明确的是，量子计算的理论向传统的计算概念提出了有趣和重要的挑战. 其原因是量子计算的理论模型被认为在实验上是可实现的，因为这个理论与自然界的运行方式相符. 如果情况不是这样，量子计算就不过是在数学上令人好奇而已.

1.5 实验量子信息处理

量子计算与量子信息是了不起的理论发现，但它的核心概念，如叠加和纠缠跟我们从周围世界得来的直觉相矛盾. 我们有什么证据表明这些概念真的描述了大自然的运行？实现大规模量子计算机在实验上可行吗？或者是否有某个物理定律从根本上禁止它们最终成为大规模？下两节我们来回答这些问题. 我们从回顾著名的 Stern-Gerlach 实验开始，该实验提供证据，支持自然界中量子比特的存在. 接着我们扩展讨论的范围，研究更广的如何建造实际量子信息处理系统的问题.

1.5.1 Stern-Gerlach 实验

量子比特是量子计算与量子信息最基本的元素. 怎么知道自然界存在具有量子比特性质的系统？本书写作时已有无数证据支持这一点，而在量子力学发展的早期，量子比特的结构却并不很明显，人们为今天所知道的量子比特，即双能级量子系统的现象而争论.

指出量子比特结构的决定性的(也是著名的)早期实验是 Stern 在 1921 年设想出来，于 1922 年与 Gerlach 共同在法兰克福(Frankfurt)完成的. 在原始的 Stern-Gerlach 实验中，热原子束从炉体穿过磁场发生偏转，随后，每个原子都被记录下来如图 1.22 所示. 原始实验是用银原子做的，其复杂的结构使要讨论的效应模糊不清. 下面我们要描述的实际上是 1927 年用氢原子做的实验，可观察到相同的效应，但研究容易一些. 但要记住，20 世纪 20 年代初的人们并没有这个便利，为解释观察到的更为复杂的效应，他们必须极富创见.

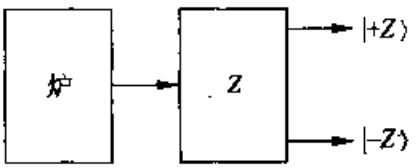


图 1.22 Stern-Gerlach 实验的抽象框图. 热的氢原子从炉体出来经过磁场，引起向上($|+Z\rangle$)或向下($|-Z\rangle$)的偏转.

氢原子包含一个质子和一个轨道电子. 可以把这个电子看作绕质子的微弱电流，这个电流使原子具有一个电磁场，每个原子都有物理学家所称的磁偶极矩(magnetic dipole moment)，结果每个原子都像一块轴对应于电子旋转方向的小磁铁. 把磁铁投入磁场会引起磁铁发生偏转，所以可以预期在 Stern-Gerlach 实验中原子也会出现类似的偏转.

原子如何偏转，依赖于原子的磁偶极矩——电子旋转所绕的轴——和由

Stern-Gerlach 装置产生的磁场，这里不进行详细说明，而是指出借助所建立的适当的 Stern-Gerlach 装置，可以让原子偏转的量依赖于原子磁偶极矩的 z 分量，其中 z 是某个固定参考轴.

进行这个实验出现两项令人吃惊的结果. 首先，由于很自然会认为，从炉体出来的热原子的偶极子定向随机分布在每个方向上，从 Stern-Gerlach 装置出来的原子在各个角度的分布应该是连续的，然而，实际所看到的是原子形成一组离散的角度. 物理学家通过假设原子的磁偶极矩是量子化的(quantized)，即呈现为某个基本量的离散倍数，来解释这一现象.

Stern-Gerlach 实验观察到的量子化让当时的物理学界吃惊，但不是震惊性的，因为那时量子化效应的证据在其他系统中也正多起来. 真正让人吃惊的是，实验中所看到的峰的数目. 使用氢原子的目的是，它们应具有零磁偶极矩. 从经典的角度看，这本身就是奇怪的，因为这意味着电子没有轨道运动，但基于当时的量子力学知识，这是可以接受的. 要使氢原子具有零磁矩，当时人们预期只能看到一束原子，并且不会被磁场偏转. 但实际上，看到了两束，一束在磁场作用下向上偏转，另一束向下.

这个令人困惑的双束之谜，在人们经过很大努力发现与氢原子电子相关联的一个称为自旋(spin)的量后，得到解释. 自旋和电子绕质子的普通旋转毫无关系，它是与电子自身相关的一个全新的量. 伟大的物理学家 Heisenberg 在这个想法刚提出时谓之勇敢，它之所以是勇敢的想法，原因在于它引进了本质上新颖的物理量. 电子的自旋被确认是对电子绕轨道运动贡献的补充，对氢原子的磁偶极矩有额外的贡献.

怎样合理描述电子的自旋？也许我们首先会猜想自旋是由一个控制氢原子向上或向下的比特决定的，然后根据进一步的实验结果，决定是否需要修改或更新这个猜测. 让我们用图 1.22 来表示原始的 Stern-Gerlach 实验装置，输出是两束原子，称为$|+Z\rangle$和$|-Z\rangle$(我们用了看起来更像量子力学的记号，当然你可以用自己喜欢的记号). 现在设想把两套 Stern-Gerlach 实验装置串联起来，如图 1.23 所示. 把第二套装置转动一下，好让磁场的偏转沿 x 轴. 在想象实验中把第一套 Stern-Gerlach 设备的$|-Z\rangle$输出断开，而把$|+Z\rangle$的输出送到第二套沿 x 轴定向的装置. 在最终的输出放置探测器，以测量原子沿 x 轴的分布.

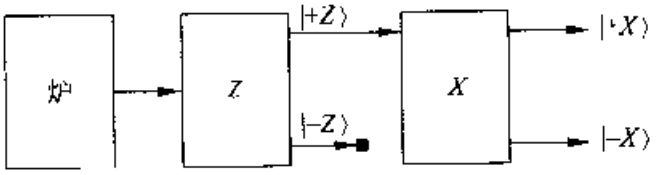


图 1.23　串联的 Stern-Gerlach 测量.

一个指向 z 轴的经典磁偶极子不具有 x 方向的净磁矩，因此在最终输出可能只会得到一个中心峰. 然而，实验中可以观测到两个等强度的峰. 因此也许这些原子很特殊，沿每个轴有独立的确定的磁矩，也就是说，每个通过第二套装置的原子可以描述为处在某个下述状态，这些状态记作$|+Z\rangle|+X\rangle$或$|+Z\rangle|-X\rangle$，以表明可能观测到自旋的两个值.

另外一个实验，如图 1.24 所示，可以把前面的输出送到 z 向的 Stern-Gerlach 装置，来测试我们的猜想. 如果原子保持$|+Z\rangle$定向，那么输出将会是只有一个峰，即在$|+Z\rangle$的输出，然而，在最终输出时，再次观察到等强度的两个束. 因此，结论似乎与经典的期望相违背，一个$|+Z\rangle$状态由等量的$|+X\rangle$和$|-X\rangle$状态组成，而一个$|+X\rangle$状态又由等量的$|+Z\rangle$和$|-Z\rangle$状态组成. 如果 Stern-Gerlach 装置沿其他轴排列，如 $\hat{y}$ 轴，仍会得到类似结论.

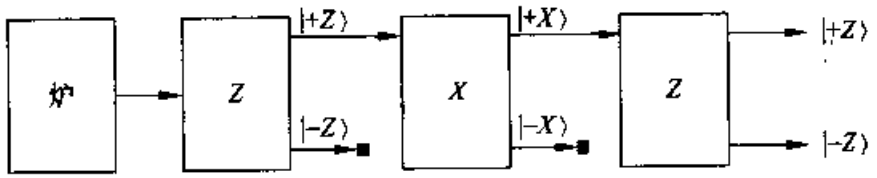


图 1.24 三阶段串联的 Stern-Gerlach 测量.

量子比特模型为观测到的实验行为提供了简单的解释. 令$|0\rangle$和$|1\rangle$为一个量子比特的状态，作如下赋值

$$|+Z\rangle \leftarrow |0\rangle \tag{1.56}$$

$$|-Z\rangle \leftarrow |1\rangle \tag{1.57}$$

$$|+X\rangle \leftarrow (|0\rangle + |1\rangle)/\sqrt{2} \tag{1.58}$$

$$|-X\rangle \leftarrow (|0\rangle - |1\rangle)/\sqrt{2} \tag{1.59}$$

则串联的 Stern-Gerlach 实验的结果可以解释为，假定 $\hat{z}$ Stern-Gerlach 装置在计算基$|0\rangle$，$|1\rangle$测量自旋，而 $\hat{x}$ Stern-Gerlach 装置相对基$(|0\rangle+|1\rangle)/\sqrt{2}$，$(|0\rangle-|1\rangle)/\sqrt{2}$测量自旋. 例如，对串联的 $\hat{z}$-$\hat{x}$-$\hat{z}$ 实验，若假定从第一套 Stern-Gerlach 实验出来的自旋处于状态$|+Z\rangle=|0\rangle=(|+X\rangle+|-X\rangle)/\sqrt{2}$，那么从第二套装置出来得到$|+X\rangle$的概率是 1/2，得到$|-X\rangle$的概率是 1/2，类似地，从第三套设备得到$|+Z\rangle$的概率是 1/2. 因此量子比特模型正确预言了这类串联的 Stern-Gerlach 实验的结果.

上述例子说明了量子比特如何可以作为自然界系统的可信模型. 当然，它没有消除量子比特模型作为理解电子自旋正确途径的全部疑问，这需要多得多的实验证据. 不过，因为有许多此类实验，我们现在相信量子比特是电子自旋的最好模型，而且我们相信量子比特模型(及其高维推广，即量子力学)能够描述所有物理系统.

我们现在考虑哪类系统特别适合用于进行量子信息处理的问题.

1.5.2　实际量子信息处理的前景

建立量子信息处理装置,是新千年科学家和工程师所面临的一项巨大挑战.我们能应付这个挑战吗?这可能吗?值得尝试吗?果真如此,怎样做呢?这些都是既困难又重要的问题,我们在本节简要回答这些问题,并贯穿全书展开论述.

最根本的问题是,是否存在某个定律禁止我们进行一种或多种形式的量子信息处理.可能有两方面障碍:噪声可能对有用的量子信息处理设置根本的障碍,量子力学可能是错的.

噪声无疑是开发实际量子信息处理装置的重要障碍.它是根本无法跨越,是永远阻止我们开发大规模量子信息处理装置的障碍吗?量子纠错码理论强烈暗示:尽管量子噪声是需要考虑的一个实际问题,但它并不造成根本问题.特别地,量子计算有一个阈值定理(threshold theorem),粗略讲,就是如果量子噪声水平可以降到某个固定的阈值以下,量子纠错码就可以进一步,本质上无限地使它下降,而仅仅增加一点计算复杂性.阈值定理对量子计算机中噪声的幅度和性质,以及进行量子计算的结构体系作了一些一般性假定.不过,如果这些假定得到满足,量子噪声的影响本质上在量子信息处理中可以忽略.

妨碍量子信息处理的第二种可能性是假如量子力学不正确.的确,探索量子力学(相对论和非相对论)的正确性是对建造量子信息处理装置感兴趣的一个原因,我们以前从来没有探索过这样的自然领域,在这个领域中大规模量子系统得到完全控制.或许,自然界在这个领域会显示出量子力学也不足以解释的新的令人吃惊的现象,果真如此,那将成为科学史上的重大发现,可以预期会像量子力学的发现那样,对其他科学技术领域产生相当大的影响.这样的发现,也可能影响量子计算与量子信息的研究.然而,事先无法预料,这个冲击是加强、减弱或不影响量子信息处理的能力.直到也只有等到这些效应被发现,才能得知它们如何影响信息处理,所以在本书下面的部分,我们基于迄今为止的全部证据,假定量子力学就是世界的完整和正确的描述.

即便建造量子信息处理装置没有根本的障碍,为什么一定要花无数的时间和金钱来试图这样做?事实上,我们已经提到想这样做的理由:量子密码系统和分解大的合数的因子的实际应用;获得对自然界和信息处理根本认识的愿望等.

这些都是投入时间和金钱来建造量子信息处理装置的很好的理由.但是,平心而论,我们需要量子和经典信息处理的相对能力的更清晰的图像,以评价它们的优缺点,为此,需要对量子计算与量子信息基础的进一步的理论研究,对问题"量子计算机是否比经典计算机更强大"的肯定回答是特别有意义的.即使这个问题的答案目前还不清楚,但有一条处于不同复杂层次上的重要应用的思路,对旨在实现量子

信息处理的研究人员是有帮助的.历史上,使用中短期目标作为达成长期目标的阶梯,常常能加速技术上的进步,如微处理器最初被用作电梯和其他简单装置的控制器,然后逐渐成为个人计算机(以后谁也不知道它会是什么)的基本元件.下面就为对达到大规模量子信息处理的长期目标感兴趣的人们勾画中短期目标的发展道路.

我们知道量子计算与量子信息有多得惊人的小规模应用,它们并不都像量子因子分解算法那样耀眼,但小规模算法易实现,使它们成为极重要的中期目标.

量子状态和量子过程的层析(tomography)是量子计算与量子信息中非常重要的过程,本身具有独立的价值.量子状态层析是确定系统量子状态的一种方法,为此,必须要战胜量子状态的隐含性质,即可以记住状态但无法用测量直接确定,所以要通过反复制备相同的量子状态,以便以不同方式测量,并建立量子状态的完整描述.量子过程层析是一个目标更高的(但密切相关的)过程,它要完整刻画量子系统的动态特性.量子过程层析能够用于刻画特定量子门的性能或量子通信的信道,或确定系统中噪声的类型和幅度.除了在量子计算与量子信息中的明显应用,量子过程层析还可作为诊断工具,在任何量子效应很重要的科学和技术领域中,帮助评价和提高原有的操作.

各种小规模的通信的原型研究也非常有意义,如量子密码系统和量子隐形传态,前者能应用在少量高度机密、关键材料的分发中.量子隐形传态的用处还没有定论,在第 12 章我们将看到隐形传态也许是在网络上远离的节点间,在有噪声情况下,传送量子状态的极有价值的原型,想法是把注意力集中于在希望通信的节点之间分发 EPR 对.EPR 对在通信过程中可能被污染,但特殊的纠缠蒸馏(entanglement distillation)协议可以用来"清洁"EPR 对,使它们能够用于量子状态从一个位置到另一位置的隐形传态.事实上,基于纠缠蒸馏和隐形传态的协议,为无噪声量子比特通信提供了优于传统量子纠错码技术的性能.

中等规模怎样呢?中等规模量子信息处理的有前途的一个应用是量子系统的仿真.模拟哪怕只含几十个量子比特的量子系统,都会耗尽最大的超级计算机还要大的资源,简单的计算就可以说明问题.设想有一个 50 量子比特系统,为描述这样系统的状态需要 $2^{50}\approx10^{15}$ 个复幅度值,如果幅度以 128 位精度存储,则需要 256 位或 32 字节存储每个幅度值,对于总共 32×10^{15} 字节的信息,或约三万二千兆兆字节信息而言,现今的计算机的容量是远远不够的.假设 Moore 律继续有效,则相当子所期待的 21 世纪 20 年代超级计算机的存储量.90 量子比特在同样精度下,需要 32×10^{27} 字节,即使用单原子表示比特来实现,也需要几公斤(或更重)的物质.

量子仿真会多有用?看来传统方法仍会被用来确定物质的基本属性,如键的长度和基本的光谱学性质,然而,一旦很好掌握了基本属性,量子仿真会成为实验室中设计和测试新分子性质的有力工具.传统的实验室布局中包括很多种硬件,如

化学药品和探测器等，来测试分子很多种可能的设计. 在量子计算机上，所有这些硬件都可以用软件来模拟，而且很可能便宜得多，也快得多. 当然，最终的设计和测试要在真实物理系统上进行，然而，量子计算机可以在大得多范围内检查潜在的设计，并同时评价出最好的最终设计. 有趣的是，这种借助计算机进行新分子设计的尝试在经典计算机上已经展开，不过，由于在经典计算机上模拟量子力学需要巨大的计算资源，从而限制了它们的成功. 在相对不远的未来，量子计算机应该能做得好得多.

大规模应用怎样？除了按比例增大的量子仿真和量子密码系统这样的应用，已知的大规模应用相对少些：包括分解大数的因子、取离散对数和量子搜索. 对前两个应用的主要兴趣来自负面效应，因为它们将限制现有的公钥密码系统的使用（对这些问题感兴趣的数学家也许对它们有实质性的现实兴趣），所以长远来看，分解因子和离散对数不大可能有那么重要的应用. 量子搜索却可能因搜索知识的广泛应用而极为有用，我们将在第6章讨论. 真正极好的应用是许多量子信息处理的更大规模的应用，这是未来的一个重要目标.

量子信息处理潜在应用的发展的设想，如何在真实物理系统中实现？现在已经有一些几个量子比特的小规模量子信息处理装置的方案，最容易的实现是基于光学技术，即电磁辐射. 像镜子和分光仪这样的简单设备可用于操作光子，有趣的是，按需要产生单个光子是主要的困难. 实验专家选择随机地不时产生单个光子的方案，以期符合要求的事件发生，量子密码系统、超密编码、量子隐形传态都已用这种光学技术实现了. 光学技术的一个主要优点是光子是量子力学信息的高度稳定的承载者，主要缺点是光子之间不能直接相互作用. 光子的相互作用必须借助如原子的其他物质，这会增加实验的噪声和复杂性. 两个光子之间的有效相互作用本质上分成两步：光子一和原子相互作用，原子接着与光子二相互作用，形成两个光子之间相互作用的总体效果.

另一种方案是基于俘获不同类型的原子的方法：有离子阱（ion trap），其中少量带电原子被俘获于受限的空间；还有中性原子阱，将不带电原子俘获于受限的空间. 基于原子阱的量子信息处理方案用原子来存储量子比特，这种方案中也用到电磁辐射，但与我们所指的量子信息处理的光学方法大不相同. 这类方案中，光子用来操作存储于原子本身的信息，而不是作为信息存储的场所. 单量子比特量子门可以在单个原子上施加合适的电磁辐射脉冲来实现. 相邻原子可以通过（例如）启动被完成的量子门的偶极子力相互作用. 而且，邻近原子之间的相互作用的精确性质可以通过向原子施加适当的电磁辐射脉冲进行修改，使实验专家可以控制系统中特定的门，来达到某些功能. 最后，在这些系统中的量子测量可以通过早已建立的量子跃迁（quantum jump）技术完成，该技术使相对量子计算基态的测量达到极高的精度.

另一类量子信息处理的方案是基于核磁共振，常用其缩写 NMR. 这类方案把量子信息存储到一个分子的原子的核自旋中，并用电磁辐射来操作信息. 其遇到的特殊困难是，在 NMR 中不可能直接访问单个核子. 相反，大量（典型值约为 10^{15}）相同性质的分子储存在溶液中，施加电磁脉冲到样品上，使每个分子产生大致相同的反应. 把每个分子想象成一台独立的计算机，则样品包含了并行（经典意义下）运行的大量计算机. NMR 面临三方面特殊困难，使它与其他量子信息处理计划有相当大的差别. 首先，分子一般要平衡在室温，这远远超过典型的自旋翻转能，以致自旋的定向近乎完全随机，这使初态噪声超过量子信息处理所希望的程度. 如何克服这个噪声的内容将在第 7 章讲述. 第二个问题是 NMR 所能做的测量的类型正好落到除了我们想要用量子信息处理做的最一般的测量以外. 然而，对于量子信息处理的许多例子来说，NMR 的测量手段是足够了. 第三，由于 NMR 中分子无法个别寻址，你可能会问如何用适当的方式对个别的量子比特进行操作. 幸运的是，分子中的不同核子可以具有不同的性质，从而使它们可能被个别寻址，或者至少在足够精细的粒度上，允许量子计算的实质性操作.

在现有的方案中，可以找到进行大规模量子信息处理所要求的许多基本要素：离子阱中小数目量子比特上可以进行极好的状态设置和量子测量；用 NMR 可以在小分子上展示极好的动态；固体系统的制造技术允许规模按比例增长到非常大. 从具备所有这些要素的单个系统发展到梦想中的量子计算机的道路漫长. 不幸的是，所有这些系统都很不相同，我们还需要很多很多年才能拥有量子计算机. 然而，我们相信这些性质在现有系统（虽然是在不同的系统）中的存在，确实预示着大规模量子信息处理器在长远未来的存在性，而且，它也暗示着把两种或更多当前技术结合起来，寻找混合设计的尝试有很大优越性. 例如，正在进行的将原子俘获到电磁空腔（electromagnetic cavity）中，这使我们能够通过光学技术对空腔中的原子进行灵活操作，用在传统原子阱中无法实现的方式使单个原子的实时反馈控制成为可能.

最后，注意不要把量子信息处理看成好像仅仅是信息处理的另一项技术是重要的. 例如，很容易把量子计算当作不过是另一种计算机演化过程中的会过时的时髦技术而拒绝它，像许多已经过时的时髦技术那样，比如磁泡内存在 20 世纪 80 年代初期，被广泛吹捧为内存领域的未来的重大进展. 这是一个错误，因为量子计算是信息处理的一个抽象模型，在技术上可以有许多不同的实现. 人们可以对量子计算的两种方案在技术上的优缺点进行比较，比较“好”的和“不好”的方案是有意义的，然而，即使是量子计算机的一个非常精糙的设计，也和经典计算机的最好的设计之间存在本质差别.

1.6　量 子 信 息

量子信息一词在量子计算与量子信息的研究中有两种不同用途. 第一个用途是可以被解释为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,这包括诸如量子计算、量子隐形传态、不可克隆原理和本书其他全部内容.

量子信息的第二个用途要专门得多,指对量子信息处理基本任务的研究. 一般不包括比如量子算法设计的内容,因为特殊量子算法的细节超出了基本的范围. 为避免混淆,我们用量子信息论来指这个更专门的领域,与经典领域中广泛使用的术语(经典)信息论相对应. 当然,量子信息论一词,有它自身的缺点,看起来好像只关心理论问题. 当然,事实并非如此. 基本过程的实验演示在量子信息论的研究中有很大意义.

本节的目的是引入量子信息论的基本思想. 即使限于量子信息处理的基本任务,对初学者来说,量子信息论内容仍是纷繁的,包括许多表面互不相关的,但统一在量子信息论题目下的主题. 部分原因是这个方向还在发展中,也不太清楚怎样把所有部分联系起来,然而,我们能够认识到统一量子信息论的研究的一些基本目标:

(1) 确定量子力学静态资源的基本类型. 量子比特就是一个例子. 另一个例子是比特;因为经典物理学作为量子物理学的特例,经典信息论中的基本静态资源与量子信息论有很大关系也就不足为奇. 另一静态资源的基本类型的例子是在分开双方之间共享的 Bell 态.

(2) 确定量子力学动态过程的基本类型. 一个简单的例子是内存,在一段时间内能够存储量子状态. 更加不平凡的过程是 Alice 和 Bob 双方的量子信息传输,复制(或试图复制)量子状态,以及保护量子信息不受噪声干扰.

(3) 基本动态过程进行中资源量化的折衷. 例如,使用带噪声的信道在双方之间可靠传送量子信息所需要的最少资源是什么?

经典信息论定义了类似的目标,然而,量子信息论比经典信息论范围更宽,因为量子信息论包含经典信息论的所有动态、静态要素,同时还有附加的动静态要素.

本节的剩余部分给出量子信息论研究问题的一些例子,每个例子当中,强调所考虑的基本动静态要素,也考虑资源的折衷. 我们从经典信息理论家非常熟悉的例子开始:通过量子信道传送经典信息. 然后我们分别介绍量子力学中出现的新的动静态过程,如量子纠错、区分量子态问题和纠缠变换. 本章的结束是,对如何把量子信息论工具应用到量子计算与量子信息研究的其他方面的一些思考.

1.6.1 量子信息论：例子问题

1. 通过量子信道的经典信息

经典信息论的基本结果是 Shannon 的无噪声信道编码定理和 Shannon 的带噪声信道编码定理. 无噪声信道编码定理定量给出存储信源发送的信息需要多少比特数；而带噪声信道编码定理给出通过一个带噪声信道多少信息可以被可靠传输.

信源(information source)指什么？定义这个概念是经典和量子信息论的一个基本问题，我们还会多次重新考察这个问题. 现在，我们采用一个临时性的定义：经典信源是一组概率 $p_j, j=1,2,\cdots,d$. 每使用一次信源，就独立地以概率 p_j 随机发出一个字母 j. 比如，如果信源是关于英文文本的，那么数目 j 可能就对应于字母表和标点，而概率 p_j 给出在正规英文文本中不同字母出现的相对频率. 尽管英语中字母的出现并不是独立的，但就我们的目的而言，这是个足够好的近似.

普通的英文文本包含了大量的冗余，可以利用冗余来压缩文本. 例如，普通英文文本中字母“e”远比字母“z”出现得频繁，压缩英文文本的一个简单方案就是用较表示字母“z”少的比特数表示字母“e”，Shannon 的无噪声信道编码定理精确给出一个压缩方案最好能做到什么程度. 确切地说，无噪声信道编码定理告诉我们，以概率 p_j 描述的经典信源可以压缩到信源的每次使用可以用平均 $H(p_j)$ 比特的信息代表，其中 $H(p_j) \equiv -\sum_j p_j \log(p_j)$ 是信源概率分布函数，称为 Shannon 熵(Shannon entropy). 进而，无噪声信道编码定理告诉我们，企图用比这更少的比特数代表信源在信息被解压缩时将会导致很高的错误概率.

Shannon 的无噪声信道编码定理是满足前面列出的信息论所有目标的一个很好的例子. 确定了两个静态资源(目标 1)：比特和信源. 确定了一个两阶段动态过程(目标 2)：压缩信源，而后解压缩恢复信源. 最后，通过最优数据压缩方案，找到确定消耗资源的定量准则.

Shannon 的第二个主要结果，带噪声信道编码定理，定量给出通过带噪声信道能可靠传输信息的量. 特别地，假设希望通过带噪声信道，把由某个信源产生的信息传送到其他地方，那个地方可能是空间上的另一点，或时间上的另一点——后一情况是噪声条件下存储信息的问题. 两种情况下的基本思想都是采用纠错码来对被产生的信息进行编码，以便在信道的另一端可以纠正信道引入的任何噪声. 纠错码做到这一点的方法是，向要在信道上传送的信息中引入足够多的冗余，以便在部分信息被污染后，仍能恢复原始消息. 比方说，带噪声信道要传送单个比特，而信道中的噪声要求，若要可靠传输，则每个由信源产生的比特在进入信道之前，必须用两个比特对其进行编码. 我们就说，这个信道具有半比特的容量，因为每次信道的

使用可以可靠传输半个比特的信息. Shannon 的带噪声信道编码定理为任意带噪声信道提供了计算其容量的通用程序.

Shannon 的带噪声信道编码定理也达到前述信息论的三个目标. 涉及两类静态资源(目标 1),信源和通过信道发送的比特. 涉及三个动态过程(目标 2). 最基本的过程是信道噪声,为克服噪声,进行纠错码的对偶编码和解码过程. 对于固定的噪声模型,如果要进行可靠信息传输,Shannon 定理通过最优纠错方案告诉我们必须引入多少冗余(目标 3).

对无噪声和带噪声信道编码定理,Shannon 只考虑了存储经典系统中信源的输出问题,比特和类似的东西. 量子信息论的一个自然问题就是,如果改变信息的存储介质,通过量子状态传送经典信息会发生什么. 比如,Alice 也许希望压缩某信源产生的经典信息,并把压缩的信息传给 Bob,Bob 接着把它解压缩. 如果存储压缩信息的介质是量子态,那么 Shannon 的无噪声信道编码定理就不能用于确定最优的编解码方案. 你也许有疑问,量子比特是否允许比经典情况有更好的压缩率? 我们将在第 12 章研究这个问题,并证明,事实上,量子比特节省不了多少在无噪声信道上需要传输的信息量.

很自然地,下一步是考虑在带噪声的量子信道上传输经典信息的问题. 在理想情况下,我们希望得到定量给出这样的信道传输信息容量的结果. 由于各种原因,估计容量是件技巧性很强的工作. 量子力学允许不同类型的噪声模型,因为它是在连续空间中,并且采用经典纠错技术来对抗噪声根本就不明显. 比如说,把经典信息用纠缠态进行编码,然后在带噪声信道中分次传送有好处吗? 或者用纠缠测量来解码有好处吗? 第 12 章我们将证明 HSW(Holevo-Schumacher-Westmoreland)定理,给出此类信道容量下界的一个估计. 事实上,一般相信 HSW 定理给出了容量的准确值,尽管还不知道完整的证明. 剩下的一个问题是,是否可以用纠缠态编码使容量超过 HSW 定理所提供的下界值. 迄今为止的所有证据暗示,这无助于提高容量,但判定这个猜想的真伪,仍是量子信息论的一个热门的未解决的问题.

2. 通过量子信道的量子信息

经典信息当然不是量子力学中惟一的静态资源,量子态自身就是一类静态自然资源,甚至比经典信息来得更自然. 我们来考察 Shannon 编码定理的不同的量子类比,这次涉及量子状态的压缩和解压缩.

首先相应于信源的经典定义,我们需要定义信源的某种量子含义. 像经典的情况那样,有几种不同的方法,但为确定起见,我们采用临时的定义,把量子信源描述为一组概率 p_i 和相应的量子状态 $|\psi_i\rangle$,每次使用信源都独立地以概率 p_i 产生 $|\psi_i\rangle$.

对这样的量子机制,信源产生的输出可以进行压缩吗? 考虑以概率 p 输出状

态$|0\rangle$和以概率$1-p$输出状态$|1\rangle$的单量子比特源，这在本质上与以概率p输出0和以概率$1-p$输出1产生单比特的经典信源相同. 于是采用相似的技术，把量子信源压缩到只用$H(p,1-p)$量子比特存储信源就不足为奇了，这里$H(\cdot)$是Shannon熵函数.

若信源以p产生状态$|0\rangle$和以概率$1-p$产生状态$(|0\rangle+|1\rangle)/\sqrt{2}$情况怎样？经典的压缩技术不再适用，因为一般而言，我们无法区分状态$|0\rangle$和$(|0\rangle+|1\rangle)/\sqrt{2}$. 仍有可能进行某种类型的压缩操作吗？

事实上，即使对于此例，一类压缩仍是可能的. 有趣的是，源产生的量子状态在经过压缩和解压缩过程后可能有微小变化，在这种意义下，压缩不再是无差错的，不过，我们要求这种变化应该非常小，在大量成组被压缩的信源输出的极限情况下是可以忽略的. 为定量化误差，我们用保真度(fidelity)来度量压缩方案，量测压缩引起的平均误差. 量子数据压缩的理论根据是被压缩数据能够以好的保真度恢复，把保真度看作类似于进行正确解压缩的概率，在块长度大的极限情况下，它的值应该趋向无误差的极限1.

Schumacher的无噪声信道编码定理定量给出在能以接近1的保真度恢复信源的约束下量子数据压缩需要的资源. 在信源以概率p_j产生正交量子状态$|\psi_j\rangle$的情形下，Schumacher定理退化为信源可以压缩到但不会超过经典极限$H(p_j)$. 然而，更一般的信源产生非正交状态情形，Schumacher定理告诉我们量子信源可以压缩多少，答案不是Shannon熵$H(p_j)$，而是一个新的熵，von Neumann熵. von Neumann熵才是正确答案. 一般地，当且仅当状态$|\psi_j\rangle$正交时，von Neumann熵与Shannon熵一致，否则针对$p_j,|\psi_j\rangle$的von Neumann熵严格小于Shannon熵$H(p_j)$. 例如，一个信源以概率p产生状态$|0\rangle$，且以概率$1-p$产生$(|0\rangle+|1\rangle)/\sqrt{2}$，信源的每次使用都可用少于$H(p,1-p)$量子比特来可靠压缩.

这种资源需要的减少直观上很容易理解. 设以概率p产生状态$|0\rangle$，且以概率$1-p$产生$(|0\rangle+|1\rangle)/\sqrt{2}$的信源使用了$n$次，由大数律，信源以很高的概率产生约$np$个$|0\rangle$的备份和$n(1-p)$个$(|0\rangle+|1\rangle)/\sqrt{2}$的备份，即不计重新排序，有形式

$$|0\rangle^{\otimes np}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n(1-p)} \tag{1.60}$$

假设我们要展开右边的$|0\rangle+|1\rangle$乘积项. 因为$n(1-p)$是个大数，再次利用大数律，可推断乘积项中$|0\rangle$和$|1\rangle$约各占一半，也就是说$|0\rangle+|1\rangle$乘积可以用一个如下形式的叠加态来近似

$$|0\rangle^{\otimes n(1-p)/2}|1\rangle^{\otimes n(1-p)/2} \tag{1.61}$$

于是信源产生的状态可以作为如下形式的叠加近似

$$|0\rangle^{\otimes n(1+p)/2}|1\rangle^{\otimes n(1-p)/2} \tag{1.62}$$

这个形式中有多少状态？大约为 n 中取 $n(1+p)/2$ 的组合数，根据 Stirling 近似，约等于 $N=2^{nH[(1-p)/2,(1-p)/2]}$. 压缩的一个简单办法是把式(1.62)形式的全部状态从 $|c_1\rangle$ 到 $|c_N\rangle$ 进行标号. 因为 j 是一个 $nH[(1-p)/2,(1-p)/2]$ 比特的数，所以可以对信源产生的 n 量子比特进行酉变换，把 $|c_j\rangle$ 变为 $|j\rangle|0\rangle^{n-nH[(1+p)/2,(1-p)/2]}$. 压缩操作就是先进行这个酉变换，再舍弃最后的 $n-nH[(1+p)/2,(1-p)/2]$ 量子比特，使压缩后的状态具有 $nH[(1+p)/2,(1-p)/2]$ 量子比特. 为解压缩，我们在压缩状态上添加状态 $|0\rangle^{n-nH[(1+p)/2,(1-p)/2]}$，并进行逆酉变换.

这个量子数据压缩和解压缩的过程导致每次使用信源需要存储 $H[(1+p)/2,(1-p)/2]$ 量子比特. 当 $p\geqslant 1/3$ 时这个数比起 $H(p,1-p)$ 量子比特来是一个改良，$H(p,1-p)$ 是我们可以从 Shannon 无噪声信道编码定理自然地期望的. 事实上，Schumacher 的无噪声信道编码定理可以使我们做得更好，不过那里结构的本质理由却和这里能够进行压缩的理由相同：我们利用了 $|0\rangle$ 和 $(|0\rangle+|1\rangle)/\sqrt{2}$ 非正交的事实. 直观上讲，状态包含某种冗余，因为都在 $|0\rangle$ 方向上有分量，导致在物理上比正交状态更具相似性. 在编码方案中我们正是利用了这种冗余性，而它也被用到了 Schumacher 的无噪声信道编码定理的完整证明中. 注意，因为当 $p<1/3$ 时，这种特别的方案没有利用状态的冗余，所以有 $p\geqslant 1/3$ 的限制，其结果是增加了问题中的冗余. 当然，这里采用的特殊方案是较随意的，通用解决方案以更加切合实际的方式利用冗余达到数据压缩.

在量子状态的压缩和解压缩上，Schumacher 的无噪声信道编码定理与 Shannon 无噪声信道编码定理相对应，有与 Shannon 带噪声信道编码定理相对应的结果吗？利用量子纠错码理论，在这个重要问题上已取得很大进展，不过，尚未得到完全令人满意的相应结果.

3. 量子的不可区分性

到现在为止，我们考虑的所有动态过程——压缩、解压缩、噪声、纠错码的编码和解码——都来自经典和量子信息论，然而，量子状态等新类型信息的引入，使动态过程的种类扩大到经典信息论范围以外，如区分量子状态的问题. 经典情况下，我们习惯于至少原则上能够区分信息的不同项. 当然，实际中纸上被污染的字母“a”很难和字母“o”相区分，但从根本上说，完全肯定地区分两种是可能的.

另一方面，对量子力学而言在任意状态之间做出区分却不总是可能的. 例如，量子力学上不存在可靠区分状态 $|0\rangle$ 和 $(|0\rangle+|1\rangle)/\sqrt{2}$ 的过程. 要证明这一点需要用到还未讲到的工具(在第 2 章)，但通过例子很容易使人相信这确实是不可能的. 例如，假设我们试图通过相对基的测量来区分这两个状态，那么，如果状态是 $|0\rangle$，测量将以概率 1 得到 0，然而，当我们测量 $(|0\rangle+|1\rangle)/\sqrt{2}$ 时，以 1/2 概率得到 0，以 1/2 概率得到 1. 于是，测到一个 1 意味着状态一定是 $(|0\rangle-|1\rangle)/\sqrt{2}$，因为它不可

能是$|0\rangle$，但是从得到的0结果，我们无法得出关于量子状态任何有用的结论.

非正交量子状态的这种不可区分性是量子计算与量子信息的核心概念，它是关于量子状态包含测量无法访问的隐含信息断言的根本，因此在量子算法和量子密码系统中扮演关键角色. 量子信息论的一个中心问题就是，研究如何定量度量非正交量子状态的可区分程度，在本引论中，我们只是指出不可区分性的两个有趣侧面——与超光速通信的联系和在量子货币方面的应用.

暂且假想我们可以区分任何量子状态，这意味着运用纠缠现象，可获得超光速通信的能力. 假设Alice和Bob共享一对纠缠的处于状态$(|00\rangle+|11\rangle)/\sqrt{2}$的量子比特，如果Alice在基中测量，测后状态就以概率1/2得$|00\rangle$，以概率1/2得$|11\rangle$，这样Bob的系统状态就以1/2概率得$|0\rangle$，1/2概率得$|1\rangle$. 然而假设Alice是相对基$|+\rangle,|-\rangle$测量的，这里回想一下$|0\rangle=(|+\rangle+|-\rangle)/\sqrt{2}$，$|1\rangle=(|+\rangle-|-\rangle)/\sqrt{2}$，经过简单计算可以把Alice和Bob的状态重写作$(|++\rangle+|--\rangle)/\sqrt{2}$. 进而，如果Alice在基$|+\rangle,|-\rangle$中测量，Bob的系统状态就分别以1/2概率为$|+\rangle$或$|-\rangle$. 到此为止还都是基本的量子力学运算. 但如果Bob有一台设备可以区分$|0\rangle,|1\rangle,|+\rangle,|-\rangle$四个状态，那么他就知道Alice测量是针对计算基还是针对基$|+\rangle,|-\rangle$进行的. 更重要的是，只要Alice完成了测量，他就可以在瞬间得到这个信息，这为Alice和Bob提供了超光速通信的手段. 当然，我们知道非正交量子状态是无法区分的，这个例子显示这条限制与我们希望自然服从的其他物理性质密切相关.

非正交量子状态的不可区分性不一定总是对我们不利，有时它是有用的. 设想一家银行发行钞票，印有(经典的)序列号和状态为$|0\rangle$或$(|0\rangle+|1\rangle)/\sqrt{2}\rangle$的一个量子比特序列，除了银行没有人知道钞票中这个双态序列是什么，银行保存着与嵌入状态匹配的序列号的列表. 这种钞票是无法精确伪造的，因为在不毁掉原始钞票的情况下，伪造者无法确切知道量子比特的状态. 当商家(信誉可信赖的)收到钞票时，通过与银行联系，告诉银行序列号，再询问嵌入钞票的状态序列，就可以验证它是否是伪造的，他们可以按银行指示在$|0\rangle,|1\rangle$或$(|0\rangle+|1\rangle)/\sqrt{2},(|0\rangle-|1\rangle)/\sqrt{2}$基中来测量量子比特以判别真伪. 以伴随检测量子比特数目指数速度增长到1的概率，任何可能的伪造都会在这个阶段被检测到. 这个思想是其他无数量子密码协议的基础，并展示了非正交量子状态的不可区分性的用途.

练习1.2 如果把两个非正交量子状态$|\psi\rangle$或$|\varphi\rangle$之一输入到一个装置，该装置能够正确识别之，试说明如何利用该装置建造一个可以克隆$|\psi\rangle$和$|\varphi\rangle$的装置，这就违反了不可克隆定理. 反过来，说明如何把克隆设备用于区分非正交量子状态.

4. 纠缠现象的产生和变换

纠缠现象是量子力学中另一类基本的静态资源. 它的性质与经典信息论中熟悉的资源之间存在惊人差异，而这些性质尚未被完全认识. 我们关于纠缠现象的结果最多非常初步，还不具备明白问题答案所需的全部术语，但我们至少可以先来看一下与纠缠现象有关的两个信息论问题.

产生纠缠现象的过程是量子信息论感兴趣的一个简单动态过程. 假设事先没有共享任何纠缠，双方需要交换多少量子比特以建立彼此共享的一个特殊纠缠状态？第二个感兴趣的动态过程是把纠缠从一种形式变成另一种形式的纠缠变换. 比方说假设 Alice 和 Bob 之间共享一个 Bell 态，希望把它变成其他类型的纠缠态，他们需要什么样的资源来做这件事？他们可以在不通信的情况下完成吗？仅仅采用经典通信能完成吗？如果需要量子通信，又需要多少量子通信呢？

回答这些问题，以及关于纠缠产生和变换的更复杂问题形成了独立的迷人领域，同时有望为完成包括量子计算在内的任务带来启发. 例如，分布式量子计算可以简单地看作在双方或多方之间生成纠缠的一个种方法，完成分布式量子计算的通信量的下界就可以从为创建相应纠缠态需要的通信量的下界导出.

1.6.2　更一般背景下的量子信息

我们对量子信息论作了最简要的介绍. 本书第三部分将会对量子信息论作深入得多的讨论，特别是第 11 章，包括量子和经典信息论中熵的基本属性，第 12 章集中于纯粹的量子信息理论.

量子信息论是量子计算与量子信息中最抽象的部分，但某种意义上说它又是最基本的. 推动量子信息论，最终是量子计算与量子信息发展的问题是，造就量子信息处理的力量是什么？是什么把量子世界和经典世界分开？什么样的资源，经典世界得不到，但被用到量子计算中？对这些问题的答案是模糊和不完整的，我们希望将来答案会清楚起来，并且能够清楚鉴别量子信息处理的潜力和限制.

问题 1.1（Feynman-Gates 对话）　虚构一段大约 2000 词的 Bill Gates 与 Richard Feynman 之间关于计算未来的友好讨论（注：你也可以在读完本书后，再回答这个问题. 参看下面的“历史和进一步阅读的材料”提供的对这个问题的一个可能回答）.

问题 1.2　量子计算与量子信息研究到目前为止，最重要的发现是什么？写一篇大约 2000 词的给受过教育的外行读者的关于这项发现的短文（注：像前一个问题一样，你可以等到读完本书再来回答这个问题）.

历史和进一步阅读的材料

本章的大多数材料在后面的章节将要更深入讨论，因此下面的历史文献和进一步阅读的材料限于后面章节不再涉及的内容.

要把量子计算与量子信息研究的历史材料完整地拼在一起，需要对许多领域的历史做全面概括. 本章试图把这些历史材料联系在一起，但由于篇幅和专业的限制，不可避免地忽略了许多背景材料. 下面推荐的材料试图作为补充.

量子力学的历史在许多地方都有讲述，我们特别推荐 Pais[Pai82, Pai86, Pai91] 的杰出著作. 这三本书中，文献[Pai86]和量子力学的发展的关系最为直接，不过，Pais 的 Einstein 传记[Pai82]和 Bohr 传记[Pai91]也包含许多有趣的材料，不过没有那么集中. Milburn[Mil97, Mil98]描述了基于量子力学的技术的兴起. Turing 关于计算机科学基础的非凡论文[Tur36]很值得阅读. 在 Davis[Dav65]，Hofstadter[Hof79]和 Penrose[Pen89]的有价值的历史性著作集中可以找到对计算机科学基础的令人愉快和富有信息的讨论. Shasha 和 Lazere 关于 15 位一流计算机科学家的传记[SL98]在计算机科学历史的许多不同方面很有启发. 最后，Knuth 的令人尊敬的系列著作[Knu97, Knu98a, Knu98b]包含了惊人数量的历史信息. Shannon 奠定信息论基础的光辉论文是很好的阅读材料[Sha48]（重印书为[SW49]）. MacWilliams 和 Sloane 的书[MS77]不仅是纠错码的优秀教科书，也包含无数有用的历史信息. 类似地，Cover 和 Thomaas 的书[CT91]是信息论的优秀教科书，也包含广泛的历史信息. Shannon 的论文集与许多有用的历史材料都收入一部由 Sloane 和 Wyner 编辑的一个大的书卷[SW93]中. Slepian[Sle74]收集了信息论方面的一组有用的预印本. 密码术是一门古老的技艺，历史错综复杂常很有趣，Kahn[Kah96]包含了密码术的大量历史信息. 为了解最新进展，我们推荐 Menezes、van Oorschot 和 Vanstone 的书[MvOV96]，Schneier 的书[Sch96a]和 Diffie 和 Landau 的书[DL98].

量子隐形传态由 Bennett、Brassard、Crépeau、Josa、Peres 和 Wootters[BBC+93]发现，后分别由 Boschi、Branca、De Martini、Hardy 和 Popescu[BBM+98]用光学技术，由 Bouwmeester、Pan、Mattlke、Eibl、Weinfurter 和 Zeilinger[BPM+97]用光子极化，由 Furusawa、Sϕrensen、Braunstein、Fuchs、Kimble 和 Polzik[FSB+98]用光的挤压态，以及由 Nielsen、Knill 和 Laflamme[NKL98]用 NMR 实现.

Deutsch 问题是由 Deutsch[Deu85]提出，在同一篇文章中给出了单比特解，n 比特的推广由 Deutsch 和 Jozsa[DJ92]给出，这些早期文章中的算法后来独立地在 Cleve、Ekert、Macchiavello 和 Mosca[CEMM98]以及 Tapp 未发表的工作中被实质性地改进. 本章我们已给出了一个该算法的改进版本，它非常符合在第 5 章将讨论的隐含子群问题的框架. Deutsch 的原始算法是随机的，Deutsch 和 Jozsa 把它改进

为确定性算法，但他们的算法需要两次计算函数值，与本章的改进算法形成对照. 不过，习惯上仍把这些算法称为 Deutsch 算法和 Deutsch-Jozsa 算法，以纪念向前跨出的两大步：Deutsch 用具体例子表明量子计算机可以比经典计算机做事快些；Deutsch 和 Jozsa 的扩展首次展示了在当时条件下求解问题所需计算规模上的类似差距.

Stern Gerlach 实验的出色讨论可在量子力学的标准教科书中找到，如 Sakurai 的书[Sak94]，Feynman、Leighton 和 Sands[FLS65a] 第三卷，以及 Cohen-Tannoudji、Diu 和 Laloë 的书[CDL77a, CDL77b].

问题 1.1 是 Rahim 的有趣文章[Rah99] 所提示的.

CHAPTER 2
第 2 章
量子力学引论

我虽不是物理学家，但我知道什么东西最重要.

——*Popeye航海家*

量子力学：科学中真正的巫术

——*Albert Einstein*

量子力学对已知世界的描述是最精确和完整的，也是理解量子计算与量子信息的基础. 本章提供透彻掌握量子计算与量子信息所需的全部量子力学背景知识，我们不假定读者有任何量子力学准备知识.

尽管有难学科目的名声，量子力学其实很容易学. 难学的印象来自某些应用中的困难，比如弄清复杂分子结构的应用，但那对掌握量子力学来说不是基本的，我们不会讨论这类应用. 惟一的预备知识是熟悉初等线性代数，如果具备这方面的背景，读者就可以开始花一些时间做出那些简单的题目，哪怕没有关子量子力学的任何准备知识.

已经熟悉量子力学的读者可以很快浏览整章内容，以熟悉我们用的符号(多数是标准的)约定，并确认已熟悉所有的材料. 基本没有基础知识的读者应该仔细学习本章内容，在练习的地方暂时停下来，并尝试去解答. 如果碰到练习上的困难，可以继续下去，到后面返回来再尝试解答.

本章从 2.1 节复习线性代数的一些内容开始. 这一节假设读者熟悉初等线性代数，但引入了物理学家在量子力学中所采用的记号，这和大多数线性代数引论中用的不同. 2.2 节给出量子力学的基本假设. 读完该节，读者就掌握了量子力学的全部基本原理，这节配了大量练习以帮助巩固对内容的理解. 本章和本书剩下的章节都是基于该节内容进行阐述，不再引入新的基本物理原理. 2.3 节解释超密编码(superdense coding)，这个简单问题的例子惊人地体现了多个量子力学原理并展示了量子信息处理的过程. 2.4 节和 2.5 节讲述有力的数学工具，密度算子、纯化(purification)和 Schmidt 分解，这些工具对量子计算与量子信息的研究特别有用，

掌握这些工具也有助于读者巩固对初等量子力学的理解. 最后,2.6 节考察量子力学如何超越通常对世界运行方式的经典理解的问题.

2.1　线 性 代 数

本书带来的烦恼不亚于所传授的知识.

——*About Vectors* 一节的第一行,*著者 Banesh Hoffmann*

人生好比复数——她既有实部又有虚部.

——*无名氏*

线性代数研究向量空间及其上的线性算子,牢固掌握初等线性代数是理解好量子力学的基础. 本节复习线性代数的一些基本概念,并给出在量子力学中使用这些概念所采用的标准记号. 这些记号总结在图 2.1 中,量子记号在左,线性代数记号在右. 读者可以浏览一下这张表,以确定知道多少右边的概念.

记　号	含　义
z^*	复数 z 的复共轭 $(1+i)^* = 1-i$
$\|\psi\rangle$	向量,又称为右态矢
$\langle\psi\|$	$\|\psi\rangle$的对偶向量,又称为左态矢
$\langle\varphi\|\psi\rangle$	向量$\|\varphi\rangle$和$\|\psi\rangle$的内积
$\|\varphi\rangle\otimes\|\psi\rangle$	$\|\varphi\rangle$和$\|\psi\rangle$的张量积
$\|\varphi\rangle\|\psi\rangle$	$\|\varphi\rangle$和$\|\psi\rangle$的张量积的缩写
A^*	矩阵 A 的复共轭
A^{T}	矩阵 A 的转置
$A^\dagger$	矩阵 A 的共轭.转置.或 Hermite 共轭,$A^\dagger=(A^{\mathrm{T}})^*$
$\langle\varphi\|A\|\psi\rangle$	向量$\|\varphi\rangle$ 和 $A\|\psi\rangle$的内积 等价地,向量 $A^\dagger\|\varphi\rangle$和 $\|\psi\rangle$的内积

图 2.1　一些线性代数概念在量子力学中的标准记号的总结. 这种风格的记号称为 Dirac 记号.

在我们看来,认同量子力学假设的主要障碍不在假设本身,而是为理解这些假设所需要的大量线性代数概念,再加上物理学家在量子力学中所采用的不常见的 Dirac 符号. 这看起来(其实不然)相当可怕. 出于这些原因,我们建议不熟悉量子力学的读者很快读完下面的材料,只是为集中理解最基本的内容才值得稍作停留. 接着就认真学习本章的主题　—量子力学基本假设——需要时再来学习必要的线性代数概念和记号.

线性代数研究的基本对象是向量空间(vector space). 我们最感兴趣的向量空间是所有 n 元复数$(z_1,\cdots,z_n)$构成的向量空间 $\mathbf{C}^n$,向量空间的元素称为向量,有时用列矩阵记号

$$\begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \tag{2.1}$$

来表示向量. 还有把向量对变成其他向量的加运算. $\mathbf{C}^n$ 上的向量加运算定义为

$$\begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} + \begin{bmatrix} z'_1 \\ \vdots \\ z'_n \end{bmatrix} = \begin{bmatrix} z_1 + z'_1 \\ \vdots \\ z_n + z'_n \end{bmatrix} \tag{2.2}$$

其中右边的加运算就是通常的复数加法. 而且向量空间中还有标量乘运算,$\mathbf{C}^n$ 上的这运算定义为

$$z\begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} zz_1 \\ \vdots \\ zz_n \end{bmatrix} \tag{2.3}$$

其中 z 是标量,即为一复数,右边的乘法是普通的复数乘法. 物理学家有时把复数称为 c-数.

我们复习线性代数的目的是描述量子力学,因此,我们用量子力学的标准记号来表述线性代数概念. 向量空间中向量的标准量子力学符号为

$$|\psi\rangle \tag{2.4}$$

其中 ψ 是该向量的标号(可以用任何标号,尽管我们更愿意用简单的标号如 ψ 和 φ),符号$|\cdot\rangle$用来表明该对象为一向量. 整个对象$|\psi\rangle$有时称为一个右态矢(ket),不过我们不常用这个术语.

向量空间包含一个特殊的零向量,记作 0. 它满足性质:对任意其他向量$|v\rangle$,都成立$|v\rangle+0=|v\rangle$. 注意我们不用右态矢的记号表示零向量,这是惟一的例外. 这个例外的原因是,零向量显然的记号$|0\rangle$,习惯上已有其他含义. 关于标量乘,对任意复数 z,有 $z0=0$. 为方便起见,我们用$(z_1,\cdots,z_n)$表示项为 $z_1,\cdots,z_n$的列矩阵. $\mathbf{C}^n$ 的零元是$(0,\cdots,0)$. 向量空间 V 的一个向量子空间是 V 的一个子集 W,满足:W 也构成一个向量空间,即 W 必须对标量乘和加运算封闭.

2.1.1 基与线性无关

向量空间的一个生成集(spanning set)是一组向量$|v_1\rangle,\cdots,|v_n\rangle$,它使得向量空间中的任意向量$|v\rangle$都能表示成该组中向量的线性组合 $|v\rangle=\sum_i a_i|v_i\rangle$. 例如,向量空间 $\mathbf{C}^2$ 的一个生成集是

$$|v_1\rangle \equiv \begin{bmatrix}1\\0\end{bmatrix}, \quad |v_2\rangle \equiv \begin{bmatrix}0\\1\end{bmatrix} \tag{2.5}$$

因为 $\mathbf{C}^2$ 中任意向量

$$|v\rangle = \begin{bmatrix}a_1\\a_2\end{bmatrix} \tag{2.6}$$

都可以写成 $|v_1\rangle$ 和 $|v_2\rangle$ 的线性组合 $|v\rangle = a_1|v_1\rangle + a_2|v_2\rangle$，于是我们说 $|v_1\rangle$ 和 $|v_2\rangle$ 张成(span)向量空间 $\mathbf{C}^2$.

一般地，向量空间可能有许多不同的生成集. 向量空间 $\mathbf{C}^2$ 的另一生成集是

$$|v_1\rangle \equiv \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, \quad |v_2\rangle \equiv \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} \tag{2.7}$$

因为任意的向量 $|v\rangle = (a_1, a_2)$ 可以写成 $|v_1\rangle$ 和 $|v_2\rangle$ 的线性组合，

$$|v\rangle = \frac{a_1 + a_2}{2}|v_1\rangle + \frac{a_1 - a_2}{2}|v_2\rangle \tag{2.8}$$

一组非零向量 $|v_1\rangle, \cdots, |v_n\rangle$ 是线性相关的，如果存在一组复数 $a_1, \cdots, a_n$，其中至少对一个 i 有 $a_i \neq 0$，

$$a_1|v_1\rangle + a_2|v_2\rangle + \cdots + a_n|v_n\rangle = 0 \tag{2.9}$$

成立. 如果一组向量不是线性相关的，则是线性无关的. 可以证明任意两个线性无关向量组如果都是向量空间 V 的生成集，则必包含相等数目的元素. 我们称这样的向量组为 V 的一个基，而且，这样的基总是存在的. 基包含向量的数目称为 V 的维数. 本书只对有限维向量空间感兴趣，无穷维向量空间有许多有趣和困难的问题，但我们不需要关心这些问题.

练习 2.1(例子线性相关)　证明(1，-1)，(1，2)和(2，1)是线性相关的.

2.1.2　线性算子与矩阵

向量空间 V 和 W 之间的线性算子(linear operator)定义为，任意对输入是线性的函数 $A: V \to W$，满足：

$$A\left(\sum_i a_i|\psi\rangle\right) = \sum_i a_i A(|\psi\rangle) \tag{2.10}$$

通常把 $A(|v\rangle)$ 记作 $A|v\rangle$. 当我们说一个线性算子 A 定义在向量空间 V 上时，指 A 是从 V 到 V 的线性算子. 恒等算子(identity operator) I_V 是任意线性空间 V 上的一个重要的线性算子，定义为对所有向量 $|v\rangle$ 有等式 $I_V|v\rangle = |v\rangle$. 只要不引起混淆，我们就省略 V，而只用 I 表示恒等算子. 另一重要算子是零算子，记作 0. 零算子把所有向量映为零向量，$0|v\rangle = 0$. 从式(2.10)易知，一旦确定了线性算子 A 在一基上的作用，A 在所有输入上的作用就完全被确定了.

设 V，W 和 X 是向量空间，而 $A: V \to W$ 和 $B: W \to X$ 是线性算子，用记号 BA

表示 B 和 A 的复合，定义为 $(BA)(|v\rangle)\equiv B(A(|v\rangle))$，$(BA)(|v\rangle)$. 简记为 $BA|v\rangle$.

理解线性算子最方便的途径是通过它们的矩阵表示(matrix representation). 事实上，线性算子和矩阵是完全等价的，不过读者可能更熟悉矩阵. 为明确二者的联系，首先要知道 $m\times n$ 阶，以 A_{ij} 为元素的矩阵 A 在同 C^n 向量进行矩阵乘法时，实际上是把 C^n 向量转移到 C^m 的一个线性算子. 更确切地，矩阵 A 是线性算子的断言意味着

$$A\sum_i a_i|\psi\rangle=\sum_i a_i A|\psi\rangle \tag{2.11}$$

其等式的作用是 A 和列向量的矩阵乘积，很显然这是对的.

我们已看到矩阵可以被视为线性算子，但能给出线性算子的一个矩阵表示吗？的确可以，我们就来说明这一点. 这个两种观点之间的等价性让我们在本书中可以互换使用矩阵和算子理论的术语. 设 A：$V\to W$ 是向量空间 V 和 W 之间的一个线性算子，设 $|v_1\rangle,\cdots,|v_m\rangle$ 是 V 的一个基，而 $|w_1\rangle,\cdots,|w_n\rangle$ 是 W 的一个基. 于是对 $1,\cdots,m$ 中每个 j，存在复数 A_{1j} 到 A_{nj}，使

$$A|v_j\rangle=\sum_i A_{ij}|w_i\rangle \tag{2.12}$$

具有元素 A_{ij} 的矩阵称为算子 A 的一个矩阵表示. A 的这个矩阵表示的说法与算子 A 的说法完全等价，我们将交替使用矩阵表示和抽象算子观点. 注意为把矩阵和线性算子联系起来，我们需要为线性算子的输入和输出向量空间指定基.

练习 2.2(矩阵表示例子) 设 V 是以 $|0\rangle$ 和 $|1\rangle$ 为基向量的向量空间，A 是从 V 到 V 的线性算子，使 $A|0\rangle=|1\rangle$，$A|1\rangle=|0\rangle$. 给出 A 相对于输入基 $|0\rangle$，$|1\rangle$ 和输出基 $|0\rangle$，$|1\rangle$ 的矩阵表示，找出使 A 具有不同矩阵表示的输入输出基.

练习 2.3(算子乘积的矩阵表示) 设 A 是从向量空间 V 到向量空间 W 的线性算子，B 是从向量空间 W 到向量空间 X 的线性算子，令 $|v_i\rangle$，$|w_j\rangle$ 和 $|x_k\rangle$ 分别为向量空间 V，W 和 X 的基. 证明线性变换 BA 的矩阵表示就是 B 和 A 在相应基下矩阵表示的矩阵乘积.

练习 2.4(恒等算子的矩阵表示) 证明如果输入和输出空间取相同的基，向量空间 V 上的恒等算子的矩阵表示中，对角线为 1 而其他元素为 0，这种矩阵称为单位阵(identity matrix).

2.1.3 Pauli 阵

Pauli 阵指四个常用矩阵，它们是 2×2 矩阵，并各有记号，图 2.2 给出了这些矩阵和相应的符号. Pauli 阵对量子计算与量子信息极有用，我们鼓励读者通过后面的例子和练习记住它们.

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \sigma \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

图 2.2　Pauli 阵. 有时会从列表中省去 I, 而只把 X, Y 和 Z 称为 Pauli 阵.

2.1.4　内积

内积是向量空间上的二元复数函数. 两个向量 $|v\rangle$ 和 $|w\rangle$ 的内积是一个复数，暂且把 $|v\rangle$ 和 $|w\rangle$ 的内积写成 $(|v\rangle, |w\rangle)$. 这并不是量子力学的标准记号，为表述上的清晰性，本章偶尔会用到 $(\cdot,\cdot)$ 的记号. 内积 $(|v\rangle, |w\rangle)$ 在量子力学中的标准符号为 $\langle v|w\rangle$，其中 $|v\rangle$ 和 $|w\rangle$ 是内积空间中的向量，符号 $\langle v|$ 表示向量 $|v\rangle$ 的对偶向量. 对偶运算是从内积空间 V 到复数 $\mathbf{C}$ 的一个线性算子，很快就会看到，对偶向量的矩阵表示正是行向量.

从 $V\times V$ 到 $\mathbf{C}$ 的函数 $(\cdot,\cdot)$ 是内积，如果它满足以下条件：

(1) $(\cdot,\cdot)$ 对第二个自变量是线性的，即

$$\left(|v\rangle, \sum_i \lambda_i |w_i\rangle\right) = \sum_i \lambda_i (|v\rangle, |w_i\rangle) \tag{2.13}$$

(2) $(|v\rangle, |w\rangle) = (|w\rangle, |v\rangle)^*$

(3) $(|v\rangle, |v\rangle) \geqslant 0$，当且仅当 $|v\rangle = 0$ 时取等号.

例如，$\mathbf{C}^n$ 具有如下定义的一个内积：

$$((y_1,\cdots,y_n),(z_1,\cdots,z_n)) \equiv \sum_i y_i^* z_i = \begin{bmatrix} y_1^* & \cdots & y_n^* \end{bmatrix} \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \tag{2.14}$$

带有内积的向量空间称为内积空间.

练习 2.5　验证 $(\cdot,\cdot)$ 定义了 $\mathbf{C}^n$ 上的一个内积.

练习 2.6　证明任意内积 $(\cdot,\cdot)$ 对第一个自变量都是共轭线性的

$$\left(\sum_i \lambda_i |w_i\rangle, |v\rangle\right) = \sum_i \lambda_i^* (|w_i\rangle, |v\rangle) \tag{2.15}$$

量子力学的讨论常提到 Hilbert 空间. 在量子计算与量子信息中遇到的有限维数复向量空间类中，Hilbert 空间与内积空间完全是一回事. 从现在起，我们就不加区分地使用这两个术语，更倾向于使用 Hilbert 空间的说法. 无穷维 Hilbert 空间在内积空间基础上要求满足附加的技术性限制，我们可不考虑这种情况.

如果向量 $|v\rangle$ 和 $|w\rangle$ 的内积为 0，则称它们为正交(orthogonal). 例如，$|w\rangle \equiv (1,0)$ 和 $|v\rangle \equiv (0,1)$ 相对于式(2.14)式定义的内积是正交的. 定义向量 $|v\rangle$ 的范数(norm)为

$$\| \, |v\rangle \, \| \equiv \sqrt{\langle v \mid v \rangle} \tag{2.16}$$

向量$|v\rangle$是单位向量(unit vector),如果满足$\| \, |v\rangle \, \| = 1$. 如果$\| \, |v\rangle \, \| = 1$,还称向量$|v\rangle$为归一化的(normalized). 对任意非零向量$|v\rangle$,向量除以其范数,称为向量的归一化,即$|v\rangle / \| \, |v\rangle \, \|$是$|v\rangle$的归一化形式. 一组以$i$为指标的向量$|i\rangle$称为标准正交(orthonormal)向量组,如果每个向量都是单位向量,不同向量之间正交,即$\langle i|j\rangle = \delta_{ij}$,其中$i$和$j$都是从指标集中取的.

练习 2.7 验证$|w\rangle \equiv (1,1)$和$|v\rangle \equiv (1,-1)$正交. 这些向量的归一化形式是什么?

设$|w_1\rangle, \cdots, |w_d\rangle$是某内积空间$V$的一个基,通过使用 Gram-Schmidt 过程的方法,能产生向量空间V的一组标准正交基$|v_1\rangle, \cdots, |v_d\rangle$. 定义$|v_1\rangle \equiv |w_1\rangle / \| \, |w_1\rangle \, \|$,且对$1 \leqslant k \leqslant d-1$,递归地定义$|v_{k+1}\rangle$为

$$|v_{k+1}\rangle \equiv \frac{|w_{k+1}\rangle - \sum_{i=1}^{k} \langle v_i \mid w_{k+1} \rangle \, |v_i\rangle}{\| \, |w_{k+1}\rangle - \sum_{i=1}^{k} \langle v_i \mid w_{k+1} \rangle \, |v_i\rangle \, \|} \tag{2.17}$$

不难验证向量$|v_1\rangle, \cdots, |v_d\rangle$构成了标准正交向量组,而且也是$V$的一个基. 于是任意的维数为$d$的有限维内积空间都有标准正交基$|v_1\rangle, \cdots, |v_d\rangle$.

练习 2.8 证明 Gram-Schmidt 过程产生V的一个标准正交基.

从现在起,提到线性算子的矩阵表示时,我们总是指相对标准正交的输入输出基的矩阵表示,同时约定当线性算子的输入输出空间相同时,除非特别说明,输入输出基也取为相同.

在这样的约定下,Hilbert 空间上的内积可以方便地以矩阵形式表述. 令$|w\rangle = \sum_i w_i \, |i\rangle$和$|v\rangle = \sum_j v_j \, |j\rangle$是向量$|w\rangle$和$|v\rangle$相对某个标准正交基$|i\rangle$的表示. 于是由于$\langle i|j\rangle = \delta_{ij}$,得

$$\langle v \mid w \rangle = \left(\sum_i v_i \, |i\rangle, \sum_j w_j \, |j\rangle \right) = \sum_{ij} v_i^* w_j \delta_{ij} = \sum_i v_i^* w_i \tag{2.18}$$

$$= \begin{bmatrix} v_1^* & \cdots & v_n^* \end{bmatrix} \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} \tag{2.19}$$

即假设表示是相对于某个标准正交基的,两个向量的内积就等于向量矩阵表示的内积. 我们还看到对偶向量$\langle v|$有很好的解释,即作为一个行向量,其分量是相应$|v\rangle$列向量表示的分量的复共轭.

外积(outer product)表示是利用内积表示线性算子的一个有用方法. 设$|v\rangle$是内积空间V中的向量,而$|w\rangle$是内积空间W的向量,定义$|w\rangle\langle v|$为从V到W的线性算子:

$$(|w\rangle\langle v|)(|v'\rangle) \equiv |w\rangle\langle v|v'\rangle = \langle v|v'\rangle |w\rangle \tag{2.20}$$

此式与我们对符号的约定非常吻合. 表达式$|w\rangle\langle v|v'\rangle$有两种可能的含义：算子$|w\rangle\langle v|$在$|v'\rangle$上的作用，$|w\rangle$与一个复数$\langle v|v'\rangle$相乘. 我们的定义使两种解释相一致，事实上，我们把前者定义为后者.

外积算子$|w\rangle\langle v|$进行线性组合的方式是显然的，因为根据定义 $\sum_i a_i |w_i\rangle\langle v_i|$ 是一个线性算子，其在 $|v'\rangle$ 上的作用是产生输出 $\sum_i a_i |w_i\rangle\langle v_i|v'\rangle$.

外积概念的有用性可以从标准正交向量的称为完备性关系(completeness relation)的重要结果看出. 令$|i\rangle$为向量空间 V 的任意标准正交基，于是任意向量 $|v\rangle$ 可写成 $|v\rangle = \sum_i v_i |i\rangle$，$v_i$ 是一组复数. 注意到$\langle i|v\rangle = v_i$，于是

$$\left(\sum_i |i\rangle\langle i|\right)|v\rangle = \sum_i |i\rangle\langle i|v\rangle = \sum_i v_i |i\rangle = |v\rangle \tag{2.21}$$

由于最后一个等式对所有$|v\rangle$成立，故有

$$\sum_i |i\rangle\langle i| = I \tag{2.22}$$

这个等式称为完备性关系. 完备性关系的一个应用是把任意线性算子表示成外积形式. 设 $A: V \to W$ 是一个线性算子，$|v_i\rangle$是 V 的一个标准正交基，且$|w_j\rangle$是 W 的一个标准正交基，两次应用完备性关系得到

$$A = I_W A I_V \tag{2.23}$$

$$= \sum_{ij} |w_j\rangle\langle w_j|A|v_i\rangle\langle v_i| \tag{2.24}$$

$$= \sum_{ij} \langle w_j|A|v_i\rangle |w_j\rangle\langle v_i| \tag{2.25}$$

这就是 A 的外积表示. 从此式还可看到相对于输入基$|v_i\rangle$和输出基$|w_j\rangle$，A 的第 i 列第 j 行元素是$\langle w_j|A|v_i\rangle$.

第二个说明完备性关系有用的应用是 Cauchy-Schwarz 不等式，这个重要的不等式在盒子 2.1 中讨论.

盒子 2.1　Cauchy-Schwarz 不等式

Cauchy-Schwarz 不等式是 Hilbert 空间的一个重要几何事实，它断言对两个任意的向量$|v\rangle$和$|w\rangle$，成立$|\langle v|w\rangle|^2 \leqslant \langle v|v\rangle\langle w|w\rangle$. 为证明，采用 Gram-Schmidt 过程构造向量空间的一个标准正交基$|i\rangle$，使基$|i\rangle$的第一个成员为 $|w\rangle/\sqrt{\langle w|w\rangle}$. 根据完备性关系 $\sum_i |i\rangle\langle i| = I$，并舍弃一些非负项，可导出

$$\langle v|v\rangle\langle v|v\rangle = \sum_i \langle v|i\rangle\langle i|v\rangle\langle w|w\rangle \tag{2.26}$$

$$\geqslant \frac{\langle v \mid w\rangle \langle w \mid v\rangle}{\langle w \mid w\rangle} \langle w \mid w\rangle \tag{2.27}$$

$$= \langle v \mid w\rangle \langle w \mid v\rangle = |\langle v \mid w\rangle|^2 \tag{2.28}$$

如所要求的，不难看出，当且仅当$|v\rangle$和$|w\rangle$有线性关系，即$|v\rangle = z|w\rangle$或$|w\rangle = z|v\rangle$对某个标量z成立，上式取等号.

练习 2.9(Pauli 算子和外积) Pauli 矩阵(图 2.2)可被视为相对标准正交基$|0\rangle, |1\rangle$的二维 Hilbert 空间上的算子，试将每个 Pauli 算子表为外积形式.

练习 2.10 设$|v_i\rangle$是内积空间 V 的一个标准正交基，相对基$|v_i\rangle$，算子$|v_j\rangle\langle v_k|$的矩阵表示是什么?

2.1.5 特征向量和特征值

线性算子 A 在向量空间上的特征向量(本征向量，eigenvector)指非零的向量$|v\rangle$，使得$A|v\rangle = v|v\rangle$，其中 v 是一个复数，称为 A 对应于$|v\rangle$的特征值(本征值，eigenvalue). 通常为方便起见，采用同一记号 v 表示特征向量的标号和特征值. 假定读者熟悉特征值和特征向量的基本性质——特别地，熟悉如何通过特征方程求出它们. 特征函数(characteristic function)定义为 $c(\lambda) \equiv \det|A - \lambda I|$，其中 det 是矩阵的行列式，可以证明特征函数仅依赖于算子 A，而不依赖子 A 的特定矩阵表示. 特征方程 $c(\lambda) = 0$ 的根是算子 A 的特征值. 由代数基本定理，每个多项式至少有一个复根，因此每个算子 A 至少有一个特征值和一个对应的特征向量，对应于一个特征值 v 的本征空间(eigenspace)是以 v 为特征值的向量的集合，它是算子 A 在其上作用的向量空间的子空间.

向量空间 V 上算子 A 的对角表示是具有形式 $A = \sum_i \lambda_i |i\rangle\langle i|$ 的一个表示，其中向量组$|i\rangle$是 A 的特征向量构成的标准正交向量组，对应的特征值为 λ_i. 如果一个算子有一个对角表示，它被称为可对角化. 在下节我们会给出 Hilbert 空间上算子可对角化的一组简单的充要条件. 作为对角表示的例子，注意 Pauli 矩阵可写作

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{2.29}$$

其中矩阵表示分别是相对标准正交向量$|0\rangle$和$|1\rangle$的. 对角表示有时称为标准正交分解.

当本征空间大于一维时，称为简并(degenerate). 例如，定义为

$$A \equiv \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{2.30}$$

的矩阵 A 对应于特征值 2 有一个二维本征空间，特征向量 (1,0,0)和(0,1,0)称为简并的，因为它们是线性无关且对应 A 的同一特征值.

练习 2.11(Pauli 矩阵的特征分解)　找出 Pauli 矩阵 X,Y 和 Z 的特征向量、特征值和对角表示.

练习 2.12　证明矩阵

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \tag{2.31}$$

不可对角化.

2.1.6　伴随与 Hermite 算子

设 A 是 Hilbert 空间 V 上的线性算子，实际上 V 上存在惟一的线性算子 $A^\dagger$ 使得对所有向量 $|v\rangle$ $|w\rangle \in V$ 成立

$$(|v\rangle, A\,|w\rangle) = (A^\dagger\,|v\rangle, |w\rangle) \tag{2.32}$$

这个线性算子称为 A 的伴随(adjoint)或 Hermite 共轭. 从定义出发易知 $(AB)^\dagger = B^\dagger A^\dagger$. 习惯上，如果 $|v\rangle$ 是向量，那么定义 $|v\rangle^\dagger \equiv \langle v|$. 根据此定义，不难看出 $(A|v\rangle)^* = \langle v|^* A^\dagger$.

练习 2.13　若 $|v\rangle$ 和 $|w\rangle$ 是两个向量，证明 $(|w\rangle\langle v|)^\dagger = |v\rangle\langle w|$.

练习 2.14(伴随的反线性(Anti-linearity of the adjoint))　证明伴随算子是反线性的

$$\left(\sum_i a_i A_i\right)^\dagger = \sum_i a_i^* A_i^\dagger \tag{2.33}$$

练习 2.15　证明 $(A^\dagger)^\dagger = A$.

在算子 A 的矩阵表示中，Hermite 共轭运算的作用是把 A 的矩阵变为共轭转置矩阵，$A^\dagger \equiv (A^*)^{\mathrm{T}}$，其中 $(*)$ 表示复共轭，T 表示转置运算. 例如我们有

$$\begin{bmatrix} 1+3\mathrm{i} & 2\mathrm{i} \\ 1+\mathrm{i} & 1-4\mathrm{i} \end{bmatrix}^\dagger = \begin{bmatrix} 1-3\mathrm{i} & 1-\mathrm{i} \\ -2\mathrm{i} & 1+4\mathrm{i} \end{bmatrix} \tag{2.34}$$

如果算子 A 的共轭转置仍为 A，则称 A 为 Hermite 或自伴(self-adjoint)算子. 投影算子(projector)是一类重要的 Hermite 算子. 设 W 是 d 维向量空间 V 的 k 维子空间，采用 Gram Schimdt 过程，可以为 V 构造一个标准正交基 $|1\rangle, \cdots, |d\rangle$，使得 $|1\rangle, \cdots, |k\rangle$ 是 W 的一个标准正交基. 定义

$$P \equiv \sum_{i=1}^{k} |i\rangle\langle i| \tag{2.35}$$

是到 W 上的投影算子. 容易验证这个定义独立于 W 的标准正交基 $|1\rangle, \cdots, |k\rangle$. 根据定义，任意向量 $|v\rangle$，$|v\rangle\langle v|$ 都是 Hermite 的，故 P 是 Hermite 的，$P^\dagger = P$. 我们会常用向量空间 P 的简称，作为投影算子 P 映到其上的向量空间. P 的正交补是

算子 $Q \equiv I - P$，容易看出 Q 是到由 $|k+1\rangle, \cdots, |d\rangle$ 张成的向量空间上的投影，这个空间也称为 P 的正交补(orthogonal complement)，也可记作 Q.

练习 2.16 证明任意投影 P 满足等式 $P^2 = P$.

算子 A 称为正规的(normal)，如果 $AA^\dagger = A^\dagger A$ 成立. 显然，Hermite 算子是正规的. 关于正规算子有一个很有名的表示定理，称为谱分解定理(spectral decomposition)，说的是一个算子是正规算子当且仅当它可对角化. 这个结果在盒子 2.2 中证明，读者需要仔细阅读.

练习 2.17 证明正规矩阵是 Hermite 的，当且仅当它的特征值为实.

矩阵 U 称为是酉的(unitary)，如果 $U^\dagger U = I$. 类似地，算子 U 也称为是酉的，如果 $UU^\dagger = I$. 容易验证算子是酉的，当且仅当其矩阵表示是酉的. 酉算子也满足 $UU^\dagger = I$，因此 U 是正规的且有谱分解. 从几何上看，酉算子很重要，因为它们保持向量之间的内积. 为证明这一点，令 $|v\rangle$ 和 $|w\rangle$ 是两个任意向量. 则 $U|v\rangle$ 和 $U|w\rangle$ 的内积与 $|v\rangle$ 和 $|w\rangle$ 的内积相同，即

$$(U|v\rangle, U|w\rangle) = \langle v|U^\dagger U|w\rangle = \langle v|I|w\rangle = \langle v|w\rangle \tag{2.36}$$

这个结果可导出任意酉的 U 有如下优雅的外积表示. 令 $|v_i\rangle$ 是一个标准正交基，定义 $|w_i\rangle \equiv U|v_i\rangle$，因为酉算子保持内积，子是 $|w_i\rangle$ 也是标准正交基，注意 $U = \sum_i |w_i\rangle\langle v_i|$. 反之，若 $|v_i\rangle$ 和 $|w_i\rangle$ 是两个标准正交基，则容易验证 $U = \sum_i |w_i\rangle\langle v_i|$ 定义的算子 U 是酉算子.

练习 2.18 证明酉矩阵的所有特征值的模都是 1，即可以写成 $e^{i\theta}$ 的形式，θ 是某个实数.

练习 2.19(Pauli 矩阵的 Hermite 性和酉性) 证明 Pauli 矩阵是 Hermite 和酉的.

练习 2.20(更换基) 设 A' 和 A'' 是向量空间 V 上一个算子 A 对两个不同的标准正交基 $|v_i\rangle$ 和 $|w_i\rangle$ 的矩阵表示，则 A' 和 A'' 的元素分别是 $A'_{ij} = \langle v_i|A|v_j\rangle$ 和 $A''_{ij} = \langle w_i|A|w_j\rangle$，刻画 A' 和 A'' 之间的关系.

半正定算子(positive operator)是 Hermite 算子的一个极重要的子类. 半正定算子 A 定义为，使得对任意向量 $|v\rangle$，$(|v\rangle, A|v\rangle)$ 都是实的非负数. 如果 $(|v\rangle, A|v\rangle)$ 对所有 $|v\rangle \neq 0$ 都严格大于零，则说 A 是正定的(positive definite). 在练习 2.24 中，读者将证明任意半正定算子自动地是 Hermite 的，于是由谱分解定理，它具有对角表示 $\sum_i \lambda_i |i\rangle\langle i|$，$\lambda_i$ 是非负特征值.

练习 2.21 对 M 是 Hermite 的情形，重复盒子 2.2 中证明谱分解的过程，并尽可能简化证明过程.

练习 2.22 证明 Hermite 算子的具有不同特征值对应的两个特征向量必须正交.

盒子 2.2　极重要的谱分解

谱分解是关于正规算子的极有用的表示定理.

定理 2.1(谱分解)　向量空间 V 上的任意正规算子 M,在 V 的某个标准正交基下可对角化.反之,任意可对角化的算子都是正规的.

证明　反过来的过程是一个简单的练习,我们只证明正向的蕴涵关系,采用对空间 V 维数 d 的归纳法证明.$d=1$ 的情况是平凡的.令 λ 是 M 的一个特征值,P 是到 λ 本征空间的投影,Q 是到正交补的投影,于是 $M=(P+Q)M(P+Q)=PMP+QMP+PMQ+QMQ$,显然 $PMP=\lambda P$.进而,因为 M 把子空间 P 映到其自身,故 $QMP=0$.我们说 $PMQ=0$.为证明这一点,令 $|v\rangle$ 为子空间 P 中的元素,则 $MM^\dagger|v\rangle=M^\dagger M|v\rangle=\lambda M^\dagger|v\rangle$,因此 $M^\dagger|v\rangle$ 的特征值是 λ,是子空间 P 的元素,可得 $QM^\dagger P=0$.对该等式取伴随运算,得到 $PMQ=0$,于是 $M=PMP+QMQ$.下面我们证明 QMQ 是正规的.为此,注意 $QM=QM(P+Q)=QMQ$,$QM^\dagger=QM^\dagger(P+Q)=QM^\dagger Q$.进而由 M 的正规性和 $Q^2=Q$ 的事实,

$$QMQQM^\dagger Q = QMQM^\dagger Q \tag{2.37}$$

$$= QMM^\dagger Q \tag{2.38}$$

$$= QM^\dagger MQ \tag{2.39}$$

$$= QM^\dagger QMQ \tag{2.40}$$

$$= QM^\dagger QQMQ \tag{2.41}$$

故 QMQ 是正规的.由归纳假设,QMQ 对子空间 Q 的某个标准正交基是可对角化的,而 PMP 已经是对于 P 的标准正交基对角化的.可知 $M=PMP+QMQ$ 相对全空间的某个标准正交基可对角化.

在外积表示形式下,这意味着 M 可以写作 $M=\sum_i \lambda_i |i\rangle\langle i|$,其中 λ_i 是 M 的特征值.$|i\rangle$ 是 V 的一个标准正交基,每个 $|i\rangle$ 是 M 的对应特征值 λ_i 的特征向量.从投影算子角度看,$M=\sum_i \lambda_i P_i$,λ_i 仍代表 M 的特征值,P_i 是到 λ_i 在 M 中的本征空间的投影.这些投影算子满足,完备关系 $\sum_i P_i = I$ 和标准正交关系 $P_i P_j = \delta_{ij} P_i$.

练习 2.23　证明投影 P 的特征值全都是非 0 即 1.

练习 2.24(半正定算子的 Hermite 性)　证明半正定算子必然是 Hermite 的(提示:证明任意算子 A 可以写成 $A=B+iC$ 的形式,其中 B 和 C 是 Hermite 的).

练习 2.25　证明对任意算子 A,$A^\dagger A$ 都是半正定的.

2.1.7 张量积

张量积是将向量空间合在一起，构成更大向量空间的一种方法，这个构造对理解量子力学的多粒子系统很关键. 下面的讨论有点抽象，如果读者还不熟悉张量积，只管跳过去等到后面讨论到量子力学中张量积时再回来.

设 V 和 W 是维数分别是 m 和 n 的向量空间，并假定 V 和 W 是 Hilbert 空间，于是 $V\otimes W$(读作“V 张量 W”)是一个 mn 维向量空间. $V\otimes W$ 的元素是 V 的元素 $|v\rangle$ 和 W 的元素 $|w\rangle$ 的张量积 $|v\rangle\otimes|w\rangle$ 的线性组合. 特别地，如果 $|i\rangle$ 和 $|j\rangle$ 是 V 和 W 的标准正交基，则 $|i\rangle\otimes|j\rangle$ 是 $V\otimes W$ 的一个基，常用缩写符号 $|v\rangle|w\rangle$，$|v,w\rangle$ 或 $|vw\rangle$ 来表示张量积 $|v\rangle\otimes|w\rangle$. 例如，当 V 是以 $|0\rangle$ $|1\rangle$ 为基向量的二维向量空间，则 $|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle$ 是 $V\otimes V$ 的一个元素.

由定义，张量积满足如下的基本性质.

(1) 对任意标量 z，V 的元素 v 和 W 的元素 w，满足

$$z(|v\rangle\otimes|w\rangle)=(z|v\rangle)\otimes|w\rangle=|v\rangle\otimes(z|w\rangle) \tag{2.42}$$

(2) 对 V 中任意的 v_1 和 v_2 和 W 中的 $|w\rangle$，满足

$$(|v_1\rangle+|v_2\rangle)\otimes|w\rangle=|v_1\rangle\otimes|w\rangle+|v_2\rangle\otimes|w\rangle \tag{2.43}$$

(3) 对 V 中任意的 $|v\rangle$ 和 W 中的 w_1 和 w_2，满足

$$|v\rangle\otimes(|w_1\rangle+|w_2\rangle)=|v\rangle\otimes|w_1\rangle+|v\rangle\otimes|w_2\rangle \tag{2.44}$$

$V\otimes W$ 上的线性算子有哪些类型？设 $|v\rangle$ 和 $|w\rangle$ 分别是 V 和 W 中向量，A 和 B 是 V 和 W 上的线性算子. 我们可以在 $V\otimes W$ 上定义一个线性算子 $A\otimes B$，定义如下

$$(A\otimes B)(|v\rangle\otimes|w\rangle)\equiv A|v\rangle\otimes B|w\rangle \tag{2.45}$$

为保证其线性，$A\otimes B$ 的定义可以自然地扩展到 $V\otimes W$ 的所有元素，即

$$(A\otimes B)\Big(\sum_i a_i|v_i\rangle\otimes|w_i\rangle\Big)\equiv\sum_i a_i A|v_i\rangle\otimes B|w_i\rangle \tag{2.46}$$

可以证明如此定义的 $A\otimes B$ 是 $V\otimes W$ 上定义良好(well-defined)的线性算子. 这两个算子张量积的概念显然可以推广到不同向量空间之间映射 $A:V\to V'$ 和 $B:W\to W'$. 实际上，任意把 $V\otimes W$ 映到 $V'\otimes W'$ 的线性算子，都可以表示为把 V 映到 V' 和把 W 映到 W' 算子张量积的线性组合

$$C=\sum_i c_i A_i\otimes B_i \tag{2.47}$$

其中，由定义得

$$\Big(\sum_i c_i A_i\otimes B_i\Big)|v\rangle\otimes|w\rangle\equiv\sum_i c_i A_i|v\rangle\otimes B_i|w\rangle \tag{2.48}$$

空间 V 和 W 上的内积可用于定义 $V\otimes W$ 上的一个自然的内积，为

$$\Big(\sum_i a_i|v_i\rangle\otimes|w_i\rangle,\sum_j b_j|v'_j\rangle\otimes|w'_j\rangle\Big)\equiv\sum_{ij}a_i^* b_j\langle v_i|v'_j\rangle\langle w_i|w'_j\rangle \tag{2.49}$$

可以证明这个函数是一个定义良好的内积. 内积空间 $V \otimes W$ 从这个内积继承了我们熟悉的其他概念：伴随性、酉性、正规性和 Hermite 性.

这些讨论都相当抽象. 但转到称为 Kronecker 积的矩阵表示，问题会具体得多. 设 A 是一个 $m \times n$ 矩阵，B 是一个 $p \times q$ 矩阵，则我们有矩阵表示

$$A \otimes B \equiv \overbrace{\begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix}}^{nq} \Big\} mp \tag{2.50}$$

在这个表示中，$A_{11}B$ 的项代表 $p \times q$ 子矩阵，其元素正比于 B，全局比例常数为 A_{11}. 例如，向量(1,2) 和(2,3) 的张量积是向量

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} \otimes \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 1 \times 2 \\ 1 \times 3 \\ 2 \times 2 \\ 2 \times 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 4 \\ 6 \end{bmatrix} \tag{2.51}$$

Pauli 矩阵 X 和 Y 的张量积是

$$X \otimes Y = \begin{bmatrix} 0 \cdot Y & 1 \cdot Y \\ 1 \cdot Y & 0 \cdot Y \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & -\mathrm{i} \\ 0 & 0 & \mathrm{i} & 0 \\ 0 & -\mathrm{i} & 0 & 0 \\ \mathrm{i} & 0 & 0 & 0 \end{bmatrix} \tag{2.52}$$

最后提一下有用的记号 $|\psi\rangle^{\otimes k}$，指 $|\psi\rangle$ 自身的 k 次张量积，例如 $|\psi\rangle^{\otimes 2} = |\psi\rangle \otimes |\psi\rangle$. 相应的记号会用于张量积空间上的算子.

练习 2.26　令 $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$，以 $|0\rangle|1\rangle$ 的张量积形式，并采用 Kronecker 积，具体写出 $|\psi\rangle^{\otimes 2}$ 和 $|\psi\rangle^{\otimes 3}$.

练习 2.27　计算 Pauli 算子张量积的矩阵表示：(1) X 和 Z；(2) I 和 X；(3) X 和 I. 张量积可对易吗?

练习 2.28　证明转置、复共轭、伴随算子对张量积是分配的，即

$$(A \otimes B)^* = A^* \otimes B^*; (A \otimes B)^{\mathrm{T}} = A^{\mathrm{T}} \otimes B^{\mathrm{T}}; (A \otimes B)^{\dagger} = A^{\dagger} \otimes B^{\dagger} \tag{2.53}$$

练习 2.29　证明两个酉算子的张量积是酉的.

练习 2.30　证明两个 Hermite 算子的张量积是 Hermite 的.

练习 2.31　证明两个半正定算子的张量积是半正定的.

练习 2.32　证明两个投影算子的张量积是一个投影算子.

练习 2.33　一个单量子比特上的 Hadamard 算子可以写作

$$H = \frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|] \tag{2.54}$$

证明 n 量子比特上的 Hadamard 变换可以写成

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{x \cdot y} |x\rangle \langle y| \tag{2.55}$$

并具体写出 $H^{\otimes 2}$ 的矩阵表示.

2.1.8 算子函数

算子和矩阵上可以定义很多重要的函数. 一般而言,给定从复数到复数的函数 f,可以通过下面的步骤定义正规矩阵上(或一个子类,如 Hermite 矩阵)的相应矩阵函数. 令 $A = \sum_a a |a\rangle\langle a|$ 是正规算子 A 的一个谱分解,定义 $f(A) = \sum_a f(a) |a\rangle\langle a|$,容易看出 $f(A)$ 是惟一定义的. 这个过程可以用于,例如,定义一个半正定算子的平方根,正定算子的对数和正规算子的指数. 例如

$$\exp(\theta Z) = \begin{bmatrix} e^{\theta} & 0 \\ 0 & e^{-\theta} \end{bmatrix} \tag{2.56}$$

因为 Z 的特征向量是 $|0\rangle$ 和 $|1\rangle$.

练习 2.34 求下面矩阵的平方根和对数

$$\begin{bmatrix} 4 & 3 \\ 3 & 4 \end{bmatrix} \tag{2.57}$$

练习 2.35(Pauli 矩阵的指数) 令 v 是任意三维单位实向量,且 θ 为实数. 证明

$$\exp(i\theta v \cdot \sigma) = \cos(\theta) I + i \sin(\theta) v \cdot \sigma \tag{2.58}$$

其中 $v \cdot \sigma \equiv \sum_{i=1}^{3} v_i \sigma_i$. 这个练习在问题 2.1 中得到推广.

另一个重要的矩阵函数是矩阵的迹. A 的迹定义为它的对角元素之和,

$$\mathrm{tr}(A) \equiv \sum_i A_{ii} \tag{2.59}$$

容易看到迹是循环(cyclic)的,即 $\mathrm{tr}(AB) = \mathrm{tr}(BA)$,是线性的,即 $\mathrm{tr}(A+B) = \mathrm{tr}(A) + \mathrm{tr}(B)$, $\mathrm{tr}(zA) = z\,\mathrm{tr}(A)$,其中 A 和 B 是任意矩阵,z 是复数. 而且,由循环性质得到矩阵的迹在酉相似变换 $A \rightarrow UAU^{\dagger}$ 下不变,因为 $\mathrm{tr}(UAU^{\dagger}) = \mathrm{tr}(U^{\dagger}UA) = \mathrm{tr}(A)$. 受这个结果启发,可以把算子 A 的迹定义为 A 的任意矩阵表示的迹. 迹在酉相似变换下的不变性,保证算子的迹是定义良好的.

作为迹的例子,设 $|\psi\rangle$ 是一单位向量且 A 是任意算子. 为计算 $\mathrm{tr}(A|\psi\rangle\langle\psi|)$,采用 Gram-Schmidt 过程,把 $|\psi\rangle$ 扩展成一个以 $|\psi\rangle$ 为首个元的标准正交基 $|i\rangle$,则有

$$\mathrm{tr}(A\mid\psi\rangle\langle\psi\mid)=\sum_i\langle i\mid A\mid\psi\rangle\langle\psi\mid i\rangle \tag{2.60}$$

$$=\langle\psi\mid A\mid\psi\rangle \tag{2.61}$$

这个结果，即 $\mathrm{tr}(A\mid\psi\rangle\langle\psi\mid)=\langle\psi\mid A\mid\psi\rangle$ 在计算一个算子的迹时极为有用.

练习 2.36　证明 Pauli 矩阵除 I 外，迹均为 0.

练习 2.37(迹的循环性质)　如果 A 和 B 是两个线性算子，证明

$$\mathrm{tr}(AB)=\mathrm{tr}(BA) \tag{2.62}$$

练习 2.38(迹的线性性质)　如果 A 和 B 是两个线性算子，证明

$$\mathrm{tr}(A+B)=\mathrm{tr}(A)+\mathrm{tr}(B) \tag{2.63}$$

且若 z 是任意复数，证明

$$\mathrm{tr}(zA)=z\mathrm{tr}(A) \tag{2.64}$$

练习 2.39(算子上的 Hilbert-Schmidt 内积)　Hilbert 空间 V 上的线性算子集合 L_V 显然是一个向量空间，即两个线性算子之和是线性算子，如果 A 是线性算子，z 是复数，则 zA 是线性、且有零元素 0. 另一个重要结果是向量空间 L_V 可赋予自然的内积结构，而成为 Hilbert 空间.

(1) 证明 $L_V\times L_V$ 上的函数 $(\cdot,\cdot)$，

$$(A,B)\equiv\mathrm{tr}(A^\dagger B) \tag{2.65}$$

是一个内积函数. 这个内积称为 Hilbert-Schmidt 或迹内积.

(2) 如果 V 是 d 维的，证明 L_V 的维数为 d^2.

(3) 求 Hilbert 空间 L_V 中 Hermite 矩阵的标准正交基.

2.1.9　对易式和反对易式

两个算子 A 和 B 之间的对易式(commutator)定义为

$$[A,B]\equiv AB-BA \tag{2.66}$$

若 $[A,B]=0$，即 $AB=BA$，则说 A 和 B 是对易的. 类似地，两个算子 A 和 B 的反对易式(anti-commtator)定义为

$$\{A,B\}\equiv AB+BA \tag{2.67}$$

如果 $\{A,B\}=0$，我们说 A 与 B 反对易. 实际上一对算子的许多重要性质可以从它们的对易式和反对易式推出. 也许最有用的关系是下面对易式与 Hermite 算子同时对角化之间的关系，即能够写成 $A=\sum_i a_i\mid i\rangle\langle i\mid$，$B=\sum_i b_i\mid i\rangle\langle i\mid$，其中 $\mid i\rangle$ 是 A 和 B 的公共特征向量的标准正交组.

定理 2.2(同时对角化定理)　设 A 和 B 是 Hermite 算子，当且仅当存在一个标准正交基，使 A 和 B 在这个基下同时是对角的，则 $[A,B]=0$. 在这种情况下，A 和 B 称为可同时对角化.

这个结果把通常很容易计算的两个算子的对易式和事先难以确定的同时可对角化性质联系起来. 例如,考虑

$$[X,Y] = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & -\mathrm{i}\\ \mathrm{i} & 0\end{bmatrix} - \begin{bmatrix}0 & -\mathrm{i}\\ \mathrm{i} & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \tag{2.68}$$

$$= 2\mathrm{i}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \tag{2.69}$$

$$= 2\mathrm{i}Z \tag{2.70}$$

可看出 X 和 Y 不能对易. 在练习 2.11 已经证明 X 和 Y 没有共同的特征向量,这与同时对角化定理的结论相符.

证明 容易验证如果 A 和 B 在同一标准正交基下时是对角的,则 $[A,B]=0$. 为证明反向命题,令 $|a,j\rangle$ 是 A 的特征值 a 的本征空间 V_a 的一个标准正交基,j 用来标记可能出现的简并情形. 注意到

$$AB\,|\,a,j\,\rangle = BA\,|\,a,j\,\rangle = aB\,|\,a,j\,\rangle \tag{2.71}$$

而且,$B|a,j\rangle$ 是本征空间的 V_a 的一个元素. 令 P_a 表示到空间 V_a 的投影,且定义 $B_a \equiv P_a B P_a$,容易看到 B_a 限制到空间 V_a 上且在 V_a 上是 Hermite 的,于是相对张成空间 V_a 的特征向量的标准正交向量组具有谱分解. 这些特征向量记作 $|a,b,k\rangle$,其中 a,b 标记 A 和 B_a 的特征值,k 表示 B_a 的可能简并. 注意 $B|a,b,k\rangle$ 是 V_a 的一个元素,于是 $B|a,b,k\rangle = P_a B|a,b,k\rangle$,同时我们有 $P_a|a,b,k\rangle = |a,b,k\rangle$,因此

$$B\,|\,a,b,k\rangle = P_a B P_a\,|\,a,b,k\rangle = b\,|\,a,b,k\rangle \tag{2.72}$$

则 $|a,b,k\rangle$ 是 B 的对应特征值 b 的特征向量,这样 $|a,b,k\rangle$ 就同时是 A 和 B 的一个特征向量的标准正交向量组,张成 A 和 B 定义在其上的整个向量空间. 即 A 和 B 可以同时对角化.

练习 2.40(Pauli 矩阵的对易关系) 验证对易关系:

$$[X,Y] = 2\mathrm{i}Z, \quad [Y,Z] = 2\mathrm{i}X, \quad [Z,X] = 2\mathrm{i}Y \tag{2.73}$$

有一个采用三个指标的反对称张量 ε_{jkl} 表示这个关系的优雅方式,其中除 $\varepsilon_{123} = \varepsilon_{231} = \varepsilon_{312} = 1$ 和 $\varepsilon_{321} = \varepsilon_{213} = \varepsilon_{132} = -1$ 外,$\varepsilon_{jkl} = 0$,可得

$$[\sigma_j,\sigma_k] = 2\mathrm{i}\sum_{l=1}^{3}\varepsilon_{jkl}\sigma_l \tag{2.74}$$

练习 2.41(Pauli 矩阵的反对易关系) 验证反对易关系:

$$\{\sigma_i,\sigma_j\} = 0 \tag{2.75}$$

其中 $i\neq j$ 都选自集合 1,2,3. 再验证($i=0,1,2,3$)

$$\sigma_i^2 = I \tag{2.76}$$

练习 2.42 验证

$$AB = \frac{[A,B]+\{A,B\}}{2} \tag{2.77}$$

练习 2.43　证明对 $j,k=1,2,3$，有

$$\sigma_j\sigma_k=\delta_{jk}I+\mathrm{i}\sum_{l=1}^{3}\varepsilon_{jkl}\sigma_l \tag{2.78}$$

练习 2.44　设$[A,B]=0$，$\{A,B\}=0$，且 A 可逆，证明 B 必为 0.

练习 2.45　证明$[A,B]^\dagger=[B^\dagger,A^\dagger]$.

练习 2.46　证明$[A,B]=-[B,A]$.

练习 2.47　设 A 和 B 都是 Hermite 的，证明 $\mathrm{i}[A,B]$是 Hermite 的.

2.1.10　极式分解和奇异值分解

极式(polar)分解和奇异值(singular value)分解是把线性算子分解成简单部分的一个有用方法. 特别地，这些分解使我们可以把一般线性算子分解成酉算子和半正定算子的乘积. 虽然我们对一般线性算子的结构的了解不是非常透彻，但我们对酉算子和半正定算子知道得相当清楚，极式分解和奇异值分解使我们利用这些知识更好地去了解一般线性算子.

定理 2.3(极式分解)　令 A 是向量空间 V 上的线性算子，则存在酉算子 U 和半正定算子 J 和 K，使得

$$A=UJ=KU \tag{2.79}$$

其中 J 和 K 是惟一满足这些方程的半正定算子，定义为 $J\equiv\sqrt{A^\dagger A}$和 $K\equiv\sqrt{AA^\dagger}$，而且，如果 A 可逆，U 还是惟一的.

称表达式 $A=UJ$ 为 A 的左极式分解，而 $A=KU$ 为 A 的右极式分解. 大多数情况下，我们会省略名称中的“左”或“右”，而对两种表达式都用极式分解名称，靠上下文指示其含义.

证明　$J\equiv\sqrt{A^\dagger A}$是一个半正定算子，于是可以进行谱分解，$J=\sum_i\lambda_i|i\rangle\langle i|$，$(\lambda_i\geqslant 0)$，定义$|\psi_i\rangle\equiv A|i\rangle$. 从定义出发，可看到$\langle\psi_i|\psi_i\rangle=\lambda_i^2$. 下面只考虑那些满足 $\lambda_i\neq 0$ 的 i. 对这些 i，定义$|e_i\rangle\equiv|\psi_i\rangle/\lambda_i$，于是$|e_i\rangle$是归一化的，而且它们还是正交的，如果 $i\neq j$，则$\langle e_i|e_j\rangle=\langle i|A^\dagger A|j\rangle/(\lambda_i\lambda_j)=\langle i|J^2|j\rangle/(\lambda_i\lambda_j)=0$.

我们考虑了满足 $\lambda_i\neq 0$ 的 i. 现在利用 Gram-Schmidt 过程来扩展标准正交组 $|e_i\rangle$，以形成标准正交基，仍记为 $|e_i\rangle$. 定义酉算子$U\equiv\sum_i|e_i\rangle\langle i|$，当 $\lambda_i\neq 0$时，我们有 $UJ|i\rangle=\lambda_i|e_i\rangle=|\psi_i\rangle=A|i\rangle$，当 $\lambda_i=0$ 时，我们有 $UJ|i\rangle=0=|\psi_i\rangle$. 我们已证明 A 和 UJ 在基 $|i\rangle$ 上的作用一致，于是 $A=UJ$.

J 是惟一的，因为 $A=UJ$ 的左边乘以伴随方程 $A^\dagger=JU^\dagger$，给出 $J^2=A^\dagger A$，也就看出 $J=\sqrt{A^\dagger A}$是惟一的. 容易知道若 A 是可逆的，则 J 也可逆，于是 U 惟一地由方程 $U=AJ^{-1}$确定，可以得到右极式分解，因为 $A=UJ=UJU^\dagger U=KU$，其中

$K \equiv UJU^\dagger$是半正定算子. 又因为 $AA^\dagger = KUU^\dagger K = K^2$,故必有 $K = \sqrt{AA^\dagger}$,证毕.

奇异值分解是极式分解和谱分解定理的结合.

推理 2.4(奇异值分解) 令 A 是一方阵,则必存在酉矩阵 U、V 和一个非负对角阵 D,使得

$$A = UDV \tag{2.80}$$

D 的对角元称为 A 的奇异值.

证明 由极式分解,对某个酉矩阵 S 和半正定矩阵 J,成立 $A = SJ$. 由谱分解定理,对酉矩阵 T 和非负对角阵 D,成立 $J = TDT^\dagger$. 令 $U \equiv ST$ 和 $V \equiv T^\dagger$,证明完成.

练习 2.48 一个半正定矩阵 P 的极式分解是什么? 一个酉矩阵 U 的极式分解和一个 Hermite 阵 H 的极式分解分别是什么?

练习 2.49 把一个正规矩阵的极式分解表示为外积形式.

练习 2.50 求如下矩阵的左右极式分解:

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \tag{2.81}$$

2.2 量子力学假设

知识从拒绝世界的表象开始.

——*Alan Key*

世界上最令人费解的事是,世界是可以理解的.

——*Albert Einstein*

量子力学用以物理理论发展的一个数学框架. 量子力学本身不能告诉我们物理系统服从什么定律,但它却提供了研究这些定律的数学和概念的框架. 下面几节我们将给出量子力学基本假设的完整描述,这些假设把物理世界和量子力学的数学描述联系了起来.

量子力学的假设是经过长期的尝试与失败后而推导出来的,经过了发明者的大量猜测和摸索. 假设的动机不明显,这不足为奇,因为量子力学的基本假设即使对专家而言也是令人吃惊的. 通过下面几节,读者将学会掌握这些假设——懂得如何应用以及何时应用这些假设.

2.2.1 状态空间

量子力学的第一条假设建立起量子力学适用的场合,即线性代数中熟知的 Hilbert 空间.

假设 1　任一孤立物理系统都有一个称为系统状态空间的复内积向量空间(即 Hilbert 空间)与之相联系，系统完全由状态向量所描述，这个向量是系统状态空间的一个单位向量.

量子力学并不告诉我们，对一个给定的物理系统，它的状态空间是什么，也不告诉我们，系统的状态向量是什么. 对特定系统找出状态空间和状态向量是困难的问题，物理学家已为此研究出许多复杂和漂亮的规则. 例如，有一门量子电动力学理论(常称为 QED)来描述原子和光的相互作用，它就是告诉我们用什么状态空间给出原子和光的量子描述. 我们对像 QED 那样的复杂理论(除了在第 7 章它们被用于物理实现)不太关心，因为我们最感兴趣的是量子力学所提供的一般框架，对我们的目的而言，关于系统状态空间作一些非常简单(并且合理)的假设，并坚持这些假设就足够了.

最简单，也是我们最常关心的量子系统，是量子比特. 一个量子比特有一个二维的状态空间. 设$|0\rangle$和$|1\rangle$构成这个状态空间的一个标准正交基，则状态空间中的任意状态向量可写作

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{2.82}$$

其中 a 和 b 是复数. 于是$|\psi\rangle$为单位向量的必要条件，即$\langle\psi|\psi\rangle=1$，就等价于$|a|^2+|b|^2=1$. 条件$\langle\psi|\psi\rangle=1$常称为状态向量的归一化条件.

我们把量子比特视为最基本的量子力学系统. 在第 7 章，将看到量子比特的物理系统是真实存在的，不过目前只抽象讨论而不涉及特定物理实现. 对量子比特的讨论总是相对某个已经固定的标准正交向量基$|0\rangle$和$|1\rangle$，直观上，状态$|0\rangle$和$|1\rangle$对应于一个比特可能取的两个值 0 和 1. 量子比特和比特的不同之处在于，这两个状态可能存在形如$a|0\rangle+b|1\rangle$的叠加，叠加态下不能确定地说状态是$|0\rangle$或$|1\rangle$.

最后介绍与描述量子状态有关的一些有用术语. 任意线性组合$\sum_i a_i|\psi_i\rangle$理解为状态$|\psi_i\rangle$的一个$|\psi_i\rangle$具有幅度a_i的叠加，于是状态

$$\frac{|0\rangle-|1\rangle}{\sqrt{2}} \tag{2.83}$$

是状态$|0\rangle$和$|1\rangle$的状态的叠加. $|0\rangle$具有幅度$1/\sqrt{2}$，状态$|1\rangle$具有幅度$-1/\sqrt{2}$.

2.2.2　演化

量子力学系统的状态$|\psi\rangle$如何随时间变化？下面的假设为描写此系统状态变化提供了一种方法.

假设 2　一个封闭量子系统的演化可以由一个酉变换来刻画. 即系统在时刻t_1的状态$|\psi\rangle$和系统在时刻t_2的状态$|\psi'\rangle$，可以通过一个仅依赖于时间t_1和t_2的

酉算子 U 相联系：

$$|\psi'\rangle = U|\psi\rangle \tag{2.84}$$

正如量子力学不告诉我们状态空间或一个特定量子系统的量子状态，它也不告诉我们什么样的酉算子 U 描述了现实世界的量子动态，量子力学仅仅向我们保证，任意封闭量子系统的演化都可以用这种方式描述. 一个显然的问题是：自然选择什么样酉算子？实际上单量子比特的情形下，所有的酉算子都可以在实际系统中实现.

让我们来看几个在量子计算与量子信息中非常重要的单量子比特上的酉算子例子. 已经遇到的这类酉算子的例子是 2.1.3 节定义的 Pauli 矩阵，第 1 章中描述的量子门. 像 1.3.1 节中所述的那样，X 矩阵常称为量子非门，它与传统非门相对应. X 和 Z Pauli 矩阵有时又称为比特翻转(bit flip)和相位翻转(phase flip)矩阵：X 矩阵把 $|0\rangle$ 变到 $|1\rangle$，而把 $|1\rangle$ 变到 $|0\rangle$，比特翻转因此得名；而 Z 矩阵保持 $|0\rangle$ 不变，把 $|1\rangle$ 变到 $-|1\rangle$，因为 -1 常称为相移因子，相位翻转因此得名. 为避免和第 4 章将要定义的相位门相混淆，一般不用相位翻转来称呼 Z(2.2.7 节有关于相位一词许多用法的更详细的讨论).

Hadamard 门是另一个有趣的酉算子，记作 H. 它有 $H|0\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$，$H|1\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$，相应的矩阵表述为

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{2.85}$$

练习 2.51 验证 Hadamard 门是酉的.

练习 2.52 验证 $H^2 = I$.

练习 2.53 H 的特征值和特征向量是什么？

假设 2 要求所描述的系统是封闭的，即它与别的系统没有任何相互作用. 当然，现实中所有系统(除非把宇宙作为整体)至少在某种程度上与别的系统有相互作用，然而，可以很好地近似描述为封闭的系统是存在的，并且可用酉演化很好地近似描述，而且，至少原则上每个开放系统都可以描述为一个更大的酉演化中的封闭系统(宇宙)的一部分. 后面将介绍更多的描述非封闭系统的工具，但现在将继续介绍封闭系统演化的描述.

假设 2 描述了封闭量子系统的量子状态在两个不同时刻的关系. 作为这条假设的一个更精细版本，可以给出描述量子系统在连续时间上的演化. 从这个更精细的假设可以重新得到假设 2. 在叙述修改的假设之前，有两点需要指出. 首先是记号的注释，下面讨论中的 H 算子不同于前面引出的 Hadamdard 算子. 其次，下面的假设用到微分方程，对在微分方程方面几乎没有背景的读者，我们再次保证除第 7 章量子信息处理的真实物理实现部分外，本书的大部分不会用到微分方程.

假设 2′　封闭量子系统的演化由 Schrödinger 方程描述：

$$\mathrm{i}\hbar \frac{\mathrm{d}|\psi\rangle}{\mathrm{d}t} = H|\psi\rangle \tag{2.86}$$

这个方程中 $\hbar$ 称为 Planck 常数，其值必须由实验确定. 它的精确值对我们并不重要，实践中，常把因子 $\hbar$ 的值放入到 H 中，而置 $\hbar = 1$，H 是一个称为封闭系统 Hamilton 量的固定 Hermite 算子.

如果知道了系统的 Hamilton 量，则(加上对 $\hbar$ 的知识)我们就至少在原则上完全了解了系统的动态. 找出描述特定物理系统的 Hamilton 量一般是个很难的问题(20 世纪物理学的许多工作与这个问题有关)，这需要从实验得来实质性结果. 对我们而言，这是在量子力学框架内由物理理论来解决的细节问题，即在原子的这样或那样的配置中需要什么样的 Hamilton 量描述，而并非量子力学理论自身需要解决的问题. 在对量子计算与量子信息的大部分讨论中不需要讨论 Hamilton 量，即使需要用到，通常也只是从假设某个矩阵为 Hamilton 量作为问题的已知起点，然后继续下去，而不考察 Hamilton 量的来历.

由于 Hamilton 量是一个 Hermite 算子，故有谱分解

$$H = \sum_E E|E\rangle\langle E| \tag{2.87}$$

其中特征值是 E，$|E\rangle$ 是相应的特征向量. 状态 $|E\rangle$ 习惯上称作能量本征态(energy eigensate)，或有时称为定态(stationary state)，而 E 是 $|E\rangle$ 的能量. 最低的能量称为系统的基态能量(ground state energy)，相应的能量本征态(或本征空间)称为基态(ground state). 状态 $|E\rangle$ 有时称为定态，原因是它们随时间的变化只是一个数值因子

$$|E\rangle \mapsto \exp(-\mathrm{i}Et/\hbar)|E\rangle \tag{2.88}$$

例如，设单量子比特具有 Hamilton 量

$$H = \hbar\omega X \tag{2.89}$$

此式中 ω 是一个参数，实际中需要通过实验确定. 这里不太关心该参数，只为给出量子计算与量子信息中有时会用到的 Hamilton 量的类型. 这个 Hamilton 量的能量本征态显然和与 X 的本征态相同，即 $(|0\rangle + |1\rangle)/\sqrt{2}$ 和 $(|0\rangle - |1\rangle)/\sqrt{2}$，分别对应能量 $\hbar\omega$ 和 $-\hbar\omega$，于是基态是 $(|0\rangle - |1\rangle)/\sqrt{2}$，基态能量是 $-\hbar\omega$.

假设 2′中 Hamilton 量的动态描述和假设 2 中的酉算子描述之间有什么关系？答案在于 Schrödinger 方程的解. 容易验证

$$|\psi(t_2)\rangle = \exp\left[\frac{-\mathrm{i}H(t_2 - t_1)}{\hbar}\right]|\psi(t_1)\rangle = U(t_1, t_2)|\psi(t_1)\rangle \tag{2.90}$$

其中定义

$$U(t_1, t_2) \equiv \exp\left[\frac{-\mathrm{i}H(t_2 - t_1)}{\hbar}\right] \tag{2.91}$$

在练习中要证明这个算子是酉的，而且，任意酉算子 U 可以用某个 Hermite 算子 K，实现 $U=\exp(iK)$ 形式，因此在用酉算子的离散时间动态描述和用 Hamilton 量的连续时间动态描述之间存在一一对应关系. 本书的大部分内容采用量子动态的酉描述.

练习 2.54 设 A 和 B 是对易的 Hermite 算子，证明 $\exp(A)\exp(B)=\exp(A+B)$（提示：利用 2.1.9 节的结果）.

练习 2.55 证明式(2.91)定义的算子 $U(t_1,t_2)$ 是酉的.

练习 2.56 利用谱分解证明 $K=-i\log(U)$ 对任意酉的 U 都是 Hermite 的，于是 $U=\exp(iK)$ 对某个 Hermite 的 K 成立.

在量子计算与量子信息中常用到以下说法，把一个酉算子应用到一个特定的量子系统上. 例如，量子线路情况下，我们可能说把酉门 X 应用到一个单量子比特上. 这是否和前面认为酉算子是描述封闭量子系统演化的说法相矛盾？毕竟如果应用一个酉算子，那么至少有一个外在的“我们”和量子系统相互作用，系统就不封闭了.

一束激光聚焦在一个原子上的情形就是这样的例子. 经过一番努力，可以写出描述整个原子-激光系统的 Hamilton 量，有趣的是，当我们只考虑原子的效应而写出的原子-激光系统的 Hamilton 量时，原子状态向量实际可以可用另一个 Hamilton 量原子 Hamilton 量近似，但不是完全描述. 原子 Hamilton 量包含和激光密度以及激光其他参数有关的项，而我们可以按需要改变这些量. 尽管原子不是一个封闭系统，原子的演化像是由我们可按需要改变的 Hamilton 量描述似的.

更一般地，对许多这类系统实际上可以写出量子系统的一个时变 Hamilton 量. 即 Hamilton 量不是常量，而是按照置于实验者控制下，在实验过程中可以改变的某些参数变化的. 于是，虽然系统是不封闭的，但在很好的近似程度上，是按照具有时变 Hamilton 量的 Schrödinger 方程演化.

因此尽管开始时系统不封闭，我们也常用酉算子描述量子系统的演化，其中一个主要的例外是下一节要描述的量子测量. 后面我们将更详细地考察从相互作用系统酉演化可推导出的可能结论，以及更准确了解实际量子系统的动态.

2.2.3 量子测量

我们已假设封闭量子系统按酉算子演化. 尽管系统演化可以不与世界其他部分相互作用，但是一定有某些时刻实验者和实验设备——换句话说外部物理世界——要观察系统，以了解系统内部的情况. 这个观测作用使系统不再封闭，也就是不再服从酉演化. 为解释这样做的影响，我们引入假设 3，以便为描述量子系统的测量提供一条途径.

假设 3　量子测量由一组测量算子 $\{M_m\}$ 描述，这些算子作用在被测系统状态空间上，指标 m 表示实验中可能的测量结果. 若在测量前，量子系统的最新状态是 $|\psi\rangle$，则结果 m 发生的可能性由

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle \tag{2.92}$$

给出，且测量后系统的状态为

$$\frac{M_m | \psi \rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}} \tag{2.93}$$

测量算子满足完备性方程，

$$\sum_m M_m^\dagger M_m = I \tag{2.94}$$

完备性方程表达了概率之和为 1 的事实：

$$1 = \sum_m p(m) = \sum_m \langle \psi | M_m^\dagger M_m | \psi \rangle \tag{2.95}$$

该方程对所有 $|\psi\rangle$ 成立，等价于完备性方程. 然而，直接检验完备性方程要容易得多，这就是其出现在假设叙述中的原因.

测量的一个简单但重要的例子是，单量子比特在计算基下的测量，这是在单量子比特上的测量，有由两个测量算子 $M_0 = |0\rangle\langle 0|$ 和 $M_1 = |1\rangle\langle 1|$ 定义的两个结果. 注意到每个测量算子都是 Hermite 的，并且 $M_0^2 = M_0$，$M_1^2 = M_1$，于是满足完备性关系，$I = M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1$. 假设被测状态是 $a|0\rangle + b|1\rangle$，则获得测量结果 0 的概率是

$$p(0) = \langle \psi | M_0^\dagger M_0 | \psi \rangle = \langle \psi | M_0 | \psi \rangle = |a|^2 \tag{2.96}$$

类似地，获得测量结果 1 的概率是 $p(1) = |b|^2$. 两种情况下，测量后的状态分别为

$$\frac{M_0 | \psi \rangle}{|a|} = \frac{a}{|a|} |0\rangle \tag{2.97}$$

$$\frac{M_1 | \psi \rangle}{|b|} = \frac{b}{|b|} |1\rangle \tag{2.98}$$

在 2.2.7 节将看到像 $a/|a|$ 这样的模为 1 的倍数实际上可以忽略，因此测后有效状态实际上正如第 1 章描述的是 $|0\rangle$ 和 $|1\rangle$.

假设 3 是基本假设，这让很多人感到困惑. 测量设备是量子力学系统，因此被测量子系统和测量设备是更大的孤立量子系统的一部分（也许需要包括被测量子系统和测量设备以外的量子系统以获得一个完整的孤立系统，但重要的是这是可以做到的）. 根据假设 2，更大的孤立量子系统可以由酉演化描述. 假设 3 可以作为结论从这个图像推导出来吗？尽管人们在这个问题上花了相当多的努力，物理学家仍在争论这是否可能. 不过，我们将采取非常实际的做法：在条件清楚的情况下应用假设 2 和假设 3，而不关心如何从一个假设推导另一个假设的问题.

下面几节我们将把假设 3 应用到几种基本但非常重要的测量场景：2.2.4 节

考虑区分一组量子状态的问题；2.2.5 节说明假设 3 的一种特殊情况，投影(projective)测量或 von Neumann 测量；2.2.6 节说明假设 3 的另一种特殊情况，POVM 测量. 许多量子力学的引论材料只讨论投影测量，而忽略对假设 3 的完整讨论或 POVM 测量的基本内容，因此，我们在盒子 2.5 中对不同类型测量之间关系进行评论.

练习 2.57(串联的测量等于单次测量) 设$\{L_l\}$和$\{M_m\}$是两组测量算子，证明先经过由一个测量算子$\{L_l\}$定义的测量后经过由测量算子$\{M_m\}$定义的测量，在物理上等价于一个由测量算子$\{N_{lm}\}$定义的单次测量，算子$\{N_{lm}\}$具有表示 $N_{lm} \equiv M_m L_l$.

2.2.4 区分量子状态

假设 3 的一个重要应用是区分量子状态. 经典世界里，研究对象的不同状态至少原则上常常是可以区分的. 例如，我们至少在理想情况下总可以知道硬币是正面还是反面向上，而在量子力学中，情况较复杂. 在 1.6 节，我们的论证倾向于支持非正交量子状态不可区分，现在以假设 3 为基础，我们可以给出对这一事实更令人信服的说明.

像量子计算与量子信息中许多其他概念一样，不可区分性通过一个包括 Alice 和 Bob 的双方游戏的类比来说明，这最容易理解. Alice 从两人都知道的某个固定状态集合中选择一个状态$|\psi_i\rangle (1 \leqslant I \leqslant n)$，她把$|\psi_i\rangle$交给 Bob，Bob 的任务是找出 Alice 给他状态的指标 i.

设状态集$|\psi_i\rangle$是正交的，于是 Bob 可以通过下面的过程做一个量子测量，来区分这些状态. 对每个指标 i 定义测量算子 $M_i \equiv |\psi_i\rangle\langle\psi_i|$，再定义一个测量算子 M_0 为半正定算子 $I - \sum_{i \neq 0} |\psi_i\rangle\langle\psi_i|$ 的非负平方根. 这些算子满足完备性关系，并且如果状态是$|\psi_i\rangle$，则 $p(i) = \langle\psi_i|M_i|\psi_i\rangle = 1$，测量结果肯定是 i. 因此，可以可靠地区分正交状态集$|\psi_i\rangle$.

与之对照，如果状态集$|\psi_i\rangle$不是正交的，那么可以证明没有量子测量可以区分这些状态. 思路是 Bob 做一个由测量算子 M_j 和输出 j 描述的测量. Bob 根据测量结果，用某些规则 $i = f(j)$来猜测指标 i，其中 $f(j)$表述猜测规则. Bob 不能区分非正交状态$|\psi_1\rangle$和$|\psi_2\rangle$的关键原因是，$|\psi_2\rangle$可以分解出一个平行于$|\psi_1\rangle$的(非零)分量和一个正交于$|\psi_1\rangle$的分量. 设 j 是使 $f(j) = 1$ 的测量结果，即当观察到 j 时，Bob 猜测状态是$|\psi_1\rangle$. 但由于$|\psi_2\rangle$有分量平行于$|\psi_2\rangle$，当状态是$|\psi_2\rangle$时，Bob 就有不为零的概率得到 j，于是有时 Bob 会误判状态. 盒子 2.3 给出非正交状态不可区分的更严格的说明，但这里我们给出了最根本的思想.

盒子 2.3 非正交状态不能可靠区分的证明

用反证法证明：没有测量可以区分非正交状态$|\psi_1\rangle$和$|\psi_2\rangle$. 反设这种测量是可能的，如果状态是$|\psi_1\rangle$($|\psi_2\rangle$)，则测量到 j 使 $f(j)=1$($f(j)=2$)的概率必为 1. 定义 $E_i \equiv \sum_{j:f(j)=i} M_j^\dagger M_j$，这些观察可以写作

$$\langle\psi_1|E_1|\psi_1\rangle = 1, \quad \langle\psi_2|E_2|\psi_2\rangle = 1 \tag{2.99}$$

由于 $\sum_i E_i = I$，故 $\sum_i \langle\psi_1|E_i|\psi_1\rangle = 1$，而由于$\langle\psi_1|E_1|\psi_1\rangle=1$，故必有$\langle\psi_1|E_2|\psi_1\rangle=0$，于是$\sqrt{E_2}|\psi_1\rangle=0$. 设我们有分解$|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\varphi\rangle$，其中$|\varphi\rangle$与$|\psi_1\rangle$正交，$|\alpha|^2+|\beta|^2=1$，且$|\beta|<1$，因为$|\psi_1\rangle$和$|\psi_2\rangle$非正交，于是$\sqrt{E_2}|\psi_2\rangle = \beta\sqrt{E_2}|\varphi\rangle$，这蕴含了与式(2.99)的矛盾，因为

$$\langle\psi_2|E_2|\psi_2\rangle = |\beta|^2\langle\varphi|E_2|\varphi\rangle \leqslant |\beta|^2 < 1 \tag{2.100}$$

其中倒数第二个不等式来自以下事实

$$\langle\varphi|E_2|\varphi\rangle \leqslant \sum_i \langle\varphi|E_i|\varphi\rangle = \langle\varphi|\varphi\rangle = 1 \tag{2.101}$$

2.2.5 投影测量

本节将说明一般测量假设 3 的一个重要特例，投影测量. 本书关于量子计算与量子信息的内容主要应用的是投影测量. 事实上，当增加了假设 2 中描述的酉变换的能力后，投影测量实际上等价于一般测量假设. 我们将在 2.2.8 节详细说明这种等价性，因为对于投影测量的测量假设与假设 3 的一般测量假设表面上相当不同.

投影测量 投影测量由被观测系统状态空间上的一个可观测量 Hermite 算子 M 描述. 该可观测量具有谱分解

$$M = \sum_m mP_m \tag{2.102}$$

其中 P_m 是到特征值 m 的本征空间 M 上的投影. 测量的可能结果对应于测量算子的特征值 m. 测量状态 ψ 时，得到结果 m 的概率为

$$p(m) = \langle\psi|P_m|\psi\rangle \tag{2.103}$$

给定测量结果 m，测量后量于系统的状态立即为

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}} \tag{2.104}$$

投影测量可以视为假设 3 的特殊情况. 设假设 3 中的测量算子除了满足完备性关系 $\sum_m M_m^\dagger M_m = I$，还满足 M_m 是正交投影算子的条件，即 M_m 是 Hermite 的，且 $M_m M_{m'} = \delta_{m,m'} M_m$，有了这些附加限制，假设 3 退化为刚刚定义的投影测量.

盒子 2.4 Heisenberger 测不准原理

也许量子力学最有名的结果就是 Heisenberger 测不准原理了. 设 A 和 B 是两个 Hermite 算子，而 $|\psi\rangle$ 是一个量子状态，设 $\langle\psi|AB|\psi\rangle = x + iy$，其中 x 和 y 是实数. 注意 $\langle\psi|[A,B]|\psi\rangle = 2iy$ 和 $\langle\psi|\{A,B\}|\psi\rangle = 2x$，这蕴含

$$|\langle\psi|[A,B]|\psi\rangle|^2 + |\langle\psi|\{A,B\}|\psi\rangle|^2 = 4|\langle\psi|AB|\psi\rangle|^2 \tag{2.105}$$

由 Chauchy-Schwarz 不等式，

$$|\langle\psi|AB|\psi\rangle|^2 \leqslant \langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle \tag{2.106}$$

结合式(2.105)，并去掉非负项，给出

$$|\langle\psi|[A,B]|\psi\rangle|^2 \leqslant 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle. \tag{2.107}$$

设 C 和 D 是两个可观测量，以 $A = C - \langle C\rangle$ 和 $B = D - \langle D\rangle$ 代入上式，我们得到 Heisenberger 测不准原理的常见形式

$$\Delta(C)\Delta(D) \geqslant \frac{|\langle\psi|[C,D]|\psi\rangle|}{2} \tag{2.108}$$

需要当心关于这个测不准原理的一种常见的误解，即认为观测 C 精确到 $\Delta(C)$，会引起 D 的值受到大小为 $\Delta(D)$ 的干扰，$\Delta(D)$ 满足类似于式(2.108)的某种关系. 虽然量子力学中的测量会干扰被测系统，但这绝对不是测不准原理的含义.

测不准原理的正确解释是：如果我们制备大量具有相同状态 $|\psi\rangle$ 的量子系统，并对一部分系统测量 C，另一部分系统测量 D，那么 C 的结果的标准偏差 $\Delta(C)$ 乘以 D 的结果的标准偏差 $\Delta(D)$ 将满足不等式(2.108).

作为测不准原理的一个例子，考虑采用测量算子 X 和 Y 对量子状态 $|0\rangle$ 下测量时的可观测量 X 和 Y. 式(2.70)中我们给出过 $[X,Y] = 2iZ$，于是测不准原理告诉我们

$$\Delta(X)\Delta(Y) \geqslant |\langle 0|Z|0\rangle| = 1 \tag{2.109}$$

一个基本结论是如直接计算可以验证的，$\Delta(X)$ 和 $\Delta(Y)$ 一定都严格大于 0.

投影测量具有许多好的性质，特别地，很容易计算投影测量的平均值. 由定义，测量的平均值(参看附录 A 中概率的基本定义和结果)是

$$E(M) = \sum_m m p(m) \tag{2.110}$$

$$= \sum_m m\langle\psi|P_m|\psi\rangle \tag{2.111}$$

$$= \langle\psi|\left(\sum_m m P_m\right)|\psi\rangle \tag{2.112}$$

$$= \langle\psi|M|\psi\rangle \tag{2.113}$$

这是一个非常有用的公式，可以简化许多计算. 可观测量 M 的平均值常写作 $\langle M\rangle \equiv \langle\psi|M|\psi\rangle$.

从这个平均值公式可导出与观测 M 相联系的标准偏差的一个公式

$$[\Delta(M)]^2 = \langle (M-\langle M\rangle)^2\rangle \tag{2.114}$$

$$= \langle M^2\rangle - \langle M\rangle^2 \tag{2.115}$$

标准差是测量 M 的观测值典型分散程度的一个度量. 特别地，如果进行大量状态为 $|\psi\rangle$ 观测的 M 实验，则观测值的标准差 $[\Delta(M)]^2$ 由公式 $[\Delta(M)]^2 = \langle M^2\rangle - \langle M\rangle^2$ 决定. 这个对可观测量给出的测量和标准差的公式是导出诸如 Heisenberg 测不准原理结果的一种优美方法(参看盒子 2.4).

练习 2.58　设量子系统处在可观测量 M 的某个本征态 $|\psi\rangle$，相应的特征值为 m，求平均观测值和标准差.

有两个广泛使用的关于测量的说法值得一提. 人们常简单地列出一组满足关系 $\sum_m P_m = I$ 和 $P_m P_{m'} = \delta_{mm'} P_m$ 的正交投影算子 P_m，而不是给出观测量来描述投影测量，这种做法的相应观测量为 $M = \sum_m m P_m$. 另一广泛采用术语"在基 $|m\rangle$ 下测量"，其中 $|m\rangle$ 构成标准正交基，就是指进行使用投影 $P_m = |m\rangle\langle m|$ 的投影测量.

让我们来看一个单量子比特上投影测量的例子. 首先是可观测量 Z 的测量，其特征值是 $+1$ 和 -1，相应的特征向量是 $|0\rangle$ 和 $|1\rangle$. 于是，例如，测量 Z 对状态 $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$，得到结果 $+1$ 的概率为 $\langle\psi|0\rangle\langle 0|\psi\rangle = 1/2$，类似地得到结果 -1 的概率为 $1/2$. 更一般地，设 $\boldsymbol{v}$ 是任意三维实向量，则可以定义观测量

$$\boldsymbol{v}\cdot\boldsymbol{\sigma} \equiv v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3 \tag{2.116}$$

这个观测量的测量由于历史原因有时称为对自旋沿 $\boldsymbol{v}$ 轴的测量. 下面两个练习中将得到该测量的一些初等，但很重要的性质.

练习 2.59　设量子比特处于 $|0\rangle$ 状态，且我们测量可观测量 X，求 X 的平均值和标准差.

练习 2.60　证明 $\boldsymbol{v}\cdot\boldsymbol{\sigma}$ 的特征值是 ± 1，且按相应本征空间的投影分别是 $P_\pm = (I \pm \boldsymbol{v}\cdot\boldsymbol{\sigma})/2$.

练习 2.61　假设测量之前的状态是 $|0\rangle$，计算对测量算子 $\boldsymbol{v}\cdot\boldsymbol{\sigma}$ 得到 $+1$ 的概率，求得到 $+1$ 后的系统状态.

2.2.6　POVM 测量

量子测量假设，即假设 3，涉及两个要素. 首先，它给出一个描述测量统计特性的规则，即分别得到不同测量结果的概率；其次，它给出描述测量后，系统状态的规则. 不过，对某些应用，系统测量后的状态几乎没有什么意义，主要关心的是系统得

到不同结果的概率. 例如,仅在结束阶段对系统进行一次测量的实验就是这种情况. 称为 POVM 形式体系的数学工具特别适合于分析在这类情况的测量结果(字头缩写 POVM 是一个技术术语,表示 positive operator-valued measure 半正定算子值测量,本书不作深入讨论),该形式体系是测量假设 3 一般描述的简单结论,但 POVM 理论非常优美并且应用广泛,故值得在此特别讨论.

设测量算子 M_m 在状态为 $|\psi\rangle$ 的量子系统上进行测量,则得到结果 m 的概率由 $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$ 给出. 如果定义

$$E_m \equiv M_m^\dagger M_m \tag{2.117}$$

则根据假设 3 和初等线性代数可知,E_m 是满足 $\sum_m E_m = I$ 和 $p(m) = \langle\psi|E_m|\psi\rangle$ 的半正定算子. 于是算子集合 E_m 足以确定不同测量结果的概率,算子 E_m 称为与测量相联系的 POVM 元,完整的集合 $\{E_m\}$ 称为一个 POVM.

由测量算子 P_m 描述的投影测量,其中 P_m 是满足 $P_m P_{m'} = \delta_{mm'} P_m$ 和 $\sum_m P_m = I$ 的投影算子,就是 POVM 的例子. 在此例中(且仅对此例)所有的 POVM 元与测量算子本身相同,因为 $E_m \equiv P_m^\dagger P_m = P_m$.

练习 2.62 证明测量算子和 POVM 元一致的任何测量都是投影测量.

上面提到 POVM 算子是半正定的且满足 $\sum_m E_m = I$. 设 $\{E_m\}$ 是任意满足 $\sum_m E_m = I$ 的半正定算子集合,证明存在一组测量算子 M_m,来定义由 POVM $\{E_m\}$ 所描述的测量. 定义 $M_m \equiv \sqrt{E_m}$,则我们看到 $\sum_m M_m^\dagger M_m = \sum_m E_m = I$,故集合 M_m 描述了一个具有 POVM $\{E_m\}$ 的测量. 出于这个原因,把 POVM 定义为任意满足如下条件的算子集合 $\{E_m\}$ 是方便的:(1)每个算子 E_m 是半正定的;(2)表达概率和为 1 的完备性 $\sum_m E_m = I$ 成立. 为完成 POVM 的描述,再次注意对给定的 POVM $\{E_m\}$,得到结果 m 的概率由 $p(m) = \langle\psi|E_m|\psi\rangle$ 给出.

我们曾把投影测量看作 POVM 的例子,但因为没有从中获得新的东西,所以并不太令人兴奋. 下面更复杂的例子说明 POVM 形式体系在量子计算与量子信息中作为向导的作用. 设 Alice 交给 Bob 处于 $|\psi_1\rangle = |0\rangle$ 或 $|\psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ 两状态之一的量子比特. 如 2.2.4 节所述,Bob 不可能完全可靠地确定他得到的是 $|\psi_1\rangle$ 还是 $|\psi_2\rangle$,但他可以进行一项只在某些时候区分状态但永远不误判状态的测量. 考虑由三个元素构成的 POVM:

$$E_1 \equiv \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1| \tag{2.118}$$

$$E_2 \equiv \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2} \tag{2.119}$$

$$E_3 = I - E_1 \quad E_2 \tag{2.120}$$

盒子 2.5　一般测量、投影测量和 POVM

量子力学的大多数概论材料只介绍投影测量，以致许多物理学家不熟悉假设 3 中对测量的一般描述，也可能不熟悉 2.2.6 节中描述的 POVM 形式体系. 大多数物理学家没有学到测量的一般形式是因为大多数物理系统只能进行非常粗糙的测量.

在量子计算与量子信息中，我们的目标是在精细的水平上控制测量的过程，因此更全面的测量形式是有帮助的.

当然，如 2.2.8 节所述，当同时考虑量子力学的其他公理时，投影测量加上酉操作事实上完全等价于一般测量，因此，掌握了投影测量的物理学家会问：从假设 3 的一般测量开始的目的何在？原因是多方面的. 首先，从数学上看，一般测量在某种意义下更简单，因为涉及到测量算子的限制较少，例如对一般测量，没有像对投影测量的 $P_i P_j = \delta_{ij} P_j$ 条件那样的限制，这个简化的结构也带给一般测量许多投影测量所不具备的有用性质. 其次，量子计算与量子信息中存在的重要问题——如区分一组量子状态的最优方式——的答案涉及一般测量，而不是投影测量.

选择从假设 3 开始的第三个理由和投影测量的一个称为可重复性的性质有关. 投影测量在如下意义下可以重复：若进行一次投影测量，得到结果 m，重复测量会再次得到 m 而不会改变状态. 为明确这一点，设 $|\psi\rangle$ 为初态，第一次测量后的状态是 $|\psi_m\rangle = (P_m|\psi\rangle)/\sqrt{\langle\psi|P_m|\psi\rangle}$，应用 P_m 到 $|\psi_m\rangle$ 并不会改变它，于是有 $\langle\psi_m|P_m|\psi_m\rangle = 1$，故重复测量每次都得到 m，且不改变状态.

投影测量的可重复性提示我们，量子力学中的许多重要测量不是投影测量. 例如，如果我们用涂有银的屏去测量光子的位置，我们就在测量过程中毁灭了光子，这当然使重复测量光子位置成为不可能！许多其他量子测量在与投影测量相同的意义下也是不可重复的，对这些测量就必须采用假设 3 的一般测量假设了. POVM 处在什么样的理论位置？最好将 POVM 视为为研究一般测量的统计特性提供最简单的方法，而不需要知道测量后状态的特殊测量，它有时可以为量子测量的研究提供额外的灵感的方便的数学工具.

可以直接验证这些半正定算子满足完备性关系 $\sum_m E_m = I$，因此构成合格的 POVM.

设 Bob 收到的是状态 $|\psi_1\rangle = |0\rangle$，他进行 POVM $\{E_1, E_2, E_3\}$ 描述的测量. 得到结果 E_1 的概率是 0，因为 E_1 使 $\langle\psi_1|E_1|\psi_1\rangle = 0$. 于是，如果测量的结果是 E_1，

Bob有把握得出，他收到的是$|\psi_2\rangle$；类似推理表明如果测量结果是E_2，那么Bob收到的必为$|\psi_1\rangle$；有时Bob可能测得E_3，他就不能对所收到的状态作出任何判断. 不过关键在于，Bob永远不会对所收到的状态作出误判，这个不错性是以有时Bob得不到判别状态的信息为代价的.

这个简单的例子说明在仅关心测量统计的情况下，POVM形式体系是对量子测量的认识的简单直观途径. 本书后面的许多场合中，我们将只关心测量的统计，因此会用POVM测量而不是假设3的一般测量.

练习 2.63 设测量由测量算子组M_m给出，证明存在酉算子组U_m使得$M_m = U_m\sqrt{E_m}$，其中E_m是与测量相联系的POVM.

练习 2.64 设Bob收到一个从线性无关组$|\psi_1\rangle,\cdots,|\psi_m\rangle$中选出的量子状态，构造一个POVM$\{E_1,E_2,\cdots,E_{m+1}\}$，使得如果结果是$E_i$，$1\leqslant i\leqslant m$，则Bob可以确认他收到的是状态$|\psi_i\rangle$(POVM必须使对每个$i$，$\langle\psi_i|E_i|\psi_i\rangle>0$).

2.2.7 相位

相位是量子力学中的常用术语，依据上下文具有几个不同的含义. 下面就概括一下这些含义. 例如，状态$e^{i\theta}|\psi\rangle$，其中$|\psi\rangle$是状态向量，θ是实数. 我们说除了全局相位因子(global phase factor)$e^{i\theta}$，状态$e^{\theta}|\psi\rangle$与$|\psi\rangle$相等. 有趣的是这两个状态的测量统计是相同的. 为明确这一点，设M_m是与某个量子测量相联系的测量算子，注意得到测量结果m的概率分别为$\langle\psi|M_m^\dagger M_m|\psi\rangle$和$\langle\psi|e^{-i\theta}M_m^\dagger M_m e^{i\theta}|\psi\rangle = \langle\psi|M_m^\dagger M_m|\psi\rangle$，于是从观察的角度，这两个状态是等同的，所以，可以忽略全局相位因子，因为它与物理系统的可观测性质无关.

另一类相位称为相对相位(relative phase)，含义很不相同. 考虑状态

$$\frac{|0\rangle+|1\rangle}{\sqrt{2}} \quad \text{和} \quad \frac{|0\rangle-|1\rangle}{\sqrt{2}} \tag{2.121}$$

第一个状态中$|1\rangle$的幅度是$1/\sqrt{2}$，第二个状态中幅度是$-1/\sqrt{2}$，两种情况的幅度的大小是一样的，但符号不同. 更一般地，我们说两个幅度a和b，相差一个相对相位，如果存在实数θ，使得$a=\exp(i\theta)b$，如果在此基下的每个幅度都由一个相位因子联系，称两个状态在某个基下，差一个相对相位. 例如，上述两个状态除了一个相对相移之外是一致的，因为$|0\rangle$的幅度一致(相对相位因子为1)，而$|1\rangle$的幅度仅差一个相对相位因子-1. 相对相位因子和全局相位因子的区别在于相对相位因子可以依幅度不同而不同，这使得相对相位依赖基选择，这不同于全局相位. 结果是，在某个基下，仅相对相位不同的状态具有物理可观测的统计差别，而不能像仅差全局相位因子状态那样，把这些状态视为物理等价.

练习 2.65 在一个基下把状态$(|0\rangle+|1\rangle)/\sqrt{2}$和$(|0\rangle-|1\rangle)/\sqrt{2}$表示成精确

到差一个相对相移.

2.2.8　复合系统

设想我们感兴趣的是两个(以上)不同物理系统组成的复合量子系统,如何描述该复合系统的状态?下面的假设描述了如何从分系统的状态空间构造出来复合系统的状态空间.

假设 4　复合物理系统的状态空间是分物理系统状态空间的张量积,若将分系统编号为 1 到 n,系统 i 的状态被置为 $|\psi_i\rangle$,则整个系统的总状态为 $|\psi_1\rangle\otimes\cdots\otimes|\psi_n\rangle$.

为什么用张量积作为描述复合物理系统的状态空间的数学结构?在一个层面上,我们可以不把它归结为更基本的概念,而是简单地作为基本假设来接受,并继续我们的讨论,毕竟,我们肯定期望用某种规范方法描述量子力学复合系统.能通过其他方式得到这个假设吗?下面是有时会用到的一个经验性推导.物理学家有时喜欢提到量子力学的叠加原理(superposition principle of quantum mechanics),指的是,如果 $|x\rangle$ 和 $|y\rangle$ 是量子系统的两个状态,那么它们的任意叠加 $\alpha|0\rangle+\beta|1\rangle$ 也应该是量子系统的一个可能状态,其中 $|\alpha|^2+|\beta|^2=1$.对于复合系统,很自然认为如果 $|A\rangle$ 是系统 A 的一个状态,$|B\rangle$ 是系统 B 的一个状态,则相应地应该有某个状态,可以记作 $|A\rangle|B\rangle$,属于联合系统 AB.应用叠加原理到这种乘积形式的状态,就得到如上提出的张量积.我们没有把叠加原理视为我们量子力学描述的一个基本部分,因为这算不上是一种推导,但它让我们看到同一思想有时可以有不同表现形式.

复合系统在文献中有许多不同的记号,这种多样化的部分原因是不同的符号更适合不同的应用,偶尔引入一些专门符号有时很方便.现在提一下一个在上下文不明确时,对表示不同系统状态和算子有用的下标符号.例如,在包含三个量子比特的系统中,用 X_2 表示作用在第二个量子比特上的 Pauli 算子 σ_x.

练习 2.66　证明对处在状态 $(|00\rangle+|11\rangle)/\sqrt{2}$ 的双量子比特系统的观测量 X_1 Z_2 测量的平均值为零.

2.2.5 节曾指出投影测量加上酉动态就可以实现一般测量,这个命题的证明要用到复合量子系统,是假设 4 作用的很好体现.设有一个状态空间为 Q 的量子系统,希望在系统 Q 上进行由测量算子 M_m 定义的测量.为此,引入状态空间为 M 的辅助系统,该系统有一个与可能得到的测量结果一一对应的标准正交归一基 $|m\rangle$.这个辅助系统可以认为仅仅是一个出现在我们结构中的一个数学装置,也可认为是为解决问题而引入的状态空间满足要求性质的附加量子系统.

令 $|0\rangle$ 是 M 的任一固定状态,在 Q 中状态 $|\psi\rangle$ 和状态 $|0\rangle$ 的积 $|\psi\rangle|0\rangle$ 上,定义

一个酉算子 U 如下：

$$U|\psi\rangle|0\rangle \equiv \sum_m M_m|\psi\rangle|m\rangle \tag{2.122}$$

利用状态集 $|m\rangle$ 的标准正交性和完备性 $\sum_m M_m^\dagger M_m = I$，可知 U 保持形如 $|\psi\rangle|0\rangle$ 状态之间的内积，即

$$\langle\varphi \quad \langle 0|U^\dagger U|\psi\rangle|0\rangle = \sum_{m,m'}\langle\varphi|M_m^\dagger M_m|\psi\rangle\langle m|m'\rangle \tag{2.123}$$

$$= \sum_m \langle\varphi|M_m^\dagger M_m|\psi\rangle \tag{2.124}$$

$$= \langle\varphi|\psi\rangle \tag{2.125}$$

由练习 2.67 的结果得到，U 可以扩展为空间 $Q\otimes M$ 上的酉算子，我们仍记为 U.

练习 2.67 设 V 是 Hilbert 空间且 W 是其子空间，设 $U: W\to V$ 是一个保持内积的线性算子，即 W 中对任意 $|w_1\rangle$ 和 $|w_2\rangle$ 有

$$\langle w_1|U^\dagger U|w_2\rangle = \langle w_1|w_2\rangle \tag{2.126}$$

证明存在扩张 U 的酉算子 U'：$V\to V$，即对所有 W 中的 $|w\rangle$ 成立 $U'|w\rangle = U|w\rangle$，但 U' 定义在整个空间 V 上. 通常略去符号“′”，仍用 U 表示其扩张.

令 U 作用于 $|\psi\rangle|0\rangle$ 后，设对两个系统进行由投影 $P_m \equiv I_Q\otimes|m\rangle\langle m|$ 描述的投影测量，结果 m 出现的概率是

$$p(m) = \langle\psi|\langle 0|U^\dagger P_m U|\psi\rangle|0\rangle \tag{2.127}$$

$$= \sum_{m',m''}\langle\psi|M_{m'}^\dagger\langle m'|(I_Q\otimes|m\rangle\langle m|)M_{m''}|\psi\rangle|m''\rangle \tag{2.128}$$

$$= \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{2.129}$$

正如假设 3 所给出的，测量后联合系统 QM 的状态依赖于测量结果 m，由下式给出

$$\frac{P_m U|\psi\rangle|0\rangle}{\sqrt{\langle\psi|\langle 0|U^\dagger P_m U|\psi\rangle|0\rangle}} = \frac{M_m|\psi\rangle|m\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \tag{2.130}$$

系统 M 的测后状态为 $|m\rangle$，而系统 Q 的状态为

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \tag{2.131}$$

这正如假设 3 所述. 因此酉动态、投影测量和引入辅助系统的能力结合在一起可实现假设 3 描述的任意形式的测量.

假设 4 还使我们能够定义与复合量子系统有关的、最有趣也最令人困惑的概念——纠缠(entanglement). 考虑双量子比特状态

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.132}$$

这个状态具有以下值得注意的性质：不存在单个量子比特的状态 $|a\rangle$ 和 $|b\rangle$，使 $|\psi\rangle = |a\rangle|b\rangle$. 该事实读者可以自己通过练习 2.68 来证实.

练习 2.68　证明对任何单量子比特状态 $a\rangle$ 和 $b\rangle$，都有 $|\psi\rangle \neq |a\rangle|b\rangle$.

复合系统中具有这条性质(不能被写作它的分系统状态的张量积)的状态称为纠缠状态(entangled state). 纠缠态在量子计算与量子信息中扮演关键角色，会在本书中反复出现，但它的起因尚不完全清楚. 在 1.3.7 节已经看到量子隐形传态中纠缠现象所起的关键作用了，本章给出纠缠量子状态奇异效应的另外两个例子，超密编码(2.3 节)和 Bell 不等式的违反(2.6 节).

2.2.9　量子力学：总览

我们现在已经说明了量子力学的所有基本假设，本书的大部分内容将以这些假设为根据推导结论，现在从全局观点来复习一下这些假设.

假设 1 通过确定如何描述一个孤立量子系统的状态来设定量子力学的研究范围. 假设 2 告诉我们封闭量子系统的动态由 Schrödinger 方程，也就是酉演化，来描述. 假设 3 告诉我们如何通过规定测量的描述来从量子系统获取信息. 假设 4 告诉我们如何把不同量子系统的状态空间组合成复合系统.

至少从经典眼光看，量子力学的独特之处在于不能直接观察状态向量. 这有点像国际象棋游戏，那里你只能知道棋子在棋盘上的排列，而永远无法找出每个棋子的精确位置. 经典物理学(和我们的直觉)告诉我们一个对象的基本属性，如能量、位置和速率，这些都是可以通过观察得到的. 在量子力学中，这些量不再是基本的，被不能直接观察的状态向量取代. 量子力学中好像存在一个只能间接和不完全访问的隐藏的世界. 而且，只观察一个经典系统不一定引起系统状态的改变. 想象一下每次你观察球都会改变它的位置，那么打网球将会多么困难. 但按照假设 3，观察量子系统是一个破坏性的过程，通常要改变系统的状态.

从量子力学的这些独特特征可以得出什么结论？有可能把量子力学重新描述成数学上等价的一种更像经典物理学的结构吗？2.6 节我们将证明 Bell 不等式，这个惊人的结果表明任何重新描述量子力学的企图都注定会失败，我们无法摆脱量子力学反直观的性质了. 当然，我们正确的反应应该是高兴，而不是伤心. 它给了我们一个开发量子力学直观化思想工具的机会，而且，可以利用状态向量的隐含特性完成在经典世界不可能的量子信息处理任务. 没有这个反直观行为，量子计算与量子信息将失去很多意义.

我们还可以转而问自己："既然量子力学和经典物理学如此不同，那么现实世界为什么看来如此经典呢？"在日常生活中为什么看不到隐含状态的迹象？事实上，经典世界可以作为量子力学在日常生活的时间、长度和质量尺度上的近似描述推导出来. 说明量子力学如何推导出经典物理学已超出了本书的范围，不过感兴趣的读者可以查阅第 8 章末的"历史和进一步阅读的材料".

2.3 应用：超密编码

超密编码(superdense coding)是初等量子力学的一个简单而惊人的应用，它以具体和不平凡的方式把前面几节涉及的初等量子力学的所有基本概念结合起来，并且是用量子机器可以完成的信息处理任务的一个理想例子.

超密编码涉及习惯上称为 Alice 和 Bob 的双方，他们彼此相距很远，他们的任务是 Alice 要给 Bob 传送一些经典信息. 设 Alice 有两个经典比特的信息要发给 Bob，但只被允许发一个单量子比特给 Bob. 她可以达到目的吗？

超密编码告诉我们，答案是肯定的. 设 Alice 和 Bob 开始共享一对处于纠缠态

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.133}$$

的量子比特，最初 Alice 拥有第一量子比特，而 Bob 拥有第二量子比特，如图 2.3 所示. 注意 $|\psi\rangle$ 是一个固定的状态，为制备这个状态，Alice 不需要发给 Bob 任何量子比特. 实际上，某个第三方可能事先制备了该纠缠态，把其中一个量子比特发送给 Alice，另一个发给 Bob.

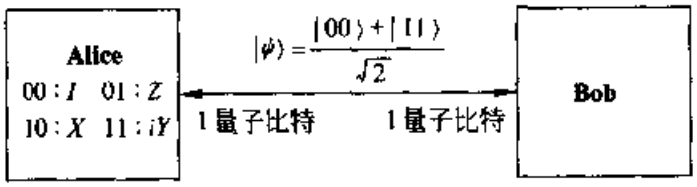


图 2.3 超密编码的起始配置，其中 Alice 和 Bob 各持有纠缠量子比特对的一半. Alice 可以用超密编码传送给 Bob 两个经典比特信息，而只用到一个单量子比特的通信和这个提前共享的纠缠态.

通过把所拥有的单量子比特发给 Bob，Alice 事实上可以传两个经典比特的信息给 Bob. 下面是她采取的步骤. 如果希望把比特串"00"发给 Bob，她不需要对她的量子比特做什么；如果希望发送"01"，则在量子比特上应用相位翻转 Z；如果希望发送"10"，则应用量子非门 X 到量子比特上；如果希望发送"11"，则应用 iY 到量子比特上. 结果很容易看出，为以下四个状态：

$$00 : |\psi\rangle \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.134}$$

$$01 : |\psi\rangle \rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{2.135}$$

$$10 : |\psi\rangle \rightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}} \tag{2.136}$$

$$\Pi_4 : |\psi\rangle \rightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{2.137}$$

如我们在1.3.6节中注意到的，这四个状态称为Bell基、Bell态或EPR对，以纪念几位首先发现纠缠现象新奇之处的先驱. 注意Bell态构成一个标准正交基，故可以通过适当的量子测量来区分它们. 如果Alice把她的量子比特发送给Bob，使Bob拥有全部两个量子比特，则通过在Bell基态中的一次测量，Bob可以确定Alice要送给他的是四个可能比特串中的哪一个.

总之，仅与一个单量子比特打交道，Alice就可以把两个比特的信息传给Bob. 当然，协议涉及两个量子比特，但Alice永远也不需要和第二量子比特打交道. 从经典角度看，如我们在第12章将证明的，Alice不可能只传送一个经典比特而完成任务. 这个令人瞩目的超密编码协议已经在实验室中得到部分证实(参看"历史和进一步阅读的材料"所包含的实验验证方面的参考文献). 在后面的章节中，我们将看到量子力学用于执行量子信息处理任务的许多其他例子，其中某些比超密编码更引人入胜. 不过，从这个漂亮的例子已经可以看到一个关键点：信息是物理的，诸如量子力学的惊人理论也许预示着惊人的信息处理能力.

练习 2.69 验证Bell基构成双量子比特空间的一个标准正交基.

练习 2.70 设E是作用在Alice的量子比特上的任意半正定算子，证明当$|\psi\rangle$是四个Bell态之一时，$\langle\psi|E\otimes I|\psi\rangle$取相同的值. 设某个怀有恶意的第三方(Eve)在超密编码协议中在发送给Bob的途中截获了Alice的量子比特，Eve可能推断出Alice试图发送的是四个比特串00,01,10,11中的哪一个吗？如果是这样，如何推断？如果不是这样，为什么？

2.4 密度算子

我们已经用状态向量的语言描述了量子力学，另一种描述是采用称为密度算子或密度矩阵的工具. 这种形式在数学上等价于状态向量方法，但它为量子力学某些最常见场合提供了方便得多的语言. 下面3节描述量子力学的密度算子形式：2.4.1节用量子状态的系综(ensemble)概念来引入密度算子；2.4.2节阐述密度算子的某些一般性质；最后，2.4.3节给出密度算子真正漂亮的应用——作为描述复合量子系统的个别子系统的工具.

2.4.1 量子状态的系综

密度算子语言为描述状态不完全已知的量子系统提供了一条方便的途径. 确切地，设量子系统以概率p_i处在一组状态$|\psi_i\rangle$的某一个，其中i是一个指标，则称

$\{p_i, |\psi_i\rangle\}$为一个纯态的系综(ensemble of pure state). 系统的密度算子定义为

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{2.138}$$

密度算子常被称作密度矩阵,我们将不区分这两个术语. 实际上,量子力学的全部假设都可以以密度算子的语言重新描述,本节和下节的目的就是解释如何进行这一转换,并说明什么时候有用. 使用密度算子语言或状态向量语言是个人喜好问题,因为两者给出相同结果,不过有时用一种观点处理问题要比另一种观点容易得多.

例如,设封闭量子系统的演化由酉算子U描述,如果系统初态为$|\psi_i\rangle$的概率是p_i,则演化发生后,系统将以概率p_i进入状态$U|\psi_i\rangle$,子是,密度算子的演化可以下式描述

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \xrightarrow{U} \sum_i p_i U |\psi_i\rangle\langle\psi_i| U^\dagger = U\rho U^\dagger \tag{2.139}$$

用密度算子语言描述测量也很容易. 设我们进行由测量算子M_m描述的测量,如果初态是$|\psi_i\rangle$,则得到结果m的概率是

$$p(m|i) = \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle = \mathrm{tr}(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|) \tag{2.140}$$

其中我们已经应用式(2.61),以得到最后一个等式. 由全概率公式(参看附录A中对此的解释和概率论的其他基本符号),得到结果m的概率是

$$p(m) = \sum_i p(m|i)p_i \tag{2.141}$$

$$= \sum_i p_i \,\mathrm{tr}(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|) \tag{2.142}$$

$$= \mathrm{tr}(M_m^\dagger M_m \rho) \tag{2.143}$$

得到测量结果m以后的系统密度算子是什么? 如果初态是$|\psi_i\rangle$,则得到结果m后的状态是

$$|\psi_i^m\rangle = \frac{M_m |\psi_i\rangle}{\sqrt{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle}} \tag{2.144}$$

于是,经过一个得到结果m的测量,我们得到个别概率为$p(i|m)$状态$|\psi_i^m\rangle$的系综. 相应的密度算子ρ_m是

$$\rho_m = \sum_i p(i|m) |\psi_i^m\rangle\langle\psi_i^m| = \sum_i p(i|m) \frac{M_m |\psi_i\rangle\langle\psi_i| M_m^\dagger}{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle} \tag{2.145}$$

但根据初等概率论,$p(i|m) = p(m,i)/p(m) = p(m|i)p_i/p(m)$,代入式(2.143)和式(2.140)得到

$$\rho_m = \sum_i p_i \frac{M_m |\psi_i\rangle\langle\psi_i| M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)} \tag{2.146}$$

$$= \frac{M_m \rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)} \tag{2.147}$$

上面的论述表明，与西演化和测量有关的量子力学基本假设可以用密度算子的语言重新描述. 下节我们将不依赖状态向量概念给出密度算子的一个内在刻画，以完成这个重新描述过程.

不过在此之前，再引入一些语言和一个关于密度算子的事实. 首先是语言. 具有精确已知状态的量子系统称为处于纯态(pure state). 这种情况下，密度算子就是 $\rho = |\psi\rangle\langle\psi|$，否则，$\rho$ 处于混合态(mixed state)，称为是在 ρ 的系综中不同纯态的混合. 练习中要求说明判断状态是纯态还是混合态的一个简单判据：纯态满足 $\mathrm{tr}(\rho^2)=1$，而混合态满足 $\mathrm{tr}(\rho^2)<1$. 关于这个名词有一个提醒：有时人们用术语混合态统称纯态和混合量子态，这种用法的起源似乎蕴含作者不必要假设状态是纯的；第二，术语纯态常用于指一个状态向量 $|\psi\rangle$，以区别于密度算子 ρ.

最后，设想量子系统以概率 p_i 处于状态 ρ_i，不难发现系统可以用密度矩阵 $\sum_i p_i\rho_i$ 来描述. 这一点的证明如下. 设 ρ_i 来自某个纯态的系综 $\{p_{ij}, |\psi_{ij}\rangle\}$(注意 i 是固定的)，于是开始处在状态 $|\psi_{ij}\rangle$ 的概率是 $p_i p_{ij}$，因此系统的密度矩阵是

$$\rho = \sum_{ij} p_i p_{ij} |\psi_{ij}\rangle\langle\psi_{ij}| \tag{2.148}$$

$$= \sum_i p_i \rho_i \tag{2.149}$$

其中用了定义 $\rho_i = \sum_j p_{ij} |\psi_{ij}\rangle\langle\psi_{ij}|$，称 ρ 为具有概率 p_i 的状态 ρ_i 的混合. 这个混合的概念在如量子噪声的分析问题中反复出现，噪声的影响使我们对量子状态的知识中引入了不确定性. 上述测量过程提供了一个简单例子. 想象一下，由于某种原因，测量结果 m 的记录丢失了，我们将以概率 $p(m)$ 处于 ρ_m，但不再知道 m 的实际值，这样，系统的状态就将由密度算子

$$\rho = \sum_m p(m)\rho_m \tag{2.150}$$

$$= \sum_m \mathrm{tr}(M_m^\dagger M_m \rho) \frac{M_m \rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)} \tag{2.151}$$

$$= \sum_m M_m \rho M_m^\dagger \tag{2.152}$$

来描述. 这是一个可以用于作为出发点，来分析系统进一步操作的紧凑公式.

2.4.2　密度算子的一般性质

密度算子虽是作为描述量子状态系综的一条途径引入的，但本节暂且不讨论这个描述，而是对密度算子进行不依赖系综解释的内在刻画. 这使我们能够不以状态向量为基础来完成量子力学的描述，我们也借此机会给出密度算子的许多其他基本性质.

密度算子的算子类由如下有用的定理刻画：

定理 2.5(密度算子的特征) 一个算子 ρ 是和某个系综 $\{p_i, |\psi_i\rangle\}$ 相关联的密度算子，当且仅当它满足如下条件.

(1) (迹条件)ρ 的迹等于 1；

(2) (半正定条件)ρ 是一半正定算子.

证明 设 $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ 是一个密度算子，则

$$\mathrm{tr}(\rho) = \sum_i p_i \,\mathrm{tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i = 1 \tag{2.153}$$

满足迹条件. 设 $|\varphi\rangle$ 是状态空间中任意一个向量，则

$$\langle\varphi|\rho|\varphi\rangle = \sum_i p_i \langle\varphi|\psi_i\rangle\langle\psi_i|\varphi\rangle \tag{2.154}$$

$$= \sum_i p_i |\langle\varphi|\psi_i\rangle|^2 \tag{2.155}$$

$$\geqslant 0 \tag{2.156}$$

满足半正定条件.

反过来，设 ρ 是满足迹和半正定条件的任意算子. 由于 ρ 半正定，它必有谱分解，

$$\rho = \sum_j \lambda_j |j\rangle\langle j| \tag{2.157}$$

其中向量组 $|j\rangle$ 是正交的，且 λ_j 是实数，是 ρ 的非负特征值. 从迹条件可知 $\sum_j \lambda_j = 1$，于是，一个以概率 λ_j 处于状态 $|j\rangle$ 的系统将具有密度算子 ρ，即系综 $\{\lambda_j, |j\rangle\}$ 是产生密度算子 ρ 的状态组的一个系综.

这个定理提供了密度算子的一个内在刻画：我们可以把密度算子定义为一个迹等于 1 的半正定算子. 该定义使我们可以重新在密度算子图像中描述量子力学假设. 为便于参考，我们把新形式的假设全列在这里：

假设 1 任意孤立物理系统与称之为这系统的状态空间相关联，它是个带内积的复向量空间(即 Hibert 空间). 系统由作用在状态空间上的密度算子完全描述，密度算子是一个半正定迹为 1 的算子 ρ. 如果量子系统以概率 p_i 处于状态 ρ_i，则系统的密度算子为 $\sum_i p_i \rho_i$.

假设 2 封闭量子系统的演化由一个酉变换描述，即系统在时刻 t_1 的状态 ρ 和在时刻 t_2 的状态 ρ' 由一个仅依赖于时间 t_1 和 t_2 的酉算子 U 联系，

$$\rho' = U\rho U^\dagger \tag{2.158}$$

假设 3 量子测量是由一组测量算子 $\{M_m\}$ 描述，这些算子作用在所测量的状态空间上，指标 m 指实验中可能出现的测量结果. 如果量子系统在测量前的最后状态是 ρ，则得到结果 m 的概率由

$$p(m) = \mathrm{tr}(M_m^{\dagger} M_m \rho) \tag{2.159}$$

给出，且测量后的系统状态为

$$\frac{M_m \rho M_m^{\dagger}}{\mathrm{tr}(M_m^{\dagger} M_m \rho)} \tag{2.160}$$

测量算子满足完备性方程

$$\sum_m M_m^{\dagger} M_m = I \tag{2.161}$$

假设 4　复合物理系统的状态空间是分物理系统状态空间的张量积，而且，如果有系统 1 到 n，其中系统 i 处于状态 ρ_i，则全系统的共同状态是 $\rho_1 \otimes \rho_2 \otimes \cdots \rho_n$.

当然在数学上，这些密度算子形式描述的量子力学基本假设等价于用状态向量的描述，不过，作为一种认识量子力学的方式，密度算子方法在以下两方面的应用上作用突出：描述状态未知的量子系统和描述复合系统的子系统. 这些内容将在下节讨论，本节余下篇幅将更详细地给出密度矩阵的性质.

练习 2.71(判断一个状态是混合态还是纯态)　令 ρ 是一个密度算子，证明 $\mathrm{tr}(\rho^2) \leqslant 1$，当且仅当 ρ 是纯态，等式成立.

假设密度矩阵的特征值和特征向量对密度矩阵所表示的量子状态系综有特殊重要性是一个迷惑人的(和让人吃惊的、普遍的)错误. 例如，人们可能设想具有密度矩阵

$$\rho = \frac{3}{4} |0\rangle\langle 0| + \frac{1}{4} |1\rangle\langle 1| \tag{2.162}$$

的量子系统必然以 3/4 概率处于状态 $|0\rangle$，而以 1/4 概率处于状态 $|1\rangle$. 然而不见得是这样. 定义

$$|a\rangle \equiv \sqrt{\frac{3}{4}} |0\rangle + \sqrt{\frac{1}{4}} |1\rangle \tag{2.163}$$

$$|b\rangle \equiv \sqrt{\frac{3}{4}} |0\rangle - \sqrt{\frac{1}{4}} |1\rangle \tag{2.164}$$

并且使量子系统状态以 1/2 概率处于状态 $|a\rangle$，1/2 概率处于状态 $|b\rangle$，容易检验相应的密度矩阵为

$$\rho = \frac{1}{2} |a\rangle\langle a| + \frac{1}{2} |b\rangle\langle b| = \frac{3}{4} |0\rangle\langle 0| + \frac{1}{4} |1\rangle\langle 1| \tag{2.165}$$

也就是说两个不同的量子状态系综可产生同一个密度矩阵. 更一般地，密度矩阵的特征值和特征向量仅表示可能产生密度矩阵的许多系综中的一个，没有理由表明哪个系统是特殊的.

在上述讨论的启发下，一个自然的问题是，什么类型的系综产生一个特定的密度矩阵？我们现在给出这个问题的解，它在量子计算与量子信息中有很多的惊人的应用，特别是在理解量子噪声和量子纠错中(第 8 章和第 10 章).

为了方便给出答案，使用未归一化到单位长度的向量 $|\tilde{\psi}_i\rangle$. 设集合 $|\tilde{\psi}_i\rangle$ 生成算

子 $\rho \equiv \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$，因此，与普通的密度算子系综的关联由式 $|\tilde{\psi}_i\rangle = \sqrt{p_i}|\psi_i\rangle$ 来描述. 两组向量 $|\tilde{\psi}_i\rangle$ 和 $|\tilde{\varphi}_j\rangle$ 何时生成同一算子 ρ? 这个问题的答案使我们可以回答什么样的系综产生给定密度矩阵的问题.

定理 2.6(密度矩阵系综中的酉自由度) 当且仅当

$$|\tilde{\psi}_i\rangle = \sum_j u_{ij} |\tilde{\varphi}_j\rangle \tag{2.166}$$

两组向量 $|\tilde{\psi}_i\rangle$ 和 $|\tilde{\varphi}_j\rangle$ 生成相同的密度矩阵，其中 u_{ij} 是带指标 i 和 j 的复酉阵. 并且我们在向量集合 $|\tilde{\psi}_i\rangle$ 或 $|\tilde{\varphi}_j\rangle$ 中向量较少的一个中补充若干 0 向量，以使两个集合的向量个数相等.

作为定理的一个结论，注意当且仅当

$$\sqrt{p_i}|\psi_i\rangle = \sum_j u_{ij}\sqrt{q_j}|\varphi_j\rangle \tag{2.167}$$

对某个酉阵 u_{ij} 成立，$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i| = \sum_j q_i|\varphi_j\rangle\langle\varphi_j|$ 对归一化状态集 $|\psi_i\rangle$ 和 $|\varphi_j\rangle$ 和概率分布 p_i 和 q_j 成立，其中我们可能要向较小的系综添加零概率的项以使两个系综具有同样大小. 因此，定理 2.6 刻画了产生一个给定密度矩阵 ρ 的系综 $\{p_i, |\psi_i\rangle\}$ 包含的自由度. 其实，很容易验证，我们前面给出的一个密度矩阵具有两个不同分解的例子式(2.162)，这是个一般结果的特殊情况. 现在来证明这个定理.

证明 设 $|\tilde{\psi}_i\rangle = \sum_j u_{ij}|\tilde{\varphi}_j\rangle$ 对某酉阵 u_{ij} 成立，则

$$\sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_{ijk} u_{ij}u_{ik}^* |\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_k| \tag{2.168}$$

$$= \sum_{jk}\Big(\sum_i u_{ki}^\dagger u_{ij}\Big)|\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_k| \tag{2.169}$$

$$= \sum_{jk}\delta_{kj}|\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_k| \tag{2.170}$$

$$= \sum_j |\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_j| \tag{2.171}$$

表明 $|\tilde{\psi}_i\rangle$ 和 $|\tilde{\varphi}_j\rangle$ 生成相同的算子.

反过来，设

$$A = \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_j |\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_j| \tag{2.172}$$

令 $A = \sum_k \lambda_k |k\rangle\langle k|$ 为 A 的一个分解，使状态 $|k\rangle$ 为标准正交，且 λ_k 为严格正. 我们的办法是把状态集 $|\tilde{\psi}_i\rangle$ 和状态集 $|\tilde{k}\rangle \equiv \sqrt{\lambda_k}|k\rangle$ 联系起来，并把状态集 $|\tilde{\varphi}_j\rangle$ 和状态集 $|\tilde{k}\rangle$ 类似地联系起来，结合两个关系导出结果. 令 $|\psi\rangle$ 为与 $|\tilde{k}\rangle$ 张成空间标准正交的任意向量，于是 $\langle\psi|\tilde{k}\rangle\langle\tilde{k}|\psi\rangle = 0$ 对所有 k 成立，则

$$0 = \langle\psi|A|\psi\rangle = \sum_i \langle\psi|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|\psi\rangle = \sum_i |\langle\psi|\tilde{\psi}_i\rangle|^2 \tag{2.173}$$

即对所有 i 和所有标准正交于 $|\tilde{k}\rangle$ 张成的空间的 $|\psi\rangle$ 成立 $\langle\psi|\tilde{\psi}_i\rangle=0$. 于是每个 $|\tilde{\psi}_i\rangle$ 可以表示成集 $|\tilde{k}\rangle$ 的一个线性组合，$|\tilde{\psi}_i\rangle=\sum_k c_{ik}|\tilde{k}\rangle$，又由于 $A=\sum_k|\tilde{k}\rangle\langle\tilde{k}|=\sum_i|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$，我们看到

$$\sum_k|\tilde{k}\rangle\langle\tilde{k}|=\sum_{kl}\left(\sum_i c_{ik}c_{il}^*\right)|\tilde{k}\rangle\langle\tilde{l}| \tag{2.174}$$

易知算子组 $|\tilde{k}\rangle\langle\tilde{l}|$ 是线性无关的，因此必然成立 $\sum_i c_{ik}c_{il}^*=\delta_{kl}$. 这保证了可以通过增加额外的列到 c，以得到一个酉阵 v，使得 $|\tilde{\psi}_i\rangle=\sum_k v_{ik}|\tilde{k}\rangle$，其中我们已经在集 $|\tilde{k}\rangle$ 中添加了零向量. 类似地，可找到酉矩阵 w，使得 $|\tilde{\varphi}_j\rangle=\sum_k w_{jk}|\tilde{k}\rangle$. 因此 $|\tilde{\psi}_i\rangle=\sum_j u_{ij}|\tilde{\varphi}_j\rangle$，其中 $u=vw^\dagger$ 是酉的.

练习 2.72(混合态的 Bloch 球面)　1.2 节引入了单量子比特纯态的 Bloch 球面描述，该描述有到混合态的如下重要推广.

(1) 证明任意混合态量子比特的密度矩阵可以写成

$$\rho=\frac{I+\boldsymbol{r}\cdot\boldsymbol{\sigma}}{2} \tag{2.175}$$

其中 $\boldsymbol{r}$ 是实三维向量，满足 $\|\boldsymbol{r}\|\leqslant 1$，这个向量称为状态 ρ 的 Bloch 向量.

(2) 求状态 $\rho=I/2$ 的 Bloch 向量表示.

(3) 证明当且仅当 $\|\boldsymbol{r}\|=1$ 状态 ρ 为纯态.

(4) 证明对纯态，这里给出的 Bloch 向量的描述与 1.2 节给出的一致.

练习 2.73　令 ρ 是密度算子，ρ 的一个最小系综(minimal ensemble)指包含等于 ρ 的秩数目的系综 $\{p_i,|\psi_i\rangle\}$. Hermite 算子 A 的支集是由 A 的非零特征值的特征向量张成的向量空间. 令 $|\psi\rangle$ 为 ρ 支集中的任一状态，证明存在包含 $|\psi\rangle$ 的一个 ρ 的最小系综，并且在任何这样的系综中，$|\psi\rangle$ 必然以概率

$$p_i=\frac{1}{\langle\psi_i|\rho^{-1}|\psi_i\rangle} \tag{2.176}$$

出现，其中 ρ^{-1} 定义为 ρ 的逆，而 ρ 视为仅作用在其支集上(这个定义避免了 ρ 可能不可逆的问题).

2.4.3　约化密度算子

密度算子最深刻的应用也许是作为描述复合系统子系统的工具，这个描述由本节的主题约化密度算子(reduced density operator)提供. 约化密度算子非常重要，事实上它是分析复合量子系统不可缺少的工具.

假设有物理系统 A 和 B，其状态由密度算子 ρ^{AB} 描述，针对系统 A 的约化密度算子定义为

$$\rho^A \equiv \mathrm{tr}_B(\rho^{AB}) \tag{2.177}$$

其中 tr_B 是一个算子映射，称为在系统 B 上的偏迹. 偏迹定义为

$$\mathrm{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) \equiv |a_1\rangle\langle a_2| \mathrm{tr}(|b_1\rangle\langle b_2|) \tag{2.178}$$

其中 $|a_1\rangle$ 和 $|a_2\rangle$ 是状态空间 A 中的两个向量，$|b_1\rangle$ 和 $|b_2\rangle$ 是状态空间 B 中的两个向量. 等式右边的迹运算是系统 B 上的普通迹运算，因此 $\mathrm{tr}(|b_1\rangle\langle|b_2|) = \langle b_2|b_1\rangle$. 我们只是在 AB 的一类特殊算子上定义了偏迹，完成偏迹的定义，需要在式(2.178)上附加对输入为线性的要求.

盒子 2.6 为什么取偏迹?

为什么在描述较大的量子系统时要用偏迹？这样做的原因在于，偏迹在如下意义下，是惟一可以正确描述复合系统子系统内可观测量的运算.

设 M 是系统 A 上的任意可观测量，且有某个测量设备可实现 M 的测量，令 $\tilde{M}$ 为在复合系统 AB 上同一测量的相应的可观测量. 我们要论证 $\tilde{M}$ 等价于 $M \otimes I_B$. 注意若系统 AB 处于状态 $|m\rangle|\psi\rangle$，其中 $|m\rangle$ 是 M 的对应于特征值 m 的本征态，且 $|\psi\rangle$ 是 B 的任意状态，则测量设备必须以概率 1 给出结果 m. 因此，如果 P_m 是可观测量 M 的 m 本征空间上的投影，则相应于 $\tilde{M}$ 的投影为 $P_m \otimes I_B$，于是有

$$\tilde{M} = \sum_m m P_m \otimes I_B = M \otimes I_B \tag{2.179}$$

下一步证明，针对系统局部观测偏迹给出的正确测量统计量. 设在系统 A 上进行观测，此测量由可观测量 M 描述. 物理上的一致性要求任何把状态 ρ^A 和系统 A 联系起来的办法，都应具备如下性质：无论是通过 ρ^A 还是通过 ρ^{AB}，都应该得到相同的测量平均值，即

$$\mathrm{tr}(M\rho^A) = \mathrm{tr}(\tilde{M}\rho^{AB}) = \mathrm{tr}((M \otimes I_B)\rho^{AB}) \tag{2.180}$$

如果选择 $\rho^A \equiv \mathrm{tr}_B(\rho^{AB})$，此式肯定得到满足. 事实上，偏迹是具有这条性质的惟一函数. 为证惟一性，设 $f(\cdot)$ 是任意满足下式的，把 AB 上的密度算子映射到 A 上密度算子的函数

$$\mathrm{tr}(Mf(\rho^{AB})) = \mathrm{tr}((M \otimes I_B)\rho^{AB}) \tag{2.181}$$

对所有可观测量 M 成立. 设 M_i 为 Hermite 算子空间相对 Hilbert-Schmidt 内积 $(X, Y) \equiv \mathrm{tr}(XY)$(对比练习 2.39)的标准正交基，则将 $f(\rho^{AB})$ 在此基上展开，得到

$$f(\rho^{AB}) = \sum_i M_i \, \mathrm{tr}(M_i f(\rho^{AB})) \tag{2.182}$$

$$= \sum_i M_i \mathrm{tr}((M_i \otimes I_B)\rho^{AB}) \tag{2.183}$$

由此可知 f 由式(2.180)惟一决定，同时，偏迹满足式(2.180)，故它是惟一具有此性质的函数.

系统 A 的约化密度算子是系统 A 状态的一个描述，这件事并不显然. 物理上的证据是，约化密度算子为系统 A 上的测量提供了正确的测量统计，这一点在盒子 2.6 中会详细说明. 下面的简单算例也许有助于对约化密度算子的理解. 首先，设量子系统处于 $\rho^{AB}=\rho\otimes\sigma$ 状态，其中 ρ 是系统 A 的一个密度算子，而 σ 是系统 B 的一个密度算子，则

$$\rho^{A}\equiv \mathrm{tr}_B(\rho\otimes\sigma)=\rho\mathrm{tr}(\sigma)=\rho \tag{2.184}$$

类似地，对这个状态 $\rho^{B}=\sigma$. Bell 态 $(|00\rangle+|11\rangle)/\sqrt{2}$ 是一个更不平凡的例子，它具有密度算子

$$\rho=\left(\frac{|00\rangle-|11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00|+\langle 11|}{\sqrt{2}}\right) \tag{2.185}$$

$$=\frac{|00\rangle\langle 00|+|11\rangle\langle 00|-|00\rangle\langle 11|+|11\rangle\langle 11|}{2} \tag{2.186}$$

对第二量子比特取迹，得到对第一量子比特的约化密度算子

$$\rho^{1}=\mathrm{tr}_2(\rho) \tag{2.187}$$

$$=\frac{\mathrm{tr}_2(|00\rangle\langle 00|)+\mathrm{tr}_2(|11\rangle\langle 00|)+\mathrm{tr}_2(|00\rangle\langle 11|)+\mathrm{tr}_2(|11\rangle\langle 11|)}{2} \tag{2.188}$$

$$=\frac{|0\rangle\langle 0|\langle 0|0\rangle+|1\rangle\langle 0|\langle 0|1\rangle+|0\rangle\langle 1|\langle 1|0\rangle+|1\rangle\langle 1|\langle 1|1\rangle}{2} \tag{2.189}$$

$$=\frac{|0\rangle\langle 0|+|1\rangle\langle 1|}{2} \tag{2.190}$$

$$=\frac{I}{2} \tag{2.191}$$

注意这个状态是一个混合态，因为 $\mathrm{tr}((I/2)^2)=1/2<1$. 这是一个非常引人瞩目的结果. 双量子比特联合系统的状态是一个精确已知的纯态，不过，第一量子比特处于混合态，即我们不具备完全知识的一个状态. 这个奇特性质，即系统的联合状态完全已知，而子系统却处于混合态，是量子纠缠现象的另一特点.

练习 2.74　设复合系统 A 和 B 处于 $|a\rangle|b\rangle$ 状态，其中 $|a\rangle$ 是系统 A 的一个纯态，而 $|b\rangle$ 是系统 B 的一个纯态，证明系统 A 的约化密度算子是一个纯态.

练习 2.75　对四个 Bell 态中的每一个，求针对每个量子比特的约化密度算子.

1. 量子隐形传态和约化的密度算子

约化密度算子的一个重要应用是分析量子隐形传态. 回忆 1.3.7 节，量子隐形传态是一个过程，这个过程假设 Alice 和 Bob 共享一个 EPR 对和一条经典信道，

并将量子信息从 Alice 传送到 Bob.

乍看起来隐形传态好像能够超光速通信，但按照相对论，这绝不可能发生. 1.3.7 节猜测是 Alice 需要将她的测量结果发送给 Bob，这阻止了超光速的通信. 约化密度算子将这一点严格化.

请回忆，就在 Alice 进行测量之前，三个量子比特的量子状态是(式(1.32))：

$$|\psi_2\rangle = \frac{1}{2}[|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle+\beta|0\rangle) + |10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(\alpha|1\rangle-\beta|0\rangle)] \quad (2.192)$$

在 Alice 的计算基下进行测量，测后，系统状态分别以概率 1/4 取

$$|00\rangle[\alpha|0\rangle+\beta|1\rangle] \quad (2.193)$$

$$|01\rangle[\alpha|1\rangle+\beta|0\rangle] \quad (2.194)$$

$$|10\rangle[\alpha|0\rangle-\beta|1\rangle] \quad (2.195)$$

$$|11\rangle[\alpha|1\rangle-\beta|0\rangle] \quad (2.196)$$

系统的密度算子为

$$\begin{aligned}\rho = \frac{1}{4}[&|00\rangle\langle 00|(\alpha|0\rangle+\beta|1\rangle)(\alpha^*\langle 0|+\beta^*\langle 1|)\\ &+|01\rangle\langle 01|(\alpha|1\rangle+\beta|0\rangle)(\alpha^*\langle 1|+\beta^*\langle 0|)\\ &+|10\rangle\langle 10|(\alpha|0\rangle-\beta|1\rangle)(\alpha^*\langle 0|-\beta^*\langle 1|)\\ &+|11\rangle\langle 11|(\alpha|1\rangle-\beta|0\rangle)(\alpha^*\langle 1|-\beta^*\langle 0|)]\end{aligned} \quad (2.197)$$

对 Alice 的系统取迹，可得 Bob 系统的约化密度算子为

$$\begin{aligned}\rho^B = \frac{1}{4}[&(\alpha|0\rangle+\beta|1\rangle)(\alpha^*\langle 0|+\beta^*\langle 1|)\\ &+(\alpha|1\rangle+\beta|0\rangle)(\alpha^*\langle 1|+\beta^*\langle 0|)\\ &+(\alpha|0\rangle-\beta|1\rangle)(\alpha^*\langle 0|-\beta^*\langle 1|)\\ &+(\alpha|1\rangle-\beta|0\rangle)(\alpha^*\langle 1|-\beta^*\langle 0|)]\end{aligned} \quad (2.198)$$

$$= \frac{2(|\alpha|^2+|\beta|^2)|0\rangle\langle 0|+2(|\alpha|^2+|\beta|^2)|1\rangle\langle 1|}{4} \quad (2.199)$$

$$= \frac{|0\rangle\langle 0|+|1\rangle\langle 1|}{2} \quad (2.200)$$

$$= \frac{I}{2} \quad (2.201)$$

其中我们在最后一行已经用了完备性. 于是，在 Alice 测量完成后，而 Bob 得到测量结果以前，Bob 系统的状态是 $I/2$. 这个状态不依赖于要隐形传态的状态 $|\psi\rangle$，因此 Bob 进行的任何测量将都不包含关于 $|\psi\rangle$ 的信息，故阻止了 Alice 用隐形传态以超光速向 Bob 传送信息.

2.5 Schmidt 分解和纯化

密度算子和偏迹仅仅是研究复合量子系统的大量有用工具中最初步的内容，这些工具对量子计算与量子信息的研究起关键作用. Schmidt 分解和纯化(purification)是另外两个很有价值的工具，本节就来介绍这两个工具并初步展示它们的作用.

定理 2.7(Schmidt 分解) 设$|\psi\rangle$是复合系统 AB 的一个纯态，则存在系统 A 的标准正交基$|i_A\rangle$和系统 B 的标准正交基$|i_B\rangle$，使得

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle \tag{2.202}$$

其中 λ_i 是满足 $\sum_i \lambda_i^2 = 1$ 的非负实数，称为 Schmidt 系数.

这个结果非常有用. 为了解其用途，考虑下面的结论：令$|\psi\rangle$是复合系统 AB 的一个纯态，则由 Schmidt 分解，得 $\rho^A = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|$ 和 $\rho^B = \sum_i \lambda_i^2 |i_B\rangle\langle i_B|$，于是两个密度算子 ρ^A 和 ρ^B 的特征值相同，即均为 λ_i^2. 量子系统的许多重要性质完全取决于系统约化密度算子的特征值，因此对复合系统的纯态而言，两个系统的这些性质将相同. 例如，考虑双量子比特的状态 $(|00\rangle+|01\rangle+|11\rangle)/\sqrt{3}$，它没有明显的对称性，但如果计算 $\mathrm{tr}((\rho^A)^2)$ 和 $\mathrm{tr}((\rho^B)^2)$，会发现它们的值相等，都是 7/9. 这只是 Schmidt 分解的一个小小的结论.

证明 证明系统 A 和 B 具有相同状态空间维数的情形，一般情况的证明留作练习 2.76. 令$|j\rangle$和$|k\rangle$分别为系统 A 和 B 的固定的标准正交基，则$|\psi\rangle$对某个具有复数元素 a_{jk} 的矩阵 a 可写成

$$|\psi\rangle = \sum_{jk} a_{jk} |j\rangle |k\rangle \tag{2.203}$$

由奇异值分解，$a = udv$，其中 d 是具有非负元素的对角阵，u 和 v 是酉矩阵. 于是

$$|\psi\rangle = \sum_{ijk} u_{ji} d_{ii} v_{ik} |j\rangle |k\rangle \tag{2.204}$$

定义 $|i_A\rangle \equiv \sum_j u_{ji} |j\rangle$，$|i_B\rangle \equiv \sum_k v_{ik} |k\rangle$ 和 $\lambda_i \equiv d_{ii}$，可给出

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle \tag{2.205}$$

从 u 的酉性和$|j\rangle$的标准正交性，容易验证$|i_A\rangle$构成一个标准正交集，同理$|i_B\rangle$也构成一个标准正交集.

练习 2.76 把 Schmidt 分解的证明推广到 A 和 B 具有不同状态空间维数的情况.

练习 2.77 设 ABC 是一个三元量子系统，举例说明存在量子状态$|\psi\rangle$，不能

写成形式

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle |i_C\rangle \tag{2.206}$$

其中 λ_i 是实数，且 $|i_A\rangle$，$|i_B\rangle$，$|i_C\rangle$ 分别是分系统的标准正交基.

基 $|i_A\rangle$ 和 $|i_B\rangle$ 分别称为 A 和 B 的 Schmidt 基，且非零 λ_i 的个数称为状态 $|\psi\rangle$ 的 Schmidt 数. Schmidt 数是复合量子系统的重要属性，在某种意义下是量化系统 A 和 B 之间纠缠的"量". 为了解这个概念，考虑下面明显而重要的性质：Schmidt 数在系统 A 或 B 的单独酉变换下保持不变. 为看清这一点，注意如果 $\sum_i \lambda_i |i_A\rangle |i_B\rangle$ 是对 $|\psi\rangle$ 的 Schmidt 分解，则 $\sum_i \lambda_i (U|i_A\rangle)|i_B\rangle$ 是 $U|\psi\rangle$ 的 Schmidt 分解，其中 U 是只作用在系统 A 上的酉算子. 这种代数不变性使 Schmidt 数成为非常有用的工具.

练习 2.78 证明当且仅当复合系统 AB 的 Schmidt 数是 1，它的状态 $|\psi\rangle$ 是积状态. 证明当且仅当 ρ^A（并且 ρ^B）是纯态，$|\psi\rangle$ 是一个积状态.

与量子计算与量子信息有关的另一技术是纯化(purification). 给定量子系统 A 的状态 ρ^A，我们可以引入另一个系统，记作 R，并为联合系统 AR 定义纯态 $|AR\rangle$，使得 $\rho^A = \mathrm{tr}_R(|AR\rangle\langle AR|)$. 也就是说，当我们只看系统 A 时，纯态 $|AR\rangle$ 退化为 ρ^A. 这是一个纯粹的数学过程，称为纯化，这使我们把纯态和混合态联系起来. 为此我们称 R 为参考系统：它是一个假想的系统，没有直接的物理意义.

为证明纯化可以对任意状态进行，我们来说明如何为 ρ^A 构造系统 R 和纯化 $|AR\rangle$. 设 ρ^A 有标准正交分解 $\rho^A = \sum_i p_i |i^A\rangle\langle i^A|$，我们为对 ρ^A 进行纯化而引入系统 R，它与 A 具有相同的状态空间，有标准正交基 $|i^R\rangle$. 为复合系统定义纯态

$$|AR\rangle \equiv \sum_i \sqrt{p_i} |i^A\rangle |i^R\rangle \tag{2.207}$$

现在计算系统 A 对应子状态 $|AR\rangle$ 的约化密度算子

$$\mathrm{tr}_R(|AR\rangle\langle AR|) = \sum_{ij} \sqrt{p_i p_j} |i^A\rangle\langle j^A| \mathrm{tr}(|i^R\rangle\langle j^R|) \tag{2.208}$$

$$= \sum_{ij} \sqrt{p_i p_j} |i^A\rangle\langle j^A| \delta_{ij} \tag{2.209}$$

$$= \sum_i p_i |i^A\rangle\langle i^A| \tag{2.210}$$

$$= \rho^A \tag{2.211}$$

于是 $|AR\rangle$ 是 ρ^A 的纯化.

注意 Schmidt 分解和纯化有密切的关系：用于纯化一个系统 A 混合态的过程是定义一个纯态. 该纯态相对系统 A 的 Schmidt 基恰好将混合态对角化，并且 Schmidt 系数是被纯化的密度算子的特征值的平方根.

本节介绍了研究复合量子系统的两个工具，Schmidt 分解和纯化. 这些工具是

研究量子计算与量子信息，特别是本书第三部分中量子信息的研究必不可少的.

练习 2.79　考虑由双量子比特组成的复合量子系统，求下面状态的 Schmidt 分解

$$\frac{|00\rangle+|11\rangle}{\sqrt{2}},\quad \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2},\quad \frac{|00\rangle+|01\rangle+|10\rangle}{\sqrt{3}} \tag{2.212}$$

练习 2.80　设$|\psi\rangle$和$|\varphi\rangle$是 A 和 B 组成的复合量子系统的两个纯态，它们具有相同的 Schmidt 数，证明存在系统 A 上的酉变换 U 和系统 B 上的酉变换 V，使得$|\psi\rangle=(U\otimes V)|\varphi\rangle$.

练习 2.81（纯化中的自由度）　令$|AR_1\rangle$和$|AR_2\rangle$是状态 ρ^A到复合系统 AR 的两个纯化，证明存在一个作用在系统 R 上的酉变换 U_R，使得$|AR_1\rangle=(I_A\otimes U_R)\ AR_2\rangle$.

练习 2.82　设$\{p_i,|\psi_i\rangle\}$是为量子系统 A 产生密度矩阵$\rho=\sum_i p_i|\psi_i\rangle\langle\psi_i|$的一个状态系综，引入一个具有标准正交基$|i\rangle$的系统 R，

(1) 证明$\sum_i\sqrt{p_i}\,|\psi_i\rangle|i\rangle$是$\rho$的一个纯化.

(2) 设我们在基$|i\rangle$中测量 R，得到输出 i. 求获得 i 的概率和相应的系统 A 状态.

(3) 令 $AR\rangle$是ρ到系统 AR 的任意一个纯化，证明存在 R 的标准正交基$|i\rangle$，使得测量后，系统 A 的相应测量后状态为$|\psi_i\rangle$，其概率为 p_i.

2.6　EPR 和 Bell 不等式

没有受到量子理论震惊的人还没有理解它.

——*Niels Bohr*

记得一次散步时，Einstein 突然停下来，转过来问我，是否真的相信月亮只在我们看它的时候才是存在的. 接下来的谈话全是关于物理学家对“存在”一词的理解.

——*Abraham Pais*

……量子现象并非出现在 Hilbert 空间里，而是出现在实验室里.

—*Asher Peres*

……不可能性证明所证明的是想象力的不足.

——*John Bell*

盒子 2.7 EPR 实验中的反关联

制备双量子比特状态

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{2.213}$$

由于历史原因，该状态称为自旋单态(spin singlet)，不难看出，这个状态是双量子比特系统的纠缠态. 设我们沿v轴在双量子比特上测量自旋，即在每个量子比特上测量可观测量$v \cdot \sigma$(式(2.116)定义)，对每个量子比特得到$+1$或-1. 实际上，无论如何选择v，两个测量的结果总是相反的. 也就是说，如果第一量子比特的测量结果是$+1$，则第二量子比特上的测量结果就是-1，反之亦然. 无论第一个量子比特是如何被测量的，第二量子比特好像始终知道第一量子比特的测量结果似的. 为证明这个论述，设$|a\rangle$和$|b\rangle$是$v \cdot \sigma$的本征态，则存在复数$\alpha,\beta,\gamma,\delta$，使得

$$|0\rangle = \alpha|a\rangle + \beta|b\rangle \tag{2.214}$$

$$|1\rangle = \gamma|a\rangle + \delta|b\rangle \tag{2.215}$$

代入得到

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = (\alpha\delta - \beta\gamma)\frac{|ab\rangle - |ba\rangle}{\sqrt{2}} \tag{2.216}$$

但$\alpha\delta - \beta\gamma$是酉矩阵$\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}$的行列式，故对某个实数$\theta$，它等于相位因子$e^{i\theta}$. 子是除了一个不可观测的全局相位因子，有

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = \frac{|ab\rangle - |ba\rangle}{\sqrt{2}} \tag{2.217}$$

结果是，若测量$v \cdot \sigma$在两个量子比特上进行，则第一量子比特上得到结果$+1$(-1)，就蕴含着第二量子比特上得到结果-1($+1$).

本章的重点在引人量子力学的工具和数学上，随着这些技术在本书接下来的章节中应用，量子力学非同寻常的非经典性质成为一个反复出现的主题. 但量子力学与经典世界之间的差别到底是在哪里？弄清这个区别，对学习如何进行经典物理学难以或不可能完成的信息处理任务至关重要. 本节以对 Bell 不等式的讨论结束本章，Bell 不等式是反映量子与经典物理学本质差别的一个引人注目的例子.

当我们提到一个对象，如一个人或一本书，我们总假定那个对象的物理性质具有独立于观察的存在性，换句话说，测量只是去揭示这些物理性质. 例如，一个网球的位置是它具有的一个性质，我们常从网球表面散发的光来测量它的位置. 随着量子力学在 20 世纪 20 和 30 年代的发展，出现了一种和经典的观点非常不同的奇怪观点. 如前所述，按照量子力学，未被观察的粒子不具有独立子测量的性质，相反，

物理性质是作为在系统上进行的测量结果出现的. 例如，按照量子力学，一个量子比特不具有“在 z 方向自旋，σ_z”和“在 x 方向自旋，σ_x”这样的确定性质. 这两个性质可以在进行适当测量后得出. 量子力学给出一套规则，给定状态向量，可以确定对可观测量 σ_z 或 σ_x 测量时，可能出现的测量结果的概率.

许多物理学家拒绝接受这种对自然的新观点，最著名的反对者是 Einstein. 在与 Boris Podolsky 和 Nathan Rosen 合著的著名的 EPR 论文中，Einstein 提出一个想象实验，他认为该实验说明量子力学并非关于自然的完整理论.

EPR 的实质论述如下. EPR 主要讨论他们所称的实在的元素（element of reality），他们认为这样的实在元素必须在任何完整的物理学理论中得到表示. 讨论的目的是要通过指出实在的元素没有被包含在量子力学中，来证明量子力学不是完整的物理学理论，方法是引入某个物理性质成为实在的元素的充分条件，即在测量前可以确切地预测该性质的值.

例如考虑分别属于 Alice 和 Bob 的量子比特组成的纠缠对：

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{2.218}$$

假定 Alice 和 Bob 彼此相距很远. Alice 沿 v 轴进行自旋测量，即她进行算子 $v \cdot \sigma$（式(2.116)定义的）的测量. 设 Alice 得到结果 $+1$，盒子 2.7 给出的简单计算显示，她可以确切地预测，如果 Bob 也沿轴 v 测量自旋，他将测得 -1. 类似地，如果 Alice 得到结果 -1，则她可以确切地预测 Bob 将在他的量子比特上测得 $+1$. 因为当 Bob 沿轴 v 测量量子比特时，Alice 总可以预测记录的测量值. 按照 EPR 准则，这个物理属性必对应一个实在的元素，并且应该在任何完整的物理学理论中被表示. 然而，如我们所展示的标准量子力学，仅仅告诉我们如何计算测量 $v \cdot \sigma$ 得到各结果的概率. 标准量子力学肯定不包含任何对所有单位向量 v 表示 $v \cdot \sigma$ 值的基本元素.

EPR 的目的是通过说明量子力学缺乏某些本质的实在元素，用他们的准则来证明量子力学是不完整的. 他们希望强行回到更经典世界，在那里，系统可以独立于系统上进行的测量而存在. 对 EPR 来说不幸的是，大多数物理学家不能接受上述推理的可信性，企图强加给自然她必须服从的法则，似乎是研究自然规律的最荒诞的方式.

事实上，自然最后嘲弄了 EPR. EPR 论文发表近 30 年后，人们提出了一项测试实验，可以用于检查 EPR 希望的强制返回的图像是否有效. 结果是自然通过实验否定这样的观点，而与量子力学相吻合.

称为 Bell 不等式的结果是这项检验性实验的关键. Bell 不等式不是关于量子力学的结果，所以我们要做的第一件事是暂时忘记量子力学的全部知识. 为得到 Bell 不等式，我们将进行一个想象实验，用关于世界运行的直观 ——Einstein 及其

合作者认为自然应该遵守的想法——进行分析. 进行直观分析后，我们再进行量子力学分析，可以证明该分析与直观分析不一致. 于是可以通过实验的方式询问自然，让她在我们对世界如何运行的直观感觉与量子力学之间作出选择.

想象进行如图 2.4 的实验，Charlie 制备两个粒子. 他如何制备粒子并不重要，重要的是他可以重复实验. 他制备好粒子后，发给 Alice 一个粒子，发给 Bob 另一个粒子.

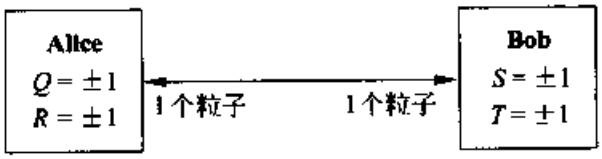


图 2.4 Bell 不等式实验的安排. Alice 可以选择测量 Q 或 R，而 Bob 可以选择测量 S 或 T. 他们同时进行测量. 假定 Alice 和 Bob 相距足够远，他们进行的测量不致相互影响.

Alice 一收到粒子，就对其进行测量. 想象她有两台不同的测量设备，故她可以从两种不同的测量中选择一种，这些测量的物理属性分别标为 P_Q 和 P_R. Alice 事先不知道她要进行哪项测量，相反，她收到粒子后通过随机掷硬币来决定要进行的测量. 为简单起见，假设测量有两个结果，+1 和−1. 设 Alice 的粒子对性质 P_Q 具有值 Q，Q 被假定为 Alice 粒子仅仅通过测量得到的客观性质，就像网球的位置是从它散发出来的光粒子得到那样. 类似地，令 R 记由测量属性 P_R 得到的值.

同样，设 Bob 可以测量两个属性 P_S 和 P_T 之一，分别得到客观存在的 S 和 T 的属性值，取为+1 或−1. Bob 事先也不决定测量哪个性质，直等到收到粒子后，再随机选择. Alice 和 Bob 绝对精确地在同一时间进行测量(或用相对论更精确的语言，是以没有因果联系的方式)，于是，Alice 的测量不可能干扰 Bob 的测量结果(反之亦然)，因为物理性的影响的传播速率不能超过光速.

我们要对 $QS+RS+RT-QT$ 进行简单的代数计算. 注意

$$QS+RS+RT-QT=(Q+R)S+(R-Q)T \tag{2.219}$$

因为 $R,Q=\pm1$，所以或 $(Q+R)S=0$，或 $(R-Q)T=0$. 从式(2.219)容易看出，对每种情况 $QS+RS+RT-QT=\pm2$. 下面设测量前系统处于 $Q=q,R=r,S=s$ 和 $T=t$ 的概率是 $p(q,r,s,t)$，这些概率可能依赖于 Charlie 如何进行制备，以及实验噪声. 令 $E(\cdot)$ 为量的均值，我们有

$$E(QS+RS+RT-QT)=\sum_{qrst}p(q,r,s,t)(qs+rs+rt-qt) \tag{2.220}$$

$$\leqslant\sum_{qrst}p(q,r,t,s)\times2 \tag{2.221}$$

$$=2 \tag{2.222}$$

而且

$$E(QS+RS+RT-QT)=\sum_{qrst}p(q,r,s,t)qs+\sum_{qrst}p(q,r,s,t)rs+\sum_{qrst}p(q,r,s,t)rt-\sum_{qrst}p(q,r,s,t)qt \tag{2.223}$$

$$=E(QS)+E(RS)+E(RT)-E(QT) \tag{2.224}$$

比较式(2.222)和式(2.224)，可得 Bell 不等式，

$$E(QS)+E(RS)+E(RT)-E(QT)\leqslant 2 \tag{2.225}$$

这个不等式又常称为 CHSH 不等式，是四个发现者的字首缩写. 是 Bell 不等式的诸多不等式中的一个，这些不等式中的第一个是 John Bell 发现的.

重复多次实验，Alice 和 Bob 可以确定 Bell 不等式中左边的每一项. 例如，进行一组实验后，Alice 和 Bob 可以在一起分析实验数据，他们分析 Alice 对 P_Q 和 Bob 对 P_S 的所有测量. 通过把实验结果乘起来，可以得到 QS 的一个样本. 对样本取平均，可以估计 $E(QS)$ 仅受实验次数限制的精度. 类似地，可以估计 Bell 不等式左边所有项，并且检验在真实的实验中，该不等式是否成立.

这时候，我们再引入一些量子力学. 想象我们进行如下的量子力学实验，Charlie 制备一个双量子比特的状态

$$|\psi\rangle=\frac{|01\rangle-|10\rangle}{\sqrt{2}} \tag{2.226}$$

他把第一量子比特传给 Alice，第二量子比特传给 Bob. 他们进行如下观测算子的测量

$$Q=Z_1,\quad S=\frac{-Z_2-X_2}{\sqrt{2}} \tag{2.227}$$

$$R=X_1,\quad T=\frac{Z_2-X_2}{\sqrt{2}} \tag{2.228}$$

简单计算可给出这些观测算子的平均值，写成量子力学$\langle\cdot\rangle$形式是

$$\langle QS\rangle=\frac{1}{\sqrt{2}},\quad \langle RS\rangle=\frac{1}{\sqrt{2}},\quad \langle RT\rangle=-\frac{1}{\sqrt{2}},\quad \langle QT\rangle=-\frac{1}{\sqrt{2}} \tag{2.229}$$

于是

$$\langle QS\rangle+\langle RS\rangle+\langle RT\rangle-\langle QT\rangle=2\sqrt{2} \tag{2.230}$$

等一下！返回式(2.225)，我们知道 QS 的平均值加上 RS 平均值加上 RT 平均值减去 QT 平均值永远不超过 2，但这里，量子力学却预言这个平均值的和是 $2\sqrt{2}$！

幸运的是，我们可以询问自然来解决这个佯谬，光子的精巧实验已在式(2.230)这个量子力学的预言与我们直观的推理得到的 Bell 不等式(2.225)之

间作出了判断. 实验的细节超出了本书的范围,但实验的结果是轰动性的,它支持量子力学的预言. 自然不服从 Bell 不等式(2.225).

这意味着什么? 这意味着我们推导 Bell 不等式的假设至少有一个是错的. 有大量工作来分析如何得到这类推理的各种变形,和分析为得到 Bell 不等式需要的不可缺少的区别细微的假定. 这里仅仅总结其要点.

证明式(2.225)的两个假设有问题:

(1) 物理性质 P_Q, P_R, P_W, P_T 具有独立于观测的值 Q, R, S, T 的假设,有时这称为实在性(reality)假定;

(2) Alice 的测量不影响 Bob 测量结果的假设;有时称为这定域性(locality)假定.

这两个假定合称定域实在性假定,当然直观上,它们是有道理的,是关于世界运行的假设,和我们的日常经验相符,但 Bell 不等式表明这两个假设至少有一个是错的.

从 Bell 等式可以学到什么? 对物理学家而言,最重要的教训是,他们深信不疑的关于世界如何运行的直觉是错的,世界不是定域实在的. 大多数物理学家认为从量子力学观点出发,应该放弃的是实在性假定,而另外一些物理学家认为应该放弃的是定域性假定. 不管怎样,Bell 不等式和实质性的实验证据现在指向一个结论,就是为发展对量子力学正确的直观理解,我们必须从观念中把定域性和实在性假定放弃其中一个或者都放弃.

量子计算与量子信息领域可以从 Bell 不等式学到什么? 历史上最有用同时又曾是最模糊的教训是:像 EPR 态那样的纠缠态会让一些深刻的事情发生. 量子计算,特别是量子信息的许多里程碑都来源于一个简单的问题:纠缠现象会给我们带来什么好处? 如我们已经看到的隐形传态和超密编码,以及本书后面会反复看到的,借助引入纠缠现象我们会经历用经典信息观点无法想象的新世界. 概括地讲,Bell 不等式教给我们:纠缠现象是一种新的基本资源,并且从本质上超越经典资源,像铁超越经典的青铜器时代那样. 量子计算与量子信息的一项主要任务就是利用这个新资源,进行用经典资源不可能或难以完成的信息处理任务.

问题 2.1(Pauli 矩阵的函数) 令 $f(\cdot)$ 是从复数到复数的任意函数,令 n 是三维单位向量,θ 是实数. 证明

$$f(\theta \boldsymbol{n} \cdot \boldsymbol{\sigma}) = \frac{f(\theta)+f(\theta)}{2} I + \frac{f(\theta)-f(-\theta)}{2} \boldsymbol{n} \cdot \boldsymbol{\sigma} \tag{2.231}$$

问题 2.2(Schmidt 数的性质) 设 $|\psi\rangle$ 是由 A 和 B 组成的复合系统的一个纯态,

(1) 证明 $|\psi\rangle$ 的 Schmidt 数等于约化密度矩阵 $\rho_A \equiv \mathrm{tr}_B(|\psi\rangle\langle\psi|)$ 的秩(注意 Hermite 算子的秩等于它的支集的维数).

(2) 设 $|\psi\rangle = \sum_j |\alpha_j\rangle |\beta_j\rangle$ 是 $|\psi\rangle$ 的一个表示，其中 $|\alpha_j\rangle$ 和 $|\beta_j\rangle$ 分别是系统 A 和 B 的(未归一化)状态，证明这个分解中的项数大于等于 $|\psi\rangle$ 的 Schmidt 数，$\mathrm{Sch}(\psi)$.

(3) 设 $|\psi\rangle = \alpha|\varphi\rangle + \beta|\gamma\rangle$，证明

$$\mathrm{Sch}(\psi) \geqslant |\mathrm{Sch}(\varphi) - \mathrm{Sch}(\gamma)| \tag{2.232}$$

问题 2.3(Tsirelson 不等式)　设 $Q = \boldsymbol{q}\cdot\boldsymbol{\sigma}$，$R = \boldsymbol{r}\cdot\boldsymbol{\sigma}$，$S = \boldsymbol{s}\cdot\boldsymbol{\sigma}$，$T = \boldsymbol{t}\cdot\boldsymbol{\sigma}$，其中 $\boldsymbol{q}$，$\boldsymbol{r}$，$\boldsymbol{s}$ 和 $\boldsymbol{t}$ 是三维空间中的实单位向量，证明

$$(Q\otimes S + R\otimes S + R\otimes T - Q\otimes T)^2 = 4I + [Q,R]\otimes[S,T] \tag{2.233}$$

利用这个结果证明

$$\langle Q\otimes S\rangle + \langle R\otimes S\rangle + \langle R\otimes T\rangle - \langle Q\otimes T\rangle \leqslant 2\sqrt{2} \tag{2.234}$$

于是式(2.230)给出了在量子力学中违反 Bell 不等式的最大量.

历史和进一步阅读的材料

线性代数的书从高中水平到研究生水平都有，而且很多. 我们乐意采用的也许是 Horn 和 Johnson [HJ85, HJ91] 的两卷本，该书通俗且有极丰富的内容. 其他有用的参考书包括 Marcus 与 Minc 的书[MM92]和 Bhatia 的书[Bha97]. Halmos[Hal58]，Perlis[Per52] 和 Strang[Str76] 是线性代数很好的引论.

有许多关于量子力学的好书，不幸的是，这些书大多数集中在与量子计算与量子线性无关的主题上. 或许最相关的一本书是 Peres 的大作[Per93]，除了对初等量子力学有极清楚的阐述外，Peres 还对 Bell 不等式及相关结果作了广泛讨论. Sakura 的书[Sak95]，Feynman、Leighton 和 Sands 杰出丛书的第三卷[FLS65a]，Cohen-Tannoudji、Diu 和 Laloë 的两卷本[CTD77a, CTD77b] 都是量子力学很好的入门书. 这三个引论性材料尽管大部分的篇幅是与量子计算和量子信息无关的内容，但在一定程度上比其他大多数量子力学课本更接近量子计算与量子信息的思想. 所以，任何想学习量子计算与量子信息的读者都不需要细读这些课本中的任何一本. 不过，特别是读物理学家写的论文的时候，其中任何一本都是方便的参考材料. 量子力学历史参考资料可以在第 1 章末找到.

许多量子力学课本只讲投影测量. 我们相信从测量的一般描述开始，对应用于量子计算与量子信息更为方便，也使初学者感到更容易. 投影测量只是它的一个特例. 当然，我们已经证明最终两种方法是等价的. 我们讲述的一般测量理论是 20 世纪 40 年代到 70 年代间形成的，大部分历史可以从 Kraus 书[Kra83] 中获取. 在 Gardiner 书[Gar91] 的 2.2 节和 Braginsky 与 Khahili 的书中[BK92] 可以找到量子测量

的有趣讨论，2.2.6 节描述的针对不同非正交态的 POVM 测量来自 Peres 书[Per88]，练习 2.64 中的推广出现在 Duan 和 Guo 的文献中[DG98].

超密编码是 Bennett 和 Wiesner[BW92]发明的，使用纠缠光子对进行不同的超密编码的实验实现由 Mattle、weinfurter、Kwiat 和 Zeilinger[MWKZ96]做出.

密度算子的形式体系由 Landau[Lan27]和 von Neumann[von27]独立引入. 密度矩阵的系综的酉自由度的结果，即定理 2.6，是 Schrödinger[Sch36]首先指出的，后来又被 Jaynes[Jay57]和 Hughston、Josa 与 Wootters[HJW93]重新发现并推广. 练习 2.73 的结果来自 Jaynes 的论文，而练习 2.81 和 2.82 的结果来自 Hughston、Josa 与 Wootters 的论文. Uhlmann[Uhl70]和 Nielson[Nie99b]研究了对给定的密度矩阵，密度矩阵分解中可能出现的概率分布的类型. 以 Schmidt 命名的分解出现在[Sch06]. 练习 2.77 的结果是 Peres[Per95]注意到的.

EPR 想象实验来自 Einstein、Podolsky 和 Rosen[EPR35]，实质上由 Bohm[Boh51]描述为我们采用的形式，有时被指为容易让人误解的 EPR“佯谬”. Bell 不等式为纪念首先推导此类不等式的 Bell[Bel64]命名. 我们给出的形式来自 Clauser、Horne、Shimony 和 Holt[CHSH69]，常称为 CHSH 不等式，这个不等式曾由 Bell 独立得到过，但没有发表.

问题 2.2 的第三部分来自 Thapliyal(私人通信)，Tsirelson 不等式来自 Tsirelson[Tsi80].

第 3 章

计算机科学简介

自然科学中，自然已经给了我们一个世界，而我们只是去发现它的规律. 在计算机上，我们可以教给计算机规律来创造一个世界.

——*Alan Kay*

我们的研究领域还处在酝酿阶段. 所幸我们不是在一个已发展了 2000 年的领域. 我们尚处在非常重要的结果不断涌现的阶段.

——*Michael Rabin*，*关于计算机科学*

算法是计算机科学的核心概念，它就像我们小时候学的两个数相加的基本计算方法那样，是完成某些任务的步骤. 本章简介计算机科学中算法的现代理论. 算法的基本模型是 Turing 机，这是一个理想化的计算机. 它很像现代的个人电脑，但基本指令集更简单，具有理想化的无限内存. Turing 机表面上的简单性很容易引起人们的误解，但它实际上是非常强大的计算设备. 我们将看到 Turing 机可以执行任何算法，即使是那些表面上看来在强大得多的计算机上运行的算法.

研究算法所要回答的一个基本问题是：完成计算任务需要什么样的资源？这个问题自然包括两个方面. 第一，我们要弄清什么样的计算任务是可能的，最好给出求解特定问题的具体算法，例如，把一组数按升序快速排列的好算法. 第二，要说明计算任务能够达到的极限，例如，给出把一组数按升序排列的任何算法所要执行操作步数的下界. 最理想的情况应该是两项任务——找到解决计算问题的算法和证明解决计算问题的能力极限——能够完全吻合. 但实际上，在已知求解一个计算问题的最好技术和关于解已知的最细致估计之间，往往存在很大差距. 本章的目的是，综述用于分析计算问题和用于构造和分析解决这些问题的算法工具.

为什么对量子计算与量子信息感兴趣的读者需要花时间了解经典的计算机科学？这有三个很好的理由. 首先，经典计算机科学提供了大量的概念和技术，它们可以非常成功地被用到量子计算与量子信息研究中，量子计算与量子信息的许多

成功来源于计算机科学现有思想和量子力学新思想的结合. 例如,量子计算的一些快速算法基于许多经典算法采用的强大工具——Fourier 变换. 一旦人们认识到量子计算机可以比经典计算机快得多地完成一种 Fourier 变换,许多重要的量子算法就出现了.

其次,计算机科学家已经花了很大力气研究在经典计算机上执行给定计算任务需要什么资源,这些结果可以用作量子计算和量子信息研究的参照. 例如,求一个给定数的素因子的问题已引起很多关注. 人们相信在经典计算机上,这个问题没有有效解(有效的概念在后面还要解释),有趣的是,已经知道这个问题在量子计算机上的有效解法. 我们要了解的是,对这个求素因子的问题,在经典计算机能够做到的和量子计算机能够做到的之间存在什么样的差距. 这个差距本身是有趣的,同时也在更广泛的意义下暗示,这类差距可能存在于一大类计算问题,而非仅仅是找素因子. 通过对这个特殊问题的进一步研究,也许能够找出它在量子计算机上比在经典计算机上更容易求解的特征,并根据这些灵感,继续寻找解决其他问题的有意义的量子算法.

最后,也是最重要的,就是学习以计算机科学家的方式进行思考. 计算机科学家和物理学家或其他自然科学家的思维方式相当不同. 任何希望深入理解量子计算与量子信息的读者一定要学会至少有时像计算机科学家那样思考,他们必须本能地知道什么技术,当然最重要的是,什么问题对计算机科学家来说最有价值.

本章的结构如下. 3.1 节引入两个计算模型: Turing 机模型和线路模型. Turing 机模型将被用作计算的基本模型,不过,在实际中,我们大多数时候采用计算的线路模型,它是量子计算研究中最有用的模型. 有了计算模型,本章其他部分讨论计算的资源要求. 3.2 节从概述我们感兴趣的计算任务开始,同时讨论一些相关的资源问题. 接着概要描述计算复杂性(computational complexity)的关键概念. 计算复杂性是一个研究解决特定计算问题必须要求的时间和空间的领域,它也根据求解的难度对问题进行大致分类. 最后,该节以考虑完成计算需要的能量资源结束. 让人吃惊的是,如果人们可以使计算成为可逆,完成计算所需要的能量可以任意小. 我们要说明如何构造可逆计算机,并指出它们对计算机科学和量子计算与量子信息来说重要的一些原因. 3.3 节以对整个计算机科学的总览结束本章,叙述重点在和量子计算与量子信息有关的问题上.

3.1 计算的模型

……算法是存在于任何编程语言之外的概念.

——*Donald Knuth*

存在一个算法完成某个任务的含义是什么? 我们小时候都学过能把两个不管

多大的数加起来的方法，这是算法的一个例子. 找到算法概念的精确数学描述是本节的目的所在.

历史上，算法的概念可追溯到若干世纪以前. 本科生就学过 Euclid 两千年前求两个正整数最大公因子的古老算法. 不过，现代算法，也就是现代计算理论的基本概念，直到 20 世纪 30 年代才由 Alonzo Church，Alan Turing 和其他计算机时代的先驱引入，这个工作是对伟大的数学家 David Hilbert 在 20 世纪早期提出的深奥问题的回应. Hilbert 问，是否存在某个算法，原则上可以求解所有的数学问题. Hilbert 希望对这个有时称为判定问题(entscheidungsproblem)的回答是肯定的.

令人吃惊的是，Hilbert 问题的回答是否定的：不存在解所有数学问题的算法. 为解决这个深奥问题，Church 和 Turing 必须以数学定义算法的直观概念. 在研究中，他们奠定了现代算法理论，以及后来现代计算机科学理论的基础.

本章采用计算理论中两种表面不同的方法. 第一种方法由 Turing 提出. Turing 为刻画执行计算任务的算法概念，定义了一类现在称为 Turing 机的机器. 在 3.1.1 节，我们先描述 Turing 机，然后讨论 Turing 机模型的一些简化的变形. 第二种方法是通过计算的线路模型，它是对下面量子计算机的研究特别有用的方法. 线路模型在 3.1.2 节描述. 虽然两种方法表面上不同，但实际上是等价的. 读者可能会问，那么为什么要引入不止一种计算模型？这样做的原因是不同的计算模型在处理特定问题时，会提供不同的视角，从两种(或更多)的途径来思考同一概念比只通过一条途径要好.

3.1.1 Turing 机

Turing 机的基本要素如图 3.1 所示. Turing 机包含四个重要元素：①一个很像普通计算机上的程序；②一个有限状态的控制器，其作用像一个裸露的微处理器，协调着机器的其他操作；③作用像计算机内存的一条带子；④一个读写头，指

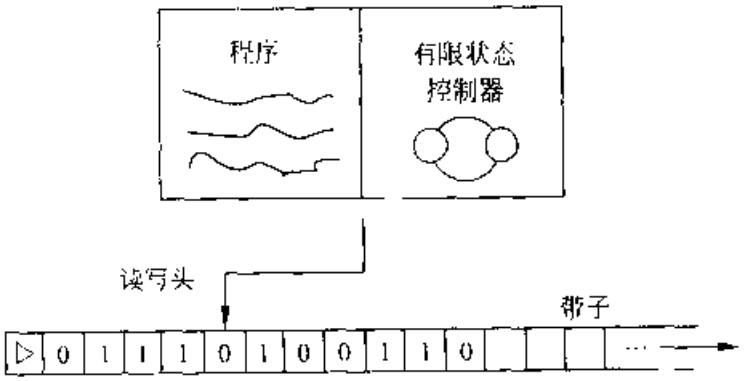


图 3.1 Turing 机的主要要素，在文中，带子上的空白记为 b，▷标志带子的左端.

向带子上当前可以读写的位置. 下面就详细描述每个部分.

Turing 机的有限状态控制器由内部状态的有限集合 $q_1,\cdots,q_m$ 组成,m 可变. 事实上对充分大的 m,这个数目实质上并不影响计算能力,故不失一般性,假设 m 是某个固定的常数. 想象有限状态控制器的最佳方式,是把它看作某种微处理器,负责协调 Turing 机的操作. 它提供离带(off-tape)的暂存,并且是机器完成所有操作的中心. 在状态 $q_1,\cdots,q_m$ 以外,还有两个特殊内部状态,标记为 q_s 和 q_h,它们分别称为开始状态和停机状态(halting state). Turing 机在计算开始的时候进入开始状态 q_s,计算的执行引起 Turing 机内部的状态变化,如果计算最终完成,Turing 机就停留在状态 q_h,以指示机器完成了操作.

Turing 机的带子(tape)是一个一维对象,在一个方向上向无穷延伸. 带子由方格的无穷序列构成. 我们将方格按 0,1,2,…编号. 每个方格包含一个符号,这个符号取自某个包含有限个不同符号的字母表 Γ,暂且假设字母表包含四个记为 0,1,b("空白"符号)和表示带子左端的 $\triangleright$ 符号. 开始,带子的左端包含一个 $\triangleright$,有限个 0 和 1,带子其他格子都是空白. 读写头找出 Turing 机带子上的一个方格作为机器当前访问的格子.

总结起来,机器开始操作时,有限状态控制处于状态 q_s,读写头在带于最左端的格子,即编号为 0 的格子,计算就按下面要定义的程序一步一步进行下去. 若当前状态是 q_h,则计算终止,计算的结果就是带子上的(非空)内容.

Turing 机的程序是具有$\langle q,x,q',x',s\rangle$形式的程序行的一个有限序列,程序行中的第一项 q 是从机器内部状态集中取出的一个状态,第二项 x 是从带子上可能出现的字母表 Γ 中取出的一个符号. 程序工作的原理是在每个机器周期,Turing 机依次查看程序行序列,找出一行$\langle q,x,\cdot,\cdot,\cdot\rangle$使得机器当前内部状态为 q,带子上正在读的符号是 x. 如果没有找到这样的程序行,内部状态变为 q_h,机器停止操作;如果找到这样的行,该行将被执行. 程序行的执行按照下面步骤:机器内部状态变为 q',带子上的符号 x 由符号 x' 覆盖,读写头按照 s 是 -1,$+1$ 或 0,分别向左右移动或不动. 惟一的例外是如果读写头在最左边的格子而 $s=-1$,读写头保持不动.

既然我们已经知道何谓 Turing 机,下面就来看看如何用它计算一个简单函数. 考虑下面 Turing 机的例子. 机器从带子上的一个二进制数 x 开始,数后边跟着空格. 机器有三个内部状态 q_1,q_2 和 q_3,开始状态 q_s 和停机状态 q_h. 机器的程序包含下面的程序行(左边的数字是为下面讨论方便而编的,不是程序的一部分):

1:$\langle q_s,\triangleright,q_1,\triangleright,+1\rangle$

2:$\langle q_1,0,q_1,b,+1\rangle$

3:$\langle q_1,1,q_1,b,+1\rangle$

4：$\langle q_1, b, q_2, b, -1\rangle$

5：$\langle q_2, b, q_2, b, -1\rangle$

6：$\langle q_2, \triangleright, q_3, \triangleright, +1\rangle$

7：$\langle q_3, b, q_h, 1, 0\rangle$

该程序计算什么函数？开始时机器处于状态 q_1，并在带子最左边的格子，于是执行第1行$\langle q_1, \triangleright, q_1, \triangleright, -1\rangle$，使读写头右移，不改变带子内容，但内部状态变为 q_1. 下二行程序保证机器在 q_1 状态，当读到带子上的0(第2行)或1(第3行)时，用空白覆盖格子内容，并使读写头连续右移，直到遇到带子上已经是空白的格子. 这时读写头向左移动一格，内部状态变为 q_2(第4行). 第5行保证读写头当读到空白时，连续向左移动，并保持带子内容不变. 这个过程持续进行直到读写头回到出发点，在那里它读到带子上的一个 $\triangleright$，将内部状态变为 q_3，再向右移动一步(第6行). 第7行完成程序，在带子上写下1，然后停机.

上述分析表明这个程序计算常值函数 $f(x)=1$. 即，不管输入到带子上的数是什么，结果总是1. 更一般地，Turing机可以视为能计算从非负整数到非负整数的函数，带子的初始状态可以用来表示函数的输入，而终了状态用来表示函数的输出.

看来好像用Turing机计算这样一个简单函数我们都要花很大气力，用Turing机能计算更复杂的函数吗？例如，我们可以构造一台机器，使得在带子上输入以一个空白分开的两个数 x 和 y，带子上输出的结果是和 $x+y$ 吗？更一般地，用Turing机可以计算什么类型的函数？

实际上Turing机可以计算无数类型的函数. 例如，它可以用来做所有基本算术操作，用来查找带子上以比特表示的字符串，和许多其他有趣的操作. 令人惊奇的是，Turing机可以模拟一台现代计算机上的所有操作！的确，按照Church和Turing提出的一个论题，计算的Turing机模型完全刻画了计算一个函数所使用的算法概念，这被称为Church-Turing论题(thesis)：Turing机可计算的函数类型恰好对应于我们自然理解的能由算法计算的函数类型.

Church Turing论题断言了严格的数学概念——Turing机可计算函数——和算法可计算的函数的直观概念之间的等价性. 这个论题的重要性在于，它使1936年之前相当模糊的现实世界算法概念的研究有可能成为严格的数学研究. 为明确这一点的重要性，考虑实分析中的连续函数的定义也许有帮助. 19世纪的数学家花了很多时间争论连续性的不同定义，直到连续性的现代定义被接受. 当定义连续性或可计算性这样的基本概念时，选择好的定义能确保人们的直观概念和精确的数学定义密切吻合，这非常重要. 从这个角度看，Church-Turing论题只是断言Turing机模型为计算机科学提供了一个好的基础，用严格的定义刻画了算法的直观含义.

逻辑上讲，直观上用算法可以计算的函数并不显然能用 Turing 机计算，Church、Turing 和许多其他人花了很多时间寻找支持 Church-Turing 论题的证据，并且 60 年来也一直没有找到反面的证据. 不过，将来也许可能发现一个自然的过程来计算 Turing 机无法计算的函数，如果这事真的发生了，那就太好了，因为可以利用那个过程帮助我们完成以前完成不了的新的计算，当然，我们需要修改可计算性的定义，并用它改进计算机科学.

练习 3.1(自然中的不可计算过程) 如何识别一个自然的过程，能够计算一个 Turing 机不可计算的函数?

练习 3.2(Turing 数) 证明每个单带的 Turing 机可以被惟一地分配一个对应的数 1,2,3,…，我们称此数为对应于 Turing 机的 Turing 数(提示：每个正整数有惟一的素因子分解 $p_1^{a_1}P_2^{a_2}\cdots p_k^{a_k}$，其中 p_i 是不同的素数，而 $a_1,\cdots,a_k$ 是非负整数).

后面的章节中，我们将看到量子计算机也服从 Church-Turing 论题，即量子计算机可以计算的函数类与 Turing 机可计算的函数类相同. 量子计算机与 Turing 机的区别在于，执行计算的效率，在量子计算机上存在计算函数能够比经典计算设备，如 Turing 机上人们相信为可能的计算远为有效.

计算的 Turing 机模型可以用来建立计算机程序设计语言中全部常用的概念，这全部细节的说明已超出本书的范围(要获得更多信息请参看本章末“历史和进一步阅读的材料”). 当给定算法时，我们常常不具体给出用来计算算法的 Turing 机，而是用远为高级的伪代码(pseudocode). 我们相信 Church-Turing 论题的正确性，即这些伪代码可以被翻译成计算的 Turing 机模型. 这里不给伪代码任何严格的定义，而是把它看作稍微正规一些的英语，或者，如果读者愿意，可把它看作一种不规范的高级程序设计语言，如 C++ 或 BASIC. 伪代码提供了算法描述的方便途径，使我们不需要涉及 Turing 机要求的极端细节的层次，盒子 3.2 给出了一个使用伪代码的例子. 伪代码在本书中也用于描述量子算法.

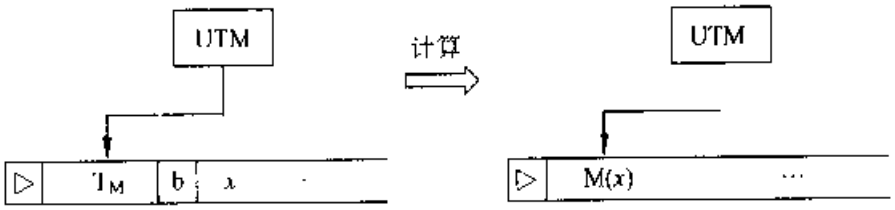
基本的 Turing 机模型有多种变形，包括具有不同带子的 Turing 机. 例如，带子可以是双边无限的，或计算是在多维带子上进行. 就目前所知，还没有一种对 Turing 模型的任何方而进行的物理上合理的改变，来扩大模型可计算的函数类.

作为例子，考虑配备多条带子的 Turing 机，先考虑两条带子的情形，从这个例子可以很容易看出，如何推广到多带的情形. 像基本 Turing 机一样，双带 Turing 机具有有限个内部状态 $q_1,\cdots,q_m$，一个初态 q_s 和一个停机态 q_h，每条带的格子含有来自某个有限字母表 Γ 的符号. 像以前一样，假设字母表仅包含四个符号 0,1,b 和 $\triangleright$，其中 $\triangleright$ 表示每条带子的左端. 机器每条带子有一个读写头. 双带 Turing 机和基本 Turing 机的主要区别在程序上，程序行的形式是 $\langle q,x_1,x_2,q',x_1',x_2',s_1,s_2\rangle$，若机器内部状态是 q，带子 1 当前位置读到 x_1，带子 2 当前位置读到 x_2，则机

盒子 3.1　通用 Turing 机

Turing 机已描述为包含三个基本元素：带子的初始组态、有限状态控制器的内部状态和机器的程序，这些元素可随机器的不同而不同. 通用 Turing 机的聪明想法使我们能够固定程序和有限状态控制器，而只留下带子的初始内容作为惟一可以改变的部分.

通用 Turing 机(如下图)具有如下属性. 令 M 是任一 Turing 机，并且 T_M 是与 M 相关联的 Turing 数，则在 T_M 的二进制表示后面接一个空白符号，再在带子的剩余部分跟上任意符号串 x，通用 Turing 机的输出结果为，机器 M 把 x 作为输入时的任何输出结果. 因此，通用 Turing 机具备模拟任何其他 Turing 机的能力!



通用 Turing 机在思想上类似于现代可编程计算机，其中现代计算机的动作——程序 ——保存在内存中，对应于把比特串 T_M 存在通用 Turing 机的带子开头部分；程序处理的数据存在内存中分开的部分，这对应于通用 Turing 机中 x 的角色；接着固定的硬件用来执行程序，产生输出，这个固定的硬件对应于通用 Turing 机的内部状态和所执行(固定的)程序.

描述构造通用 Turing 机的细节已超出本身的范围(尽管用功的读者可以尝试去构造)，关键在于，通用 Turing 机的存在表明，一台固定的机器可以运行不管什么样的算法. 通用 Turing 机的存在也说明了，Turing 机内部状态数目不太重要的断言，因为只要数目 m 超过通用 Turing 机需要的内部状态数，该机器就可以用来模拟具有任意数目内部状态的 Turing 机.

器的内部状态会变为 q'，x_1 被 x_1' 覆盖，x_2 被 x_2' 覆盖，带子 1 和带子 2 的读写头分别按照 s_1 和 s_2 分别是 $+1$，-1 还是 0 来移动.

基本 Turing 机和双带 Turing 机在什么意义下是等价的计算模型？它们的等价性在于两个计算模型可以彼此模拟(simulate). 设有一个双带 Turing 机，把第一个带子上的比特串 x 作为输入，除去带端标志 ▷，两个带子其他格子均为空白. 该机器计算函数 $f(x)$，其中函数 $f(x)$ 定义为 Turing 机停机后带子 1 上的内容. 值得注意的是，事实上，给定一个计算函数 f 的双带 Turing 机，存在一个等价的单带 Turing 机也能计算 f. 我们不打算进行具体解释，但基本的思想是，单带 Turing

机可以通过用一条带子存储双带 Turing 机两条带子的内容来模拟双带 Turing 机. 为进行这个仿真需要一些附加的计算量,但重要的是原则上仿真总是可以进行的. 实际上,存在一台通用 Turing 机(universal Turing machine)(参见盒子 3.1),能够模拟任何其他 Turing 机.

Turing 机模型的另一个有趣的变形是,在模型中引入随机性. 例如,想象 Turing 机可以执行如下效果的程序:若内部状态是 q,且读写头读到 x,则掷一枚均匀的硬币,如果硬币正面朝上,把内部状态变为 q_{i_H},如果反面朝上,变为 q_{i_T},其中 q_{i_H} 和 q_{i_T} 是 Turing 机的两个内部状态. 该程序行可表为 (q,x,q_{i_H},q_{i_T}). 不过即使是这样,也不能从本质上改变 Turing 机计算模型计算能力,不难看出,可以通过在一台确定性 Turing 机上模拟这算法的效果,即具体找出对应硬币投掷结果不同值的所有可能计算路径. 当然,这个确定性仿真可能远远不如随机模型来得有效,但现在讨论的关键是,可计算的函数类不因模型中引入的随机性而有所变化.

练习 3.3(颠倒比特串的 Turing 机) 给出一个把一个输入的二进制数 x 以比特的逆序输出的 Turing 机(提示:本练习和下面的练习使用多带 Turing 机,并且/或用 $\triangleright$,0,1 和空白以外的符号可能会有帮助).

练习 3.4(模 2 加法的 Turing 机) 给出一个把两个二进制数 x,y 进行模 2 加的 Turing 机,设两个数以二进制形式放在带子上,先是 x,跟一个空白符,再是 y,如果两个数不一样长,可以假设已经在前面添加了 0,以使其长度相等.

现在回到引发计算机科学奠基者们原始灵感的 Hilbert 的判定问题,即存在判定一切数学问题的算法吗? Church 和 Turing 给出的答案是否定的,在盒子 3.2 中,我们将说明 Turing 对这个了不起的事实的证明. 这种不可判定性(undecidability)的现象现在已远远超出了 Church 和 Turing 所构造的例子. 例如,现在知道两个拓扑空间是否拓扑等价(同胚(homeomorphic))的判断问题是不可判定的,在问题 3.4 中将证明,存在不可判定的与动态系统行为有关的简单问题. 这些以及其他例子的参考资料在本章末的"历史和进一步阅读的材料"部分给出.

除了本身的价值以外,不可判定性预示着计算机科学,也是量子计算与量子信息关注的一个重要主题:容易解问题和难解问题之间的区别. 不可判定性提供了难解问题的极端例子——它们如此困难以致不可能求解.

练习 3.5(没有输入的停机问题) 证明给定一个 Turing 机 M,没有算法可以确定当机器输入是空白带子的时候,M 是否停机.

练习 3.6(概率停机问题) 用与练习 3.2 类似的方法,为概率 Turing 机进行编码. 如果机器 x 对输入 x,至少以 1/2 概率停机,将概率停机函数 $h_p(x)$ 定义为 1,如果机器 x 对输入 x,停机的概率小于 1/2,则 $h_p(x)$ 定义为 0. 证明不存在概率 Turing 机,使对所有 x,以严格大于 1/2 的概率正确输出函数 $h_p(x)$.

练习 3.7(停机黑箱(oracle)) 设有一个黑箱(black box)能对非负整数的输

入 x，给出 $h(x)$ 的值，这里 $h(\cdot)$ 是盒子 3.2 定义的停机函数。这类黑箱有时称为停机问题的一个 oracle. 假设有一台扩充了 oracle 能力的标准 Turing 机. 获得它的办法是使用双带 Turing 机，再向 Turing 机增加一条额外的程序指令来调用 oracle，并把 $h(x)$ 的值打印在第二条带子上，而 x 是第二条带子上的当前内容. 显然，这个模型比经典的 Turing 机模型的计算能力更强. 对该模型的停机问题是不可判定的吗？也就是说，有 oracle 帮助的停机问题的 Turing 机，能判断一个运行在 oracle Turing 机上的程序，对特定的输入是否会停机？

盒子 3.2　停 机 问 题

练习 3.2 中已经证明每个 Turing 机可以惟一地和数列 1，2，3，…中的一个数相关联. 为解决 Hilbert 的问题，Turing 用这个数来提出停机问题：具有 Turing 数 x 的机器对输入的数 y 会停机吗？这是一个定义良好的有趣数学问题，这关系到我们的算法是否会终止的问题，但实际上不存在能解这个停机问题的算法. 为明白这一点，Turing 提出是否存在算法解一个更特殊的问题：具有 Turing 数 x 的机器对输入的同一个数 x 是否会停机？Turing 定义了停机函数

$$h(x) \equiv \begin{cases} 0, \text{如果第 } x \text{ 号机器数 } x \text{ 对输入 } x \text{ 不停机} \\ 1, \text{如果第 } x \text{ 号机器数 } x \text{ 对输入 } x \text{ 停机} \end{cases}$$

如果有算法解停机问题，则一定存在一个算法计算 $h(x)$. 我们要导出矛盾. 反设这样的算法是存在的，记作 HALT(x)，考虑计算函数 TURING(x) 的算法，其伪代码如下

```
TURING(x)
y ← HALT(x)
if y=0 then
    停机
else
    永远循环
end if
```

由于 HALT 是一个合法的程序，TURING 必然也是一个合法的程序，其 Turing 数记作 t. 由停机函数的定义，当且仅当 TURING 对输入 t 停机，$h(t)=1$. 但通过检查 TURING 程序，我们可以看到当且仅当 $h(t)=0$，TURING 对输入 t 停机，于是 $h(t)=1$，当且仅当 $h(t)=0$，出现矛盾. 因此，我们当初的存在一个算法来计算 $h(x)$ 的假设是错的，我们可以得出不存在解停机问题的算法的结论.

3.1.2 线路

Turing 机是相当理想化的计算模型，实际的计算机的大小总是有限的，而我们假设的 Turing 机的大小是无界的. 本节研究另一种计算模型，线路模型，这种模型在计算能力上等价于 Turing 机模型，但在许多应用中更方便也更接近实际. 特别地，计算的线路模型是对量子计算机的研究有特殊重要性的预备知识.

一个线路由连线(wire)和门(gate)组成，分别负责信息传递和完成简单的计算任务. 例如，图 3.2 中展示的一个单比特输入为 a 的简单线路，这个比特通过一个非门，非门把该比特进行翻转，把 1 变为 0，把 0 变为 1. 非门前后的连线仅仅是承载比特出入非门，它们可以代表比特在空间的移动，也可以仅仅是经过时间的变化.

更一般地，线路可以包含许多输入输出比特、许多连线和许多逻辑门. 一个逻辑门(logic gate)是一个从某个固定数目 k 输入比特到某个固定数目 l 输出比特的函数 f：$\{0,1\}^k \to \{0,1\}^l$. 例如，非门是单输入比特到单输出比特计算函数 $f(a)=1\oplus a$ 的门，其中 a 是单比特，而$\oplus$是模 2 加法. 通常还约定线路中没有回路，以避免可能的不稳定性，如图 3.3 所示. 我们称这样的线路为无环的，并且将坚持计算的线路模型中的线路都是无环的约定.

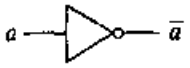


图 3.2 执行单输入比特上单个非门运算的基本线路.

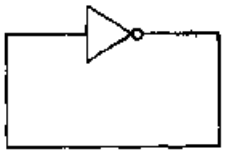


图 3.3 包含回路的线路可以是不稳定的，在计算的线路模型中通常不允许出现回路.

计算中会用到许多其他基本逻辑门，包括与门、或门、异或门、与非门和或非门，这些门都具有双比特输入和单比特输出. 当且仅当它的两个输入都是 1，与门输出 1；当且仅当至少有一个输入是 1，或门输出 1；异或门的输出是输入的模 2 和；与非门和或非门以与和或门的输出作输入，再应用一个非运算到该输出上. 这些门的作用如图 3.4 所示.

图 3.4 中未包含两类重要的门，扇出门（FANOUT）和交叉门(CROSSOVER). 在线路中我们常允许比特“分开”，用一个比特的两个备份来代替这个比特自身，这种运算称为扇出. 我们还用到比特的交叉，即把两个比特的值互换. 图 3.4 中没有包含的第三类运算，实际根本不算真正的门，它只是能制备一个辅助或工作比特，以允许计算过程有额外的工作空间.

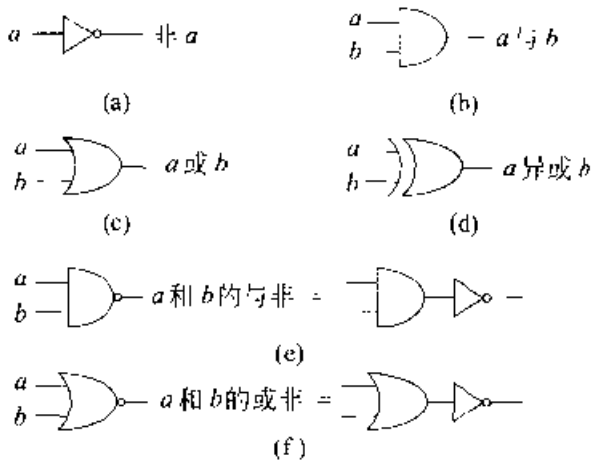


图 3.4　执行与(AND)、或(OR)、异或(XOR)、与非(NAND)和或非(NOR)门运算的基本线路.

这些简单的线路元件可以一起用来完成无数类型的计算，下面我们将证明这些元件可以用于计算任何函数. 同时，来看一下两个 n 比特整数相加的电路的简单例子，实质上用的是全世界孩子在学校里都学到的算法. 该电路的基本元件是小规模的称为半加器(half-adder)的电路，如图 3.5 所示. 半加器有两个输入比特 x 和 y，输出是这两个比特的模 2 和，并当 x 和 y 都是 1 时置进位比特 1，否则为 0.

两个串联的半加器可构造成一个全加器(full-adder)，如图 3.6 所示. 全加器有三个输入比特 x，y 和 c，比特 x 和 y 是被加数，而 c 是从前一步来的进位. 电路有两个输出比特，一个输出比特是三个输入比特的模 2 和 $x\oplus y\oplus c$，第二个输出比特 c'，是进位，当输入的两个以上是 1 是置 1，否则为 0.

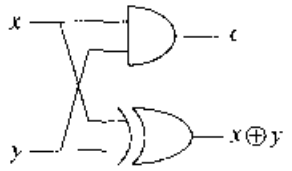


图 3.5　半加器线路. 进位比特 c 当 x 和 y 都是 1 时置 1，否则为 0.

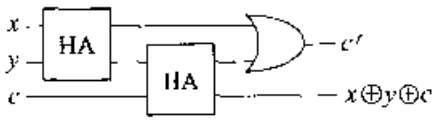


图 3.6　全加器线路.

多个全加器串联可得到把两个 n 比特整数相加的线路，图 3.7 给出了 $n=3$ 的情形.

我们较早曾断言，用固定数目的门就可以计算任意函数 $f:\{0,1\}^n\to\{0,1\}^m$，现在就来证明一个从 n 输入比特到单输出比特的函数 $f:\{0,1\}^n\to\{0,1\}$ 的简化情况，这样的函数称为 Boolean 函数(Boolean function)，相应的线路称为 Boolean 线路(Boolean circuit). 通用的一般证明可以从 Boolean 函数的特殊情况立即得

到，证明基于对 n 的归纳. 对 $n=1$ 的情况，有四个可能的函数：恒等函数，由一条单线组成；比特翻转函数，用一个单非门实现；把输入比特替换为 0 的函数，可由把输入与上初态为 0 的工作比特实现；把输入替换为 1 的函数，可由输入或上初态为 1 的工作比特实现.

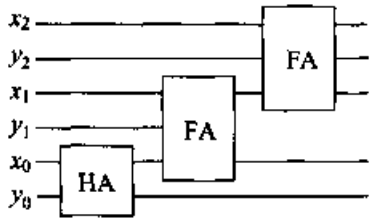


图 3.7 使用初等算法实现两个三比特整数 $x=x_2x_1x_0$ 和 $y=y_2y_1y_0$ 的加法线路.

为完成归纳证明，假设任意 n 比特函数可由一线路计算，另外 f 是一个 $n+1$ 比特函数. 定义 n 比特函数 f_0 和 f_1 分别为 $f_0(x_1,\cdots,x_n)\equiv f(0,x_1,\cdots,x_n)$ 和 $f_1(x_1,\cdots,x_n)\equiv f(1,x_1,\cdots,x_n)$，这是两个 n 比特函数，由归纳假设可以用线路计算.

现在可以设计用来计算 f 的线路了，这个线路根据输入的后 n 个比特计算函数 f_0 和 f_1，然后根据第一位输入是 0 或 1，来输出适当的答案. 图 3.8 给出了一个完成此项任务的线路，归纳完成.

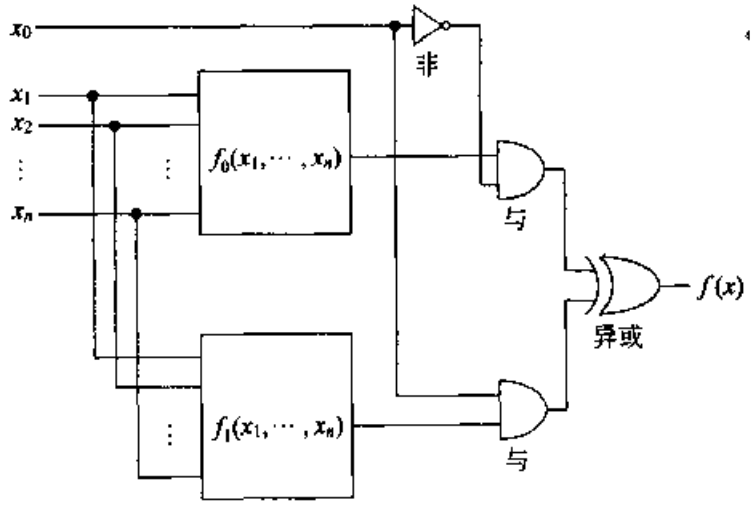


图 3.8 计算任意 $n+1$ 比特函数的线路，由归纳假设存在计算 n 比特函数 f_0 和 f_1 的线路.

通用线路设计中包含五种元素：(1)保存比特的状态的连线；(2)用于 $n=1$ 情况证明的处于标准状态的辅助比特；(3)把输入的单比特输出为其两个拷贝的扇出运算；(4)交换两个比特的值的交叉运算；(5)与、异或和非门. 第 4 章将对照经典线路模型，来定义计算的量子线路模型. 值得注意的是，这五类元素为把线路模型推广到量子情形，提出了一些有趣的挑战性问题：建造、保存量子比特的好的量子连线的方式并非显然，甚至在原理上，由于不可克隆原理(如 1.3.5 节说明

的)，扇出运算在量子力学中不能以直接方式进行，并且与门和异或门都是不可逆的，因此也不能直接以酉量子门的方式实现. 定义量子计算模型的线路肯定要考虑许多问题.

练习 3.8(与非门的通用性)　证明如果可以使用连线、辅助比特和扇出运算，与非门可模拟与门、异或门和非门.

现在从量子的讨论回到经典线路的属性. 较早提到 Turing 机模型和计算的线路模型是等价的，两者在什么意义下是等价的？表面上，两类模型差别很大，Turing 机模型的无界性使它更适合抽象地界定算法的含义，而线路模型则更接近刻画实际的物理计算机可以达到的功能.

两类模型由要引入的一致线路族(uniform circuit family)概念联系起来. 一个线路族由一个指标是正整数 n 的线路集合$\{C_n\}$构成，线路 C_n 具有 n 输入比特，具有任意有限数目的附加工作比特和输出比特，它在至多 n 比特的输入数 x 上的输出比特记作 $C_n(x)$. 要求线路是相容的，即若 $m<n$，且 x 的长度不超过 m，则$C_m(x)=C_n(x)$. 线路族$\{C_n\}$能够计算的函数就是对长度为 n 比特的 x 满足 $C(x)=C_n(x)$的函数 $C(\cdot)$. 例如，考虑一个计算 n 位数平方的线路 C_n，这样就定义了一个计算函数 $C(x)=x^2$ 的线路族$\{C_n\}$，其中 x 是任意正整数.

不过，光考虑无约束的线路族是不够的，实践中，需要有一个算法来构造线路. 事实上，如果在线路族上不作任何限制，可以计算所有类型的函数，包括一个合理的计算模型所不能计算的函数. 例如，令 $h_n(x)$记 x 的值限制在长度为 n 比特的停机函数，h_n 是 n 比特到 1 比特的函数，而已经证明存在线路 C_n 可以计算 $h_n(\cdot)$，因此线路族$\{C_n\}$能够计算停机函数. 不过阻止我们用这个线路族解停机问题的是，没有一个算法来对所有的 n 构造线路 C_n，增加这样一项约束就导致了一致线路族的概念.

如果存在 Turing 机上的某个算法，对给定的 n 产生 C_n 的一个描述，则线路族$\{C_n\}$称为一致线路族，即算法输出一个描述：对线路 C_n 用什么门，如何连接，用怎样的辅助比特，扇出和交叉运算，线路的输出从哪里引出的. 例如，前面描述的平方 n 比特数的线路族肯定是一个一致线路族，因为存在一个算法，对给定的 n，输出一个用以平方 n 比特数的线路描述. 读者可以把这个算法看作工程师能对任意的 n 产生一个线路的描述(进而构造线路)的方法. 与之对照，一个线路族不是一致的，就称为非一致线路族，没有算法可以用来对任意 n 构造某些类型的线路，使我们的工程师无法构造线路来计算像停机函数那样的函数.

直观上，一致线路族是一族可以由合理算法产生的线路，可以证明由一致线路族可计算的函数类恰好是 Turing 机可计算的函数类. 在一致性约束下，Turing 机计算模型中的结果通常可以直接翻译到线路的计算模型，反之亦然. 类似地，后面会关注量子线路计算模型的一致性问题.

3.2 计算问题的分析

计算问题的分析依赖于对三个基本问题的回答：

(1) 什么是计算问题？两个数相乘是一个计算问题，对计算机编程，使它在作诗方面超过人也是.为在分析计算问题的一般理论上取得进展，我们把称为判定问题的一类特殊问题分离出来，并集中注意这类问题.作这种限制可以让理论既优雅又有丰富的结构，最重要的是，它的一套理论原则可以应用到超出判定问题以外的问题.

(2) 怎样设计算法求解给定的计算问题？一旦问题给定，可以用什么算法来解该问题？存在解一大类问题的通用技术吗？怎样保证一个算法像所声称的那样工作.

(3) 解一个给定计算问题的最少资源需要是什么？运行一个算法需要消耗如时间、空间和能量的资源，不同情况下，可能希望最小化一种或多种资源的消耗，可以按照求解需要的资源对问题分类吗？

下面几节考察这 3 个问题，重点是问题 1 和 3.虽然问题 1，什么是计算问题？也许是最基本的问题，但我们要等到 3.2.3 节再回答.这之前先在 3.2.1 节建立一些与资源量化有关的概念，然后在 3.2.2 节概述计算复杂性的关键概念.

问题 2，如何设计好的算法，是许多研究者、无数天才工作的内容.但这方面结果数量如此之多，以致在这个简介中，我们甚至不能描述设计好算法的主要思想，如果读者对这个美妙的主题感兴趣，我们推荐参考本章末的“历史和进一步阅读的材料”部分.我们与这个主题最紧密的直接联系在于本书后一部分讨论量子算法的时候.创造量子算法涉及的技术往往是，现有的经典计算机算法设计的深刻思想和量子力学算法设计中新的专门技术的创造混合，而且因为量子算法设计的精神在多方面类似于经典算法设计，所以我们鼓励读者至少熟悉算法设计的基本思想.

问题 3，解给定计算问题的最少资源需要是什么，是下面几节关注的主要焦点.例如，设有两个数，都是 n 比特长，希望进行相乘，如果乘法是在单带 Turing 机上，Turing 机为完成此任务需要执行多少计算步骤？在执行此项任务时 Turing 机上需要的空间是多少？

这些都是可能提出的资源问题类型的例子.一般而言，计算机用到很多类型的不同资源，但我们大多数注意力集中在时间、空间和能量上.按计算机科学的传统，时间和空间是研究算法关心的两类主要资源，我们在 3.2.2 节到 3.2.4 节研究这些问题.能量以往考虑得较少，不过，对能量需求的研究激发出可逆经典计算的方向，反过来成为量子计算的首要必备基础，因此我们在 3.2.5 节将相当详尽地考察计算的能量要求.

3.2.1　如何量化计算资源

计算的不同模型导致不同的资源需要，即使是从单带 Turing 机到双带 Turing 机这样简单的变化，也可能带来一个给定计算问题的资源变化. 对人们已经彻底了解的像整数相加那样的计算任务，考察计算模型之间的差别也许是有意义的，然而，对初次探讨的问题，我们希望用独立于计算模型的相对细节差别的方式，来量化所需要的资源. 渐近记号是为此形成的可用来概括函数的实质行为的一个工具，它可以用于总结运行一个算法本质上需要多少时间步，而不需要关心精确的时间计量. 本节就来详细描述这个记号，并把它用到一个简单问题，把一组名字按字母顺序排序算法的分析，以说明计算资源的量化过程.

例如，若我们对两个 n 比特数相加需要的门数日感兴趣，门的准确数目会妨碍对总体的把握：也许一个特定算法要用 $24n+2\lceil \log n \rceil +16$ 个门来进行这项任务. 不过，在大规模问题的极端情况惟一重要的是 $21n$ 的项，可以舍弃对算法分析居次要地位的常数因子. 算法的实质行为总起来说就是运算的次数要求的规模大致为 n，其中 n 是被加数长度的比特数. 渐近记号由三个使其精确化的工具组成.

O（大“O”）记号为函数行为设定上界. 设函数 $f(n)$ 和 $g(n)$ 是两个非负整数函数，我们说“$f(n)$ 属于函数类 $O(g(n))$”，或简单地“$f(n)$ 是 $O(g(n))$ 的”，如果存在常数 c 和 n_0，使得对所有大于 n_0 的 n，成立 $f(n) \leqslant cg(n)$，即对于充分大的 n，除去一个不重要的常数因子，函数 $g(n)$ 是 $f(n)$ 一个上界. 大 O 记号在特定算法的最坏情况分析中特别有用，那种情况下我们常满足于得到算法需要的资源的一个上界估计.

当研究一类算法——如两数相乘算法的整个类——的行为时，找出资源需求的下界是有意义的. 对这种情形，使用 Ω 记号. 一个函数 $f(n)$ 称为是 $\Omega(g(n))$ 的，如果存在常数 c 和 n_0，使得对所有大于 n_0 的 n，成立 $cg(n) \leqslant f(n)$. 即对充分大的 n，除去一个不重要的常数因子，$g(n)$ 是 $f(n)$ 的一个下界.

最后，Θ（“大 Θ”）记号用于指示除去不重要的常数因子，$f(n)$ 和 $g(n)$ 的行为渐近相同，即，我们说 $f(n)$ 是 $\Theta(g(n))$ 当且仅当它同时是 $O(g(n))$ 和 $\Omega(g(n))$ 的.

现在考虑渐近记号的一些例子. 因为对所有正数 n 有 $2n \leqslant 2n^2$，故函数 $2n$ 属于类 $O(n^2)$. 函数 2^n 是 $\Omega(n^3)$ 的，因为 $n^3 \leqslant 2^n$ 对充分大的 n 成立. 最后，函数 $7n^2+\sqrt{n}\log(n)$ 是 $\Theta(n^2)$ 的，因为对充分大的 n，$7n^2 \leqslant 7n^2+\sqrt{n}\log(n) \leqslant 8n^2$. 下面的练习中你将发现渐近记号对算法分析有用的初等性质.

练习 3.9　证明 $f(n)$ 是 $O(g(n))$ 的，当且仅当 $g(n)$ 是 $\Omega(f(n))$ 的. 推导 $f(n)$ 是 $\Theta(g(n))$ 的，当且仅当 $g(n)$ 是 $\Theta(f(n))$ 的.

练习 3.10　设 $g(n)$ 是一个 k 阶多项式，证明对所有 $l \geqslant k$，$g(n)$ 是 $O(n^l)$ 的.

练习 3.11 证明对所有 $k>0$，$\log(n)$ 是 $O(n^k)$的.

练习 3.12($n^{\log(n)}$是超多项式的) 证明 n^k 对所有 k 都是$O(n^{\log(n)})$的，但 $n^{\log(n)}$ 永远不是 $O(n^k)$的.

练习 3.13($n^{\log(n)}$是次指数的) 证明对任意 $c>1$，c^n 是$\Omega(n^{\log(n)})$的，但 $n^{\log(n)}$ 永远不是$\Omega(c^n)$的.

练习 3.14 设 $e(n)$是 $O(f(n))$，而 $g(n)$是 $O(h(n))$，证明 $e(n)g(n)$是 $O(f(n)h(n))$的.

下面的 n 元名单排成字母序问题的资源量化是渐近记号一个简单应用的例子. 许多排序算法基于比较和交换操作：n 元名单中的两个元进行比较，如果顺序不对就交换. 如果比较和交换操作是访问名单的惟一途径，那么为对名单正确排序，需要多少次操作?

解这个排序问题的一个简单的比较交换算法如下：(注意 compare-and-swap(j,k)比较名单中第 j 和 k 项，如果顺序不对就交换它们)

```
for j = 1 to n−1
    for k = j+1 to n
      compare-and-swap(j,k)
    end k
end j
```

显然，上述算法能够正确地对 n 个名字的名单进行排序. 注意算法执行比较交换操作的次数是$(n-1)+(n-2)+\cdots+1=n(n-1)/2$，于是算法使用比较交换操作的次数是$\Theta(n^2)$的. 可以做得更好吗? 事实上可以. 已经知道堆排序(heap sort)这样的算法执行 $O(n\log n)$次比较交换，而且，在练习 3.15 中，将通过简单的计数来证明任何基于比较交换操作的算法都需要 $\Omega(n\log n)$次这样的操作，于是，排序问题一般需要$\Theta(n\log n)$次比较交换操作.

练习 3.15(基于比较交换的排序的下界) 设应用一系列比较交换操作，把一个 n 元名单排好序，名单有 $n!$ 种可能的初始顺序. 证明经过 k 次比较交换操作，至多 2^k 个可能的初始顺序完全排好序，则把所有可能初始顺序都排好序需要 $\Omega(n\log n)$次比较交换操作.

3.2.2 计算复杂性

没有算法可以解某个问题的想法——是一个不会改变的基本事实——这个想法令人着迷.

——*Stephen Cook*

有时某些事情是不可能的倒是一件好事. 我为没有人能对我做的许多事情感

到庆幸.

——*Leonid Levin*

选择多项式算法作为非形式化的"实际上能够有效计算"概念的数学描述受到多方批评并不令人惊讶.……最终我们为此提出的辩护必然是：采用多项式最坏情况性能作为有效性结果的准则能导出一套对实际有意义的漂亮而有用的理论，离开这样的简化，则这一切都无法做到.

——*Christos Papadimitrion*

完成一项计算需要什么样的时间空间资源？许多情况下，这是我们对一个计算问题能够提出的最重要的问题.数的加法和乘法这样的问题被视为可以有效解决，因为在消耗很少空间的前提下，有快速算法进行加法和乘法.很多其他问题没有已知的快速算法，并且实际上不可能求解，并非因为不存在算法，而是因为所有已知算法消耗太多时间或空间，以致在实践中毫无用处.

计算复杂性研究解决计算问题需要的时间和空间资源.计算复杂性的任务是证明解决问题最好算法所需要资源的下界估计，即使算法不是具体已知的.本节和下两节将综述计算复杂性，它的主要概念和这个领域中一些重要的结果.注意计算复杂性在某种意义上是对算法设计的补充，在理想情形下，能够设计的最有效的算法与计算复杂性理论证明的下界完全吻合，不幸的是，实际常常不是这样.本书不打算详细考查经典算法的设计.

形式化描述计算复杂性的理论的一个困难在于，解同一个问题的不同计算模型可能需要不同的资源，例如，多带 Turing 机解许多问题比单带 Turing 机快得多.如下粗略的方式用于解决这个困难.设一个问题由输入的 n 比特给定，如我们可能想知道一个特定的 n 比特数是否为素数.各问题间的计算复杂性主要差别是：能以 n 的多项式为界的资源解决，或需比 n 的任意多项式增长更快的资源来解决.后一种情况我们常说资源要求对问题规模是指数性(exponential)的，这是对指数说法的滥用，因为存在如 $n^{\log n}$ 类的函数比任何多项式增长快(因此按这个惯例是指数的)，但比任何真正的指数增长都要慢.如果存在一个算法，用多项式资源来求解一个问题，则该问题将被视为容易、可解(tractable)或可行(feasible)，而如果已知的最好算法需要指数资源，则称为难、不可解(intractable)或不可行(infeasible).

如一个简单例子，假设两个数的二进制展开为 $x_1 \cdots x_{m_1}$ 和 $y_1 \cdots y_{m_2}$，希望求这两个数之和.输入的总长度为 $n \equiv m_1 + m_2$，容易看出两个数可以用次数为 $\Theta(n)$ 的基本操作完成相加，这个算法使用多项式(实际上是线性)数量的操作完成任务.与之对照，人们相信(虽然尚未证明)，把一个整数分解成素因子的问题却是不可解的，即没有 $O(p(n))$ 次操作的算法能把任一 n 比特整数分解因子，其中 p 是 n 的某个固定的多项式函数.后面还会给出许多在这个意义下不可解问题的例子.

多项式与指数的分类相当粗糙. 在实践中,一个用 $2^{n/1000}$ 个操作的求解算法可能比一个运行 n^{1000} 操作的算法更有用. 仅对非常大的输入长度($n \approx 10^8$),这个有效的多项式算法才比非有效的指数算法更可取,对许多情形来说选择这里的非有效指数算法更实际些.

不过,主要基于多项式与指数分类来研究计算复杂性有许多原因. 首先,历史上,多项式算法几乎毫无例外地远远快于指数算法. 我们推测造成这种情况的原因是由于缺乏想象力:想出要求 n, n^2 或其他低阶多项式操作的算法比找到一个 n^{1000} 操作的算法容易得多,尽管后一种情况的例子是存在的. 因此,人类头脑对简单算法的偏好,意味着实际上的多项式算法往往比指数算法要有效得多.

第二个也是更根本的,强调多项式与指数分类的原因来自强 Church-Turing 论题(strong Church-Turing thesis). 如 1.1 节讨论的,20 世纪 60 到 70 年代概率 Turing 机看起来是最强大的合理计算模型. 更准确地说,研究人员一致发现,如果在某个非概率 Turing 机的计算模型上用 k 步基本操作可以计算一个函数,那么总可以在概率 Turing 机上用最多 $p(k)$ 步基本操作计算同一函数,其中 $p(\cdot)$ 是某个多项式函数. 这个命题称为强 Church-Turing 论题:任何计算模型,都可用基本操作次数至多为多项式增长的概率 Turing 机模拟.

强 Church-Turing 论题对计算复杂性理论来说是一个大新闻,因为它意味着只需要把关心的范围限制在概率 Turing 机计算模型上. 毕竟,如果一个问题在概率 Turing 机上没有多项式解法,那么强 Church-Turing 论题认为在任何计算设备上都不会有有效解法. 于是强 Church-Turing 论题蕴含如果把有效性概念和多项式算法等同起来,整个计算复杂性理论将有一个优雅的、与模型无关的形式,并且这个优雅的形式对把"多项式可解"与"有效可解"等同起来的看法形成产生了强烈推动作用. 当然,对量子计算机感兴趣的一个主要原因是,对强 Church-Turing 论题的怀疑,因为被认为在所有经典计算机,包括概率 Turing 机上,不可解的问题可以在量子计算机上有效求解. 不过,了解和掌握强 Church-Turing 论题对寻找与模型无关的计算复杂性理论还是有用的.

最后,我们注意到,在实践中,计算机科学家不只对问题的多项式与指数的分类感兴趣. 因为这只是明白计算问题难度的最初步和最粗略的步骤,当然,这是极重要的区别,它说明了计算机科学资源问题的很多一般的要点. 本书的大部分内容,将主要集中在评价算法的有效性.

考察多项式与指数分类的优点后,我们不得不坦承计算复杂性理论的一个非常出名的失败:证明存在需要指数资源来解的有意义的问题,是非常困难的. 很容易非构造性地证明大多数问题需要指数资源(见练习 3.16),并且进而猜想许多有趣的问题需要指数资源求解,但至少根据现有的知识作出严格证明看来还很难.

这个计算复杂性的失败对量子计算意义深远,因为量子计算机的计算能力可

以和经典计算复杂性理论的一些主要的尚未解决的问题联系起来. 在这些问题解决之前，不能肯定地说量子计算机的计算能力如何，甚至它是否比经典计算机更强大.

练习 3.16(存在难以计算的函数)　证明存在至少需要 $2^n/\log n$ 逻辑门，来计算的 n 输入 Boolean 函数.

3.2.3　判定问题和复杂性 P 类和 NP 类

许多计算问题可以非常清楚地描述为判定问题(decision problem)——答案为是或否的问题. 例如，一个给定的数 m 是否为素数？这是素性(primality)判定问题. 计算复杂性很容易和常常被描述为判定问题形式主要出于两个原因：这种理论的形式最简单也最优雅，同时又可以以自然的方式推广到更复杂的情形；而且历史上计算复杂性理论基本上是从判定问题的研究产生的.

虽然大多数判定问题可以用简单和熟悉的语言来叙述，但是形式语言的术语对判定问题的一般属性的讨论仍然非常有帮助. 在这类术语中，字母表 Σ 上的一个语言 L 是 Σ 上全体(有限)字符串集合 Σ^* 的一个子集. 例如，若 $\Sigma=\{0,1\}$，则偶数二进制表示的集合，$L=\{0,10,100,110,\cdots\}$ 就是 Σ 上的一个语言.

判定问题可以用不同方式编码为关于语言的问题. 比如，素性判定问题可以用二进制字母表 $\Sigma=\{0,1\}$ 编码，Σ^* 中的字符串可以自然地理解为非负整数. 例如，0010 可以解释为数 2，语言 L 定义为由全体素数对应的二进制串组成.

为解决素性判定问题，我们希望一台 Turing 机从给定的数 n 开始，最终输出与当 n 为素数时为“肯定”，当 n 不是素数为“否定”相等价的结果. 为使这个想法精确化，稍微修改一下我们的(第 3.1.1 节的)Turing 机模型，把 q_h 换成分别表示“肯定”和“否定”的答案的两个状态 q_Y 和 q_N，其他方面机器的行为完全不变，并且在进入 q_Y 或 q_N 时停机. 更一般地，一个语言 L 由 Turing 机判定，如果机器可以判断带子上的输入 x 是否为 L 的一个元素，如果 $x\in L$，最终会停在 q_Y 状态，如果 $x\notin L$，最终会停在 q_N 状态. 依出现的两种情况，我们说机器接受或拒绝 x.

我们可以多快地判断一个数是否为素数呢？也就是说，判定表示素性判定问题的语言的最快的 Turing 机是怎样的？我们说一个问题是 TIME($f(n)$)的，如果存在一个 Turing 机，可以在 $O(f(n))$ 时间内判定一个候选的 x，这里 n 是 x 的长度. 如果一个问题对某个 k 是 TIME(n^k)的，则它被称为多项式时间可解的. 对某个 k，为 TIME(n^k)的全部语言的集合记作 P. P 是复杂性类的第一个例子，更一般地，一个复杂性类定义为一个语言的集合. 计算复杂性理论的许多工作是，有关各种复杂性类的定义和了解不同复杂性类之间的关系. 存在不能在多项式时间求解的问题并不奇怪，不幸的是，证明任何一个问题不能在多项式时间求解却都非常困难，虽然人们猜想很多问题都是这样的. 一个被认为不属于 P 的简单例子是有趣

的因子判定问题(factoring decision problem)：给定一个合数 m 和 $l<m$，m 有一个小于 l 的不平凡因子吗？

因子问题的一个有趣性质是如果某人声称答案为"是，m 有一个小于 l 的不平凡因子"，则他可以通过指出一个因子来确立这个事实，其他人可以简单地用长除法来有效地检验，我们称这个因子为 m 有小于 l 因子这个事实的一个证据(witness)．证据容易检验的思想是下面定义复杂性 NP 类的关键思想．我们曾把因子问题形式化为一个判定问题，但读者很容易验证这个判定问题等价于求一个数因子的问题．

练习 3.17 当且仅当因子判定问题属于 P 类，才存在多项式时间的算法，来寻找数 m 的因子．

因子问题是已知的重要而复杂的 NP 类问题的一个例子．NP 类中，问题的特点是，"肯定"实例借助合适的证据能很容易地被验证．更严格地说，语言 L 在 NP 中，如果存在一个 Turing 机 M 具有下述性质：

(1) 若 $x\in L$，则存在一个证据串 w，使得 M 从 x-空白-w 状态开始，在 $|x|$ 的多项式时间后停机于状态 q_Y．

(2) 若 $x\notin L$，则对所有试图成为证据的串 w，机器从 x-空白-w 状态开始，在 $|x|$ 的多项式时间后停机于状态 q_N．

NP 定义中存在一个有趣的不对称性，即尽管必须迅速对 $x\in L$ 判断一个可能的证据是否真的是证据，但是不需要对 $x\notin L$ 找出一个证据．例如，在因子问题中，有简单的办法来验证一个数有小于 m 的因子，但举出一个证据来证明一个数没有小于 m 的因子却是很难办到．这暗示我们定义 coNP，即否定实例具有证据的问题类，显然 coNP 类中的语言恰好是 NP 中语言的补集．

P 和 NP 类是什么关系？显然 P 是 NP 的子集．计算机科学中最著名的未解决问题(open problem)就是是否存在不在 P 中的 NP 问题，常简记为 P≠NP 问题．大多数计算机科学家相信 P≠NP，但几十年过去了，仍没有人能证明它，P=NP 的可能性仍然存在．

练习 3.18 证明若 coNP≠NP，则 P≠NP．

初次了解，很容易认为猜想 P≠NP 应该是容易解决的．看几个在 P 和 NP 中的例子，对弄清为什么它实际上非常微妙是有帮助的．我们从图论中选取例子，图论有多得惊人的判定问题，这些问题有着丰富的应用．一个图由有限顶点集 $\{v_1,\cdots,v_n\}$ 和连接顶点的边组成的，边就是顶点组成的对 $\{v_i,v_j\}$．暂且考虑无向图(undirected graph)，其中顶点的顺

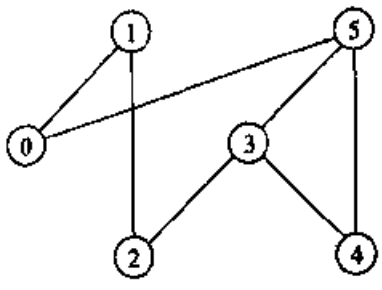


图 3.9 一个图．

序(在每个边的顶点对中)是没有关系的，类似的思想可以在顶点顺序有关系的有向图(directed graph)中探讨. 图 3.9 给出了一个典型的图.

图 3.9 中的一个圈(cycle)是一个顶点序列 $v_1,\cdots,v_m$，这样使每个顶点对(v_j, v_{j-1})是一条边，并且(v_1, v_m)也是一条边. 一个简单圈(simple cycle)是除了第一和最后一个顶点外，其余顶点没有重复，一个 Hamilton 圈是一个经过图的每个顶点的简单圈. 图 3.10 给出包含和不包含 Hamilton 圈的图的例子.

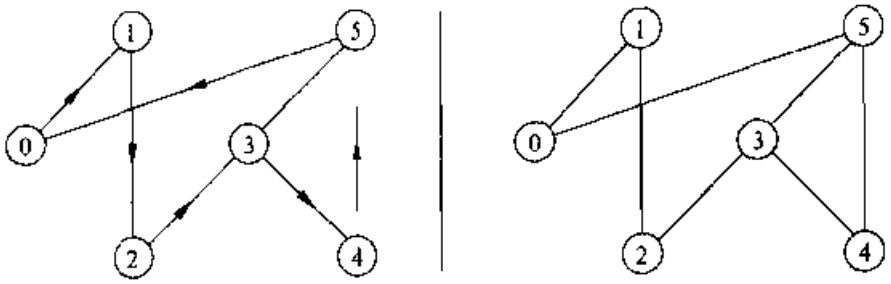


图 3.10　左图包含一个 Hamilton 圈，0，1，2，3，4，5，0. 可以检验右图不含 Hamilton 圈.

Hamilton 圈(HC)问题就是确定一个给定的图是否包含一个 Hamilton 圈. HC 是 NP 中的一个判定问题，因为如果一个给定图有一个 Hamilton 圈，则该圈可被用作一个容易检查的证据；而且，HC 没有已知的多项式时间算法. 事实上，HC 是一个称为 NP 完全问题(NP-complete problem)类中的问题，也被视作 NP 类中最难的问题，因为若 t 时间内可以解 HC，则其他 NP 中的问题可在 $O(\text{poly}(t))$时间内解决，这也意味着如果任何 NP 完全问题有多项式时间解，则可推出P=NP.

有一个 Euler 圈(Euler cycle，EC)判定问题表面上类似于 HC，却有着令人吃惊的不同属性. Euler 圈是图 G 的一个边序列，图的每条边恰好经过一次. Euler 圈判定问题是要确定，一个给定的 n 顶点图 G，是否包含一个 Euler 圈，事实上和 HC 是同样的问题，只不过要求遍历边而不是顶点. 考虑下面的著名定理，证明作为练习 3.20.

定理 3.1(Euler 定理)　当且仅当每个顶点有偶数条边与之相连，一个连通图包含一个 Euler 圈.

Euler 定理给出解 EC 问题的有效方法. 首先，检查图是否连通，这很容易在 $O(n^2)$步操作内完成，如练习 3.19 所示. 如果图不连通，则显然没有 Euler 圈. 如果图是连通的，则对每个顶点检查是否相连边的数目是偶数，如果有一个顶点不是这样，则没有 Euler 圈，否则有. 因为有 n 个顶点，故最多有 $n(n-1)/2$ 条边，所以算法需要 $O(n^3)$个基本操作. 因此 EC 属于 P. 不知什么原因，在遍历边问题中，存在可以用来为 EC 提供有效算法的结构，却没有反映在遍历顶点的问题中. 如果 HC 问题真的缺乏这种结构，那么为什么一种情况出现这样的结构，而另一种情况不出

现的原因就完全不清楚了.

练习 3.19 可达性问题就是确定在图的两个顶点之间是否存在一条路径. 证明若图有 n 个顶点,则可达性分析可以用 $O(n)$步操作完成. 用可达性的解法证明,判定一个图是否连通,可以用 $O(n^2)$步操作完成.

练习 3.20(Euler 定理) 证明 Euler 定理,即,如果每个顶点都有偶数条边相连,给出求一个 Euler 圈的构造性过程.

因子判定问题和求因子问题的等价性是计算机科学中最重要思想之一的归约(reduction)的特殊实例. 直观上,我们知道某些问题可以看作另外一些问题的特例. 归约的一个不平凡的例子是 HC 到旅行商(traveling salesman)判定问题(TSP)的归约. 旅行商判定问题叙述如下:给定 n 个城市 $1,2,\cdots,n$ 和每对城市之间的一个非负整数距离 d_{ij},给定一个距离 d,判断是否存在一个经过所有城市,小子距离 d 的旅行.

HC 到 TSP 的归约是这样的. 设我们有一个包含 n 个顶点的图,把每个顶点视为一个城市,并且如果城市 i 和 j 是相连的,把它们之间的距离 d_{ij} 定义为 1,如果是不相连的则距离定义为 2. 通过这样的手续,我们把这个图变成 TSP 的一个实例. 于是所有城市的一个距离小于 $n+1$ 的旅行的距离必然为 n,并且必然是图的一个 Hamilton 圈. 反过来,如果存在一个 Hamilton 圈,则距离小于 $n+1$ 的城市旅行路线也一定存在. 通过这种方式,给定一个求解 TSP 问题的算法,可以在不花太多代价的情况下,把它转化为求解 HC 问题的算法. 从这里可以得出两点推论. 首先,如果 TSP 可解,那么 HC 也可解;其次,如果 HC 是难的,那么 TSP 也是难的. 这是称为归约(reduction)通用技术的一个例子. 我们把 HC 问题归约为 TSP 问题,这是一项将贯穿全书反复使用的技术.

更一般的归约概念如图 3.11 所示. 语言 B 称为可归约为另一语言 A,如果存在一个 Turing 机在多项式时间内对输入 x 给出结果 $R(x)$,并且当且仅当 $R(x)\in A, x\in B$. 因此,如果有一个算法判定 A,则花费很小的额外代价就可以判定 B,在这个意义下,语言 B 本质上不比语言 A 更难判定.

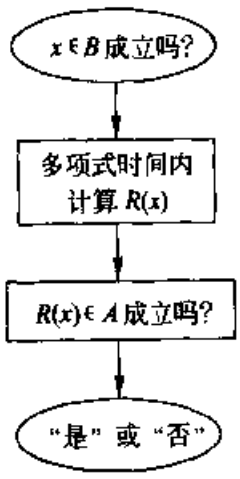


图 3.11 B 到 A 的归约.

练习 3.21(归约的传递性) 证明如果语言 L_1 可归约为语言 L_2,语言 L_2 又可以归约为 L_3,则语言 L_1 可归约为语言 L_3.

一些复杂性类包含针对该类的完全问题,这指的是存在一个属于该类的语言 L,如果这个类中每个其他语言都可以归约为 L,那么在这个意义下 L 是"最难"判定的. 并非所有类都有完全问题,但我

们关心的许多类中的确包含完全问题. P 提供了一个平凡的例子. 令 L 是 P 中的任意一个非空和不等于全体字符串集合的语言，即存在一个字符串 x_1 使得 $x_1 \notin L$，和字符串 x_2 使 $x_2 \in L$. 于是 P 中任意其他语言 L' 可以按如下方式归约为 L：给定一个输入 x，用多项式时间判定过程决定 $x \in L'$ 是否成立. 如果不成立，则置 $R(x) = x_1$，否则置 $R(x) = x_2$.

练习 3.22　设语言 L 对一个复杂性类是完全的，L' 是该类中的另一种使得 L 可以归约到 L' 的语言，证明 L' 对这个复杂类也是完全的.

更不平凡的情况是，NP 类也包含完全问题. 这类问题的一个例子，也是所有其他 NP 完全问题的原型问题是线路可满足性(circuit satisfiability)问题或称 CSAT：给定一个由与或非门组成的 Boolean 线路，线路是否存在一组输入，使得线路的输出为 1，即线路对某个输入情形为可满足. CSAT 的 NP 完全性称为 Cook-Levin 定理. 下面会给出证明的梗概.

定理 3.2(Cook-Levin 定理)　CSAT 是 NP 完全的.

证明　证明分成两部分. 第一部分要证 CSAT 是 NP 的，第二部分证明任何一个 NP 类中的语言可归约到 CSAT. 两个部分都基于仿真(simulation)技术：第一部分实质上是证明 Turing 机可以有效模拟线路，而第二部分实质上是证明线路可以有效模拟 Turing 机. 两部分证明都相当直接，为说明的目的，我们会对第二部分说明更详细些.

证明的第一部分是证明 CSAT 属于 NP 类. 给定一个包含 n 个元件的线路，一个可能的证据 w，显然一台 Turing 机上在多项式时间内可以检查 w 是否满足线路，这就证明 CSAT 属于 NP.

证明的第二部分是证明任意语言 $L \in$ NP 可以归约为 CSAT，即，要证明存在一个多项式时间可计算的归约 R，使得当且仅当 $R(x)$ 满足线路时 $x \in L$. 归约的思想是找出线路来模拟检查语言 L 实例——对 (x,w) 的机器 M 的动作证据. 线路的输入变量代表证据，因为找出一个证据来满足线路应等价于 M 对某个特定的证据 w 接受 (x,w). 不失一般性，我们对 M 作如下假定来简化它的结构：

(1) M 的带子字母表仅包含符号 $\triangleright$，0，1 和空白；

(2) M 的运行最多使用 $t(n)$ 时间和 $s(n)$ 空间，其中 $t(n)$ 和 $s(n)$ 都是 n 的多项式；

(3) 实际上机器 M 可以假定为，所有输入 n 运行时间恰好为 $t(n)$. 这可以通过对每个 $x = \triangleright$，0，1 和空白增加行 $\langle q_Y, x, q_Y, x, 0\rangle$ 和 $\langle q_N, x, q_N, x, 0\rangle$，准确地在 $t(n)$ 步人为停机而做到.

模拟 M 结构的基本思想框架如图 3.12 所示. Turing 机的每个内部状态由线路的一个比特表示，把相应的比特记作 $\tilde{q}_0, \tilde{q}_1, \cdots, \tilde{q}_m, \tilde{q}_Y, \tilde{q}_N$. 开始时，$\tilde{q}_0$ 被置为 1，其他表示内部状态的比特均置为 0. Turing 机带子上的每个方格用三个比特表示：

两个比特表示当前带子上该格子中存储的字母表(▷,0,1 或空白)中的字母,一个标志比特,当读写头指向该方格置时为 1,否则置为 0. 把表示带子内容的比特记作 $(u_1,v_1),\cdots,(u_{s(n)},v_{s(n)})$,把相应的标志位记作 $f_1,\cdots,f_{s(n)}$. 开始时恰当设定 u_j 和 v_j 以表示输入 x 和 w,同时设 $f_1=1$,所有其他 $f_j=0$. 还有一个单独附加的全局标志比特 F,它的作用下面会说明,F 开始时置为 0. 我们把除了表示证据 w 的比特以外的线路所有输入比特视为已经给定,表示证据 w 的比特组则视为线路的变量.

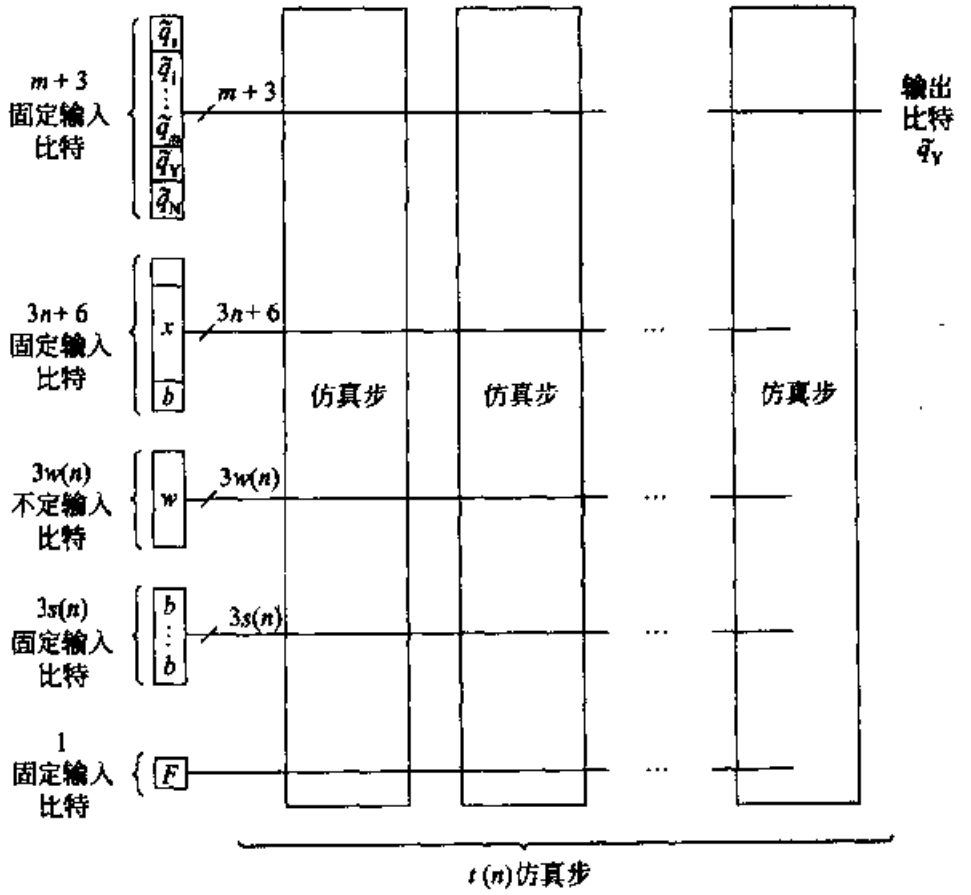


图 3.12 用线路模拟 Turing 机仿真步的草图.

M 的动作可以重复 $t(n)$ 次一个仿真步而得到,仿真都是模拟 Turing 机中单条程序行的执行. 每个仿真步可以分解为对应于个别程序行的一系列步骤,其中最后一步总是把全局标志 F 复位为 0,如图 3.13 所示. 为完成仿真,仅需要模拟形如 $\langle q_i,x,q_j,x',s\rangle$ 的程序行. 为方便起见,设 $q_i\neq q_j$,但 $q_i=q_j$ 时也可以进行类似的构造. 模拟过程如下:

(1) 检查 $\bar{q}_i=1$ 是否成立,这表示当前机器状态是 q_i.

(2) 对带子的每个方格:

① 检查全局标志是否设为 0,表示 Turing 机还没有动作执行.

② 检查标志位置为 1,表示读写头指向该方格.

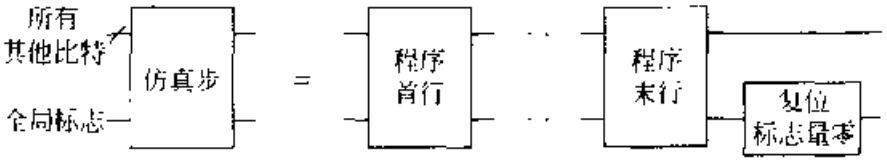


图 3.13　用线路来模拟 Turing 机仿真步的草图.

③ 检查被模拟的当前带子内容是 x.

④ 如果全部条件满足，进行下面步骤：

- 置 $\bar{q}_i=0$ 和 $\tilde{q}_j=1$；
- 把被模拟的带子内容更新为 x'；
- 把标志位按照是否 $s=+1,0,-1$ 和是否我们处于带子的左端更新为适当的邻近格子；
- 把全局标志位置为 1，指示本轮计算已经结束.

这是一个涉及常数比特的固定过程，根据 3.1.2 节的通用性结果可以用包含固定数目门的线路来执行.

容易看出整个线路的门数目是多项式规模 $O(t(n)(s(n)+n))$. 在线路的输出端，显然，当且仅当机器 M 接受 (x,w)，有 $\tilde{q}_Y=1$. 于是，当且仅当存在 w 使得机器 M 接受 (x,w)，线路为可满足，故我们找到了一个从 L 到 CSAT 的期望的归约.

CSAT 为我们较容易地证明许多其他 NP 完全问题提供了一条途径. 我们不直接去证明一个问题是 NP 完全的，而是先证明问题是 NP 的并且 CSAT 可以归约到它，于是根据练习 3.22 可知该问题一定是 NP 完全的. 盒子 3.3 给出了少数几个 NP 完全问题的例子. NP 完全问题的另一个例子是用 Boolean 公式形式给出的可满足性(satisfiability)问题(SAT). 回忆一个 Boolean 公式 φ，它由下列元素组成：一组 Boolean 变量 $x_1,x_2,\cdots$；Boolean 连接词，即有一个或两个输入一个输出的 Boolean 函数，如 $\wedge$(与)、$\vee$(或)和 $\neg$(非)；括号. 对一组给定的 Boolean 变量，Boolean 公式的真假是按照通常的 Boolean 代数确定的. 例如，公式 $\varphi=x_1\vee\neg x_2$ 具有满足性赋值 $x_1=0$ 和 $x_2=0$，而当 $x_1=0$ 和 $x_2=1$ 却不是满足性赋值. 可满足性问题就是确定对一个给定的 Boolean 公式 φ，是否可以由某个可能的赋值满足.

练习 3.23　先证明 SAT 是 NP 的，再证明 CSAT 可归约为 SAT，从而证明 SAT 是 NP 完全的(提示：为构造归约，也许把 CSAT 实例中的每根连线表示成 Boolean 公式中的不同变量会有帮助).

SAT 的一个重要受限情形，3-可满足性问题(3SAT)，也是 NP 完全的. 3SAT 问题考虑的是 3-合取范式(conjunctive normal form)的问题. 一个公式称为合取范式(conjunctive normal form)，如果它是一组子句(clause)的“与”，每个子句是一个

或多个文字(literal)的"或",一个文字是一个 x 或 $\neg x$ 形式的表达式. 例如,公式 $(x_1 \vee \neg x_2) \wedge (x_2 \vee x_3 \vee \neg x_4)$ 就是一个合取范式. 一个公式是 3-合取范式或写作 3-CNF,如果每个子句恰好包含三个文字. 例如公式 $(\neg x_1 \vee x_2 \vee \neg x_2) \wedge (\neg x_1 \vee x_3 \vee \neg x_4) \wedge (x_2 \vee x_3 \vee x_4)$ 就是一个 3-合取范式. 3-可满足性问题就是,确定一个 3-合取范式形式的公式是否可满足.

3SAT 的 NP 完全性证明是直接的,但在这个综述中包含这个证明显得有点冗长. 3SAT 问题在某种意义上甚至超过 CSAT 和 SAT,成为人们最为熟知的 NP 完全问题,并且构成无数其他问题 NP 完全性证明的基础. 我们用 2SAT 问题可以在多项式时间求解的惊人事实来结束关于 NP 完全性的讨论,相应于 3SAT,2SAT 每个子句包含两个文字.

练习 3.24(2SAT 的有效解法) 设 φ 是一个合取范式形式的 Boolean 公式,其中每个子句仅含两个文字.

(1) 构造一个具有有向边的(有向)图 $G(\varphi)$,其定义如下:G 的顶点对应于 φ 中变量 x_i 和它们的非 $\neg x_i$. 当且仅当在 φ 中出现子句 $(\neg \alpha \vee \beta)$ 或于句 $(\beta \vee \neg \alpha)$,图 G 中有一(有向)边 (α, β). 证明当且仅当存在变量 x 使得在 $G(\varphi)$ 中有道路从 x 到 $\neg x$ 和从 $\neg x$ 到 x,φ 不可满足.

(2) 证明对一个给定的有 n 个顶点的有向图 G,可以在多项式时间确定两个顶点 v_1 和 v_2 是否相连.

(3) 找出一个解 2SAT 问题的有效算法.

盒子 3.3 一些 NP 完全问题

NP 类的重要性部分来自无数计算问题已知为 NP 完全的事实. 不可能指望在这里综述这样的题目(参看"历史和进一步阅读的材料"),但通过下面从许多不同数学领域来的例子,可以感觉一下五花八门的 NP 完全问题类.

- 团(图论):一个团是一个无向图 G 的顶点子集,该集每对顶点均有边连接. 团的大小就是它包含顶点的个数. 给定一个整数 m 和一个图 G,G 是否包含一个大小为 m 的团?
- 子集(算术):给定一个正整数的有限集合 S 和一个目标 t,S 是否有子集的和等于 t?
- 0-1 整数规划(线性规划):给定一个整数的 $m \times n$ 矩阵 A 和一个 m 维整数值向量 y,是否存在一个分量在 $\{0,1\}$ 中取值的 n 维向量 x,使得 $Ax \leqslant y$?
- 顶点覆盖(图论):一个无向图 G 的一个顶点覆盖是顶点的一个子集 V',使得图中每条边至少有一个顶点属于 V'. 给定一个整数 m 和一个图 G,图 G 是否有一个顶点覆盖包含 m 个顶点?

设 P≠NP，则可证明存在一个既不是多项式资源可解又不是 NP 完全的非空问题类 NPI(NP 中间问题). 很显然，没有已知的 NPI 问题(否则我们就知道 P≠NP 了)，但有些问题被认为是可能的候选问题. 因子问题和图同构问题是候选问题中最有可能的两个.

图同构：设 G 和 G' 是顶点集合 $V=\{v_1,\cdots,v_n\}$ 上的两个无向图. G 和 G' 同构吗？即是否存在一一映射 $\varphi: V\to V$，使得当且仅当边 $(\varphi(v_i),\varphi(v_j))$ 包含在图 G' 中边 (v_i,v_j) 包含在图 G 中.

量子计算与量子信息研究者对 NPI 类中的问题感兴趣有两个原因. 首先，希望找到用以求解不在 P 类中的问题的快速量子算法；其次，很多人怀疑量子计算机不能有效求解 NP 中的全部问题，从而排除了 NP 完全问题，因此很自然地把注意力集中到 NPI 类上. 实际上已经发现了因子问题的快速的量子算法(第 5 章)，并且这已经激发起对其他可能是 NPI 问题的快速量子算法的寻找.

3.2.4　更多的复杂性类

我们已经考察了某些重要的复杂性类的基本性质. 复杂性类的类型非常丰富，在这些复杂性类之间已知或可能存在许多不平凡的关系. 对学习量子计算与量子信息而言，不需要明白所有这些不同的复杂性类，不过，对重要的复杂性类稍作了解还是有用的，因为许多复杂性类在量子计算与量子信息研究中有自然的对应物，而且，如果要了解量子计算机的能力如何，也应该明白量子计算机所能解的问题类在经典计算机所定义的复杂性类的家族中处于什么位置.

复杂性类的定义中本质上有三种属性可以改变：感兴趣的资源(时间、空间……)，考虑的问题(判定问题、优化问题……)和采用的计算模型(确定性 Turing 机，概率 Turing 机、量子计算机……). 不奇怪，这提供了定义复杂性类的极宽的范围. 本节总结了几个最重要的复杂性类及其某些基本性质. 我们首先考察感兴趣的资源由时间转为空间所定义的一个复杂性类.

最自然的空间受限复杂性类是判定问题的 PSAPCE 类，PSPACE 类是在 Turing 机上用多项式数量的工作比特，在不限制时间情况下可以求解的问题类(参看练习 3.25). 显然，P 包含在 PSAPCE 中，因为在多项式时间内，停机的 Turing 机只能访问多项式数量的方格. 但 NP 也是 PSPACE 的子集. 为明确这一点，设 L 是 NP 类中的任一语言，设规模为 n 的问题的证据至多是 $p(n)$ 规模的，其中 $p(n)$ 是 n 的某个多项式. 为确定该问题是否有解，可以顺序测试全部 $2^{p(n)}$ 个可能证据，每个测试执行时间是多项式的，因而只用到多项式空间. 如果擦除测试当中所有的中间工作单元，那么就可以用多项式空间来测试所有可能.

不幸的是，到目前为止，我们甚至不知道 PSAPCE 类是否包含不在 P 类中的问题. 这是个特别值得注意的问题——使用无限制的时间和多项式空间资源看起

来似乎应该比仅有多项式量的时间的功能更强大，然而，尽管有相当的努力和天才的研究，这件事还是没有被证明. 后面将看到，在量子计算机上可以用多项式时间解的问题类是 PSAPCE 类的一个子集，因此若能证明一个问题在量子计算机上可有效求解，却不能在经典计算机上有效求解，就可推出 P≠PSPACE 的结论，从而解决计算机科学中的一个主要的著名问题. 从积极的观点看，这个结果说明量子计算的思想可能有助于证明 P≠PSPACE；从消极的角度看，也许会得出结论，严格证明量子计算机可以用来有效解决经典计算机上不可解问题还有很长的路要走. 更可悲的是，P=PSPACE 仍是有可能的，果真如此，量子计算机就将不会有任何超越经典计算机的好处. 不过，几乎没有(如果不是绝对没有的话)计算复杂性理论专家相信 P=PSPACE.

练习 3.25(PSPACE⊆EXP) 复杂性类 EXP(表示指数时间) 包含所有由 Turing 机在指数时间，即 $O(2^{n^k})$ 内可以判定的判定问题，这里 k 是任意常数，证明 PSPACE⊆EXP(提示：如果 Turing 机有 l 个内部状态，m 字符的字母表，并使用空间 $p(n)$，论证机器最多可能处在 $lm^{p(n)}$ 个不同状态中的一个状态，并且如果 Turing 机要避免无穷循环，必须在重复访问一个状态之前停机).

练习 3.26(L⊆P) 复杂性类 L(表示对数空间)包含所有由 Turing 机在对数空间，即 $O(\log(n))$，内可以判定的判定问题. 更准确地，类 L 用一个双带 Turing 机定义，第一个带子包含问题的实例，规模为 n，是一条只读的带子，即只允许不改变第一条带子内容的程序行；第二条带子是初始空白的工作带. 对数空间的限制是针对第二条带的. 证明 L⊆P.

使用更多的时间和空间能带来更强大的计算能力吗？这个问题的答案对两种情况都是肯定的. 粗略地说，时间层次定理(time hierarchy theorem)表明 TIME($f(n)$)是 TIME($f(n)\log^2(f(n))$)的严格真子集. 类似地，空间层次定理(space hierarchy theorem)表明 SPACE($f(n)$)是 SPACE($f(n)\log(f(n))$)的严格真子集，其中 SPACE($f(n)$)是由所有能用 $O(f(n))$ 空间资源判定的语言组成的复杂性类. 这两个层次定理对复杂性类的等价关系有有趣的推论. 我们知道

$$\mathrm{L}\subseteq\mathrm{P}\subseteq\mathrm{NP}\subseteq\mathrm{PSPACE}\subseteq\mathrm{EXP} \tag{3.1}$$

不幸的是，虽然每个包含关系都被认为是严格的，但还没有一个已被证明是严格的. 不过时间层次定理蕴含 P 是 EXP 的严格真子集，空间层次定理蕴含 L 是 PSAPCE 的严格真子集，于是可知式(3.1)中至少有一个包含关系是严格的，尽管我们不知道是哪一个.

一旦我们知道一个问题是 NP 完全的，或其他难度准则成立，我们能做些什么？事实表明我们对问题的分析还远没有结束. 一个可能的解决途径是找出问题的可以解决的特殊情况. 例如，在练习 3.24 中，我们看到尽管 SAT 是 NP 完全的，2SAT 问题却有有效解法. 另一个解决办法是改变所考虑问题的类型，这个技巧常

导致新的复杂性类型. 例如，不去找出 NP 完全问题的精确解，而是代之以寻找能找到问题近似解的好算法. 又如，顶点覆盖是一个 NP 完全问题，但在练习 3.27，我们证明有可能找到精确到因子 2 以内的最小顶点覆盖. 另一方面，问题 3.6 中证明除非 P=NP，否则不可能精确到任何因子近似求解 TSP 问题.

练习 3.27(顶点覆盖的近似算法)　令 $G=(V,E)$ 是一个无向图，证明下列算法找到 G 的一个顶点覆盖，这个顶点覆盖一定是因子 2 以内的最小顶点覆盖.

$VC=\varnothing$（空集）
$E'\quad E$
do until $E'=\varnothing$
　　令 (α,β) 是 E' 的任意边
　　$VC=VC\cup\{\alpha,\beta\}$
　　从 E' 中移去与 α 和 β 相连的边
　　返回 VC.

为什么可以近似某个 NP 完全问题，却不能近似另一个 NP 完全问题？难道，一个问题不是可以有效地变换为另一个问题吗？这当然是对的，不过这种变化却不一定保持“好的近似”的概念，结果是，对 NP 类中问题的近似算法的复杂性理论的结构超出了 NP 类的结构. 存在一整套近似算法的计算复杂性理论，可惜超出了本书的范围，不过基本想法是以一种保持好的近似的方式，定义从一个近似问题到另一个问题的有效归约. 用这样的思想，可以把 MAXSNP 这样的对应于 NP 类的复杂性类定义为能够有效验证近似解的问题类. 就像 NP 类，MAXSNP 也有完全问题，并且确定 MAXSNP 类与可以有效近似求解问题类的关系是一个有趣的未解决问题.

最后讨论计算模型的改变导出的一个复杂类. 假设 Turing 机增加了投掷硬币的能力，靠掷硬币的结果决定计算过程中的动作，这样的 Turing 机只能以一定概率接受或拒绝输入. 复杂类 BPP(bounded-error probabilistic time)包含所有具有如下性质的语言 L，即存在一个概率 Turing 机 M 使得：若 $x\in L$，则 M 以至少 3/4 概率接受 x；若 $x\notin L$，则至少以 3/4 概率拒绝 x. 下面的练习表明常数 3/4 的概率本质上具有任意性.

练习 3.28(BPP 类定义中常数的任意性)　设 k 是一个固定常数，$1/2<k\leqslant 1$. 设 L 是一个满足如下性质的语言，即存在一个 Turing 机 M 具有性质：每当 $x\in L$ 时，M 至少以 k 概率接受 x，当 $x\notin L$，M 至少以 k 概率拒绝 x. 证明 $L\in$ BPP.

事实上，盒子 3.4 中讨论的 Chernoff 界，蕴含只要重复一个 BPP 类中语言的判定算法，成功的概率总可以放大到一点，这点在本质上等于 1. 出于这个原因，BPP 类甚至比 P 类更适合作为通常认为在经典计算机上可以有效解决的判定问题类. BPP 类的量子对应物称为 BQP 类，正是我们在研究量子算法中最感兴趣

的类.

盒子 3.4 BPP 和 Chernoff 界

设我们有一个算法对一个判定问题以 $1/2+\varepsilon$ 概率给出准确答案，出错的概率是 $1/2-\varepsilon$. 如果运行算法 n 次，猜正确答案是最频繁出现的结果似乎很合理. 这个过程可靠到什么程度？Chernoff 界是回答这个问题的一个初等概率的简单答案.

定理 3.3(Chernoff 界) 设 $X_1,\cdots,X_n$ 是独立同分布随机变量，每个随机变量取 1 的概率为 $1/2+\varepsilon$，取 0 的概率为 $1/2-\varepsilon$，则

$$p\left(\sum_{i=1}^{n} X_i \leqslant \frac{n}{2}\right) \leqslant \mathrm{e}^{-2\varepsilon^2 n} \tag{3.2}$$

证明 考虑任意包含至多 $n/2$ 个 1 的序列 $(x_1,\cdots,x_n)$，当含有 $\lfloor n/2 \rfloor$ 个 1 时，这种序列出现的概率达到最大，因此

$$p(X_1 = x_1,\cdots,X_n = x_n) \leqslant \left(\frac{1}{2}-\varepsilon\right)^{\frac{n}{2}}\left(\frac{1}{2}+\varepsilon\right)^{\frac{n}{2}} \tag{3.3}$$

$$= \frac{(1-4\varepsilon^2)^{\frac{n}{2}}}{2^n} \tag{3.4}$$

总共至多有 2^n 个这样的序列，于是

$$p\left(\sum_i X_i \leqslant \frac{n}{2}\right) \leqslant 2^n \times \frac{(1-4\varepsilon^2)^{\frac{n}{2}}}{2^n} = (1-4\varepsilon^2)^{\frac{n}{2}} \tag{3.5}$$

最后，通过计算，$1-x \leqslant \exp(-x)$，故

$$p\left(\sum_i X_i \leqslant \frac{n}{2}\right) \leqslant \mathrm{e}^{-4\varepsilon^2 n/2} = \mathrm{e}^{-2\varepsilon^2 n} \tag{3.6}$$

这表明对固定的 ε，随着算法重复次数增加，出错的概率将按指数速率减小. 对 BPP 的情况，我们有 $\varepsilon = 1/4$，于是算法重复几百次，出错概率就降低到 10^{-30} 以下，这时计算机元件出错的可能性就大大高于算法概率性质引起错误的可能性了.

3.2.5 能量与计算

计算复杂性研究了求解一个计算问题所需要时间和空间量. 另一类重要的计算资源是能量，本节研究计算的能量需求. 让人吃惊的是，包括经典和量子计算在内的计算原则上都可以不消耗任何能量！计算中的能量消耗实际上与计算的可逆性有深刻的联系. 考虑一个门，如与非门，它有两个比特输入和一个比特输出. 这类门本身是不可逆的，因为，给定该门的输出，无法惟一地确定输入. 例如，如果与非

门的输出是 1，则输入可以是 00，01，或 10 中的任何一个. 另一方面，非门是可逆逻辑门的一个例子，因为给定非门的输出，可以推断出输入必须是什么.

认识不可逆性的另外一条途径是把它看作信息的擦除. 如果一个逻辑门是不可逆的，则输入到门的部分信息在门运算的时候将不可恢复地丢失，即某些信息被门擦除了. 反过来，在可逆计算中，没有信息被擦除，因为输入总可以从输出得到恢复. 因此，说计算是可逆的等价于说计算过程中没有信息被擦除.

计算中的能量消耗与可逆性有什么联系呢？Landauer 原理提供了答案：要擦除信息就必须消耗能量. 更确切地，Landauer 原理可以叙述如下.

Landauer 原理（第一形式）　假设计算机擦除一比特的信息，散发到环境中的能量的总量至少是 $k_B T \ln 2$，其中 k_B 称为 Boltzmann 常数，T 是计算机所在的环境温度.

按照热力学定律，Landauer 原理可以不以能量消耗形式而是以熵形式给出.

Landauer 原理（第二形式）　假设计算机擦除一比特的信息，环境的熵增量至少是 $k_B \ln 2$，其中 k_B 是 Boltzmann 常数.

证实 Landauer 原理是个物理学问题，已超出了本书的范围，如果读者希望了解为什么 Landauer 原理成立，请参看本章末的“历史和进一步阅读的材料”. 如果我们接受所给的 Landauer 原理，那么就引出许多有趣的问题. 首先，Landauer 原理只提供了为擦除信息要消耗能量的下限，现有的计算机跟这个下界接近到什么程度？答案是不很接近. 实际上 2000 年左右的计算机的每个逻辑运算大概消耗 $500 k_B T \ln 2$ 的能量.

尽管现有计算机远没有达到 Landauer 原理给出的下限，弄清可以减少多少能量消耗仍然是有意义的重要问题. 除了问题本身的意义，关心这个问题的一个现实原因源于 Moore 定律：如果计算机的能力不断增强，除非每个操作的能量消耗至少像计算能力提高一样迅速降低，否则消耗的总能量必然增加.

如果所有计算都是可逆的，那么 Landauer 原理将蕴含计算机消耗能量没有下限，因为根本没有任何比特在可逆计算中被擦除. 当然，也许其他物理原理会要求能量的消耗，幸运的是，实际并非如此. 但在不擦除信息条件下，可能进行通用计算吗？物理学家可能曲解这个问题，他们可能会说这个问题的答案一定是肯定的. 因为根据我们现在对物理学规律的了解，它们从根本上说是可逆的，即如果知道封闭物理系统的终了状态，则物理学定律允许我们求出系统的初始状态. 如果我们相信那些定律是正确的，那么必然得出结论说在与和或等不可逆逻辑门中一定隐藏着一些可逆计算. 但隐含的可逆性在哪里，能够用它来构造显式的可逆计算机吗？

我们将用两种不同的技术给出，能够进行通用计算的、可逆的、基于线路的模型. 第一个模型，完全由撞球和镜子构成，它给出可逆计算的一个漂亮的、具体实现

的原理. 第二个模型,基于称为 Toffoli 门的逻辑门(见 1.4.1 节),从更抽象观点处理可逆计算,它在后面的量子计算与量子信息中将大有用处. 为通用计算建立可逆 Turing 机也是可能的,但我们不在这里研究它们,因为对量子计算而言,事实上可逆线路模型要有用得多.

撞球计算机(billiard ball computer)的基本思想如图 3.14 所示. 撞球的"输入"从左边进入计算机,在从右边的出口离开之前,与镜子以及其他球发生碰撞,在输入点上出现或不出现撞球,分别用来指示逻辑上的 1 或 0. 这个模型的有趣之处在于,它显然是可逆的,在它的操作范围内完全服从经典力学的定律. 而且,这样的计算模型在下述意义下是通用的,即它可被用于模拟任何在计算的标准线路模型上的计算.

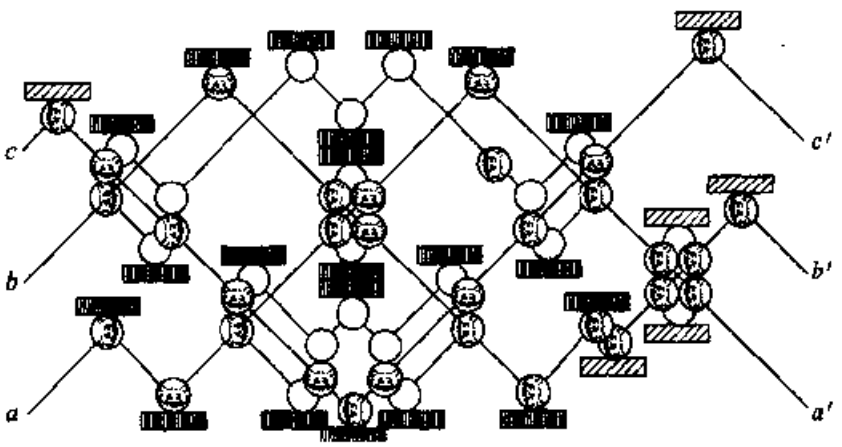


图 3.14 一个简单的撞球计算机,有三个输入比特和三个输出比特,分别从左边输入从右边输出. 球的出现与否分别指示一个 1 或 0. 空的圆圈表示碰撞作用下可能的路径. 这个特别的计算机可以实现书中讨论的 Fredkin 经典可逆逻辑门.

当然,即使能造出撞球计算机,也将是非常不稳定的,就像任何撞球手可以证明的,滚过无摩擦光滑表面的球很容易在小的扰动下偏离原来的路线. 计算的撞球模型依赖完美的操作条件,不允许有类似热噪声引起的外界干扰. 虽然可以进行周期性的修正,但这样获得的信息将不得不被擦除,这就需要做功,于是消耗能量来减少对噪声的敏感性,这对实际的现实世界的计算机是必需的. 在我们这个引论中,将忽略撞球计算机中的噪声影响,集中注意力在理解可逆计算的本质要素上.

撞球计算机提供了实现称为 Fredkin 门的通用逻辑门的一种优雅方法,实际上,Fredkin 门的性质为可逆逻辑门和线路提供了一个通用原则的概要. Fredkin 门有三个输入比特和三个输出比特,分别记作 a,b,c 和 a',b',c'. 比特 c 是控制比特,其值不能被 Fredkin 门的动作改变,即 $c'=c$. c 被称为控制比特的原因是,它

控制着另外两比特 a 和 b 的变化. 如果 c 被置为 0 则 a 和 b 就保持不变,即 $a'=a$, $b'=b$. 如果 c 被置为 1,则 a 和 b 将交换,即 $a'=b, b'=a$. Fredkin 门的完整真值表列在图 3.15 中. 容易看出 Fredkin 门是可逆的,因为根据输出 a', b', c',可以确定输入 a, b, c. 实际上,为恢复输入 a, b 和 c,仅需要把另一个 Fredkin 门应用到 $a' b', c'$ 上.

输入			输出		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	0	1
1	0	0	1	0	0
1	0	1	0	1	1
1	1	0	1	1	0
1	1	1	1	1	1

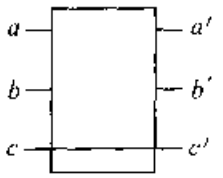


图 3.15 Fredkin 门的真值表和线路表示. 比特 a 和 b 在比特 c 置位时交换,否则保持不变.

练习 3.29(Fredkin 门是自逆(self-inverse)的) 证明连续应用两个 Fredkin 门,输出与输入相同.

检查图 3.14 中的撞球的路径,不难验证这个撞球计算机实现了 Fredkin 门.

练习 3.30 验证图 3.14 中的撞球计算机实现了 Fredkin 门.

除了可逆性,Fredkin 门还有一个有趣的性质,就是在输入输出之间保持 1 的个数. 从撞球计算机角度看,这对应于进入 Fredkin 门的撞球的数目等于出来的球数,于是,它有时又称为一个保守(concervative)可逆路径门. 这样的可逆性和保守性对一个物理学家来说是非常有意义的,因为它们可能是基于基本物理原理提出来的. 自然界的定律是可逆的,可能的例外是 2.2.3 节讨论过的量子力学的测量假设. 保守性可以看作是与质量守恒性质或能量守恒性质对应,事实上,在计算的撞球模型中保守性恰好对应质量守恒.

Fredkin 门不仅是可逆的和保守的,它还是一个通用逻辑门. 如图 3.16 所示, Fredkin 门可以设成模拟与、非、交叉与扇出函数,因此可以模拟任意经典线路.

Fredkin 门模拟不可逆门如与门,利用了两方面的思想. 首先,允许特殊状态 0 或 1 的辅助比特输入到 Fredkin 门. 其次,Fredkin 门的输出包含后续计算不用的额外"垃圾". 这些辅助和垃圾比特对计算没有直接的作用,它们的重要性在于使计算成为可逆. 事实上像与和或这样的不可逆门可以视为辅助和垃圾比特被隐藏的结果. 总结起来,给定经典线路计算的函数 $f(x)$,我们能够建立一个完全由 Fredkin 门构成的可逆线路,其中输入是 x,再加上一些处于标准状态的辅助比特,来计算 $f(x)$和一些额外的"垃圾"输出 $g(x)$. 因此,可以把计算表示为 $(x, a) \to (f(x), g(x))$.

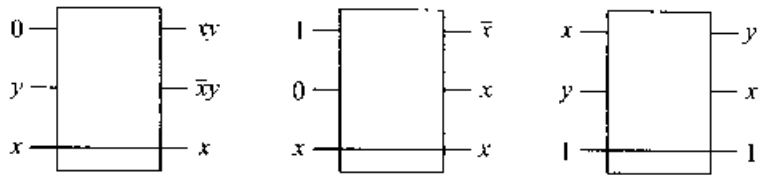


图 3.16 被配置用来执行基本门与(左)、非(中)和基本路由函数、交叉(右)运算的 Fredkin 门. 中间的门也用作执行扇出运算,因为它在输出产生 x 的两个拷贝. 注意这些配置的每一个都要求使用制备成标准状态的额外辅助比特,例如,与门的第一条线上的 0 输入,一般地输出会包含后边计算不用的"垃圾".

现在已经知道如何以可逆方式计算函数,不幸的是,这种计算会产生不希望的垃圾比特. 通过一些修改,实际上可以执行垃圾比特均为标准状态的计算. 这种结构对量子计算非常重要,因为依赖于 x 值的垃圾比特的存在一般会毁掉量子计算中关键的干涉(interference)性质. 为明白这是怎样做到的,假定可逆门库中有非门,这样总可以假定辅助比特 a 是从 0 开始,在需要 1 的时候可以通过加非门由 0 得到. 为方便起见,假定经典的受控非门也是可用的. 经典受控非门可以类似 1.3.2 节量子受控非门方式定义,即把输入 (c,t) 变为 $(c,t\oplus c)$,其中 $\oplus$ 表示模 2 加法. 注意 $t=0$ 给出 $(c,0)\rightarrow(c,c)$,于是受控非门可以看作一个输出没有"垃圾"比特的可逆的复制门或扇出门.

通过在线路开始处附加非门,计算的动作可以写作 $(x,0)\rightarrow(f(x),g(x))$,还可以把受控非门加到线路开头,以产生一个在后续计算中不变的 x 的备份. 经过这个修改,线路的动作可写作

$$(x,0,0)\rightarrow(x,f(x),g(x)) \tag{3.7}$$

式(3.7)是表述可逆电路动作的很有用的方式,因为它使我们能用称为退计算(uncomputation)的思想,以很小的计算代价去掉"垃圾"比特. 其思想叙述如下. 设从一个状态为 $(x,0,0,y)$ 的四寄存器计算机开始,第二个寄存器用来存计算结果,第三个寄存器用来为计算提供工作空间,即存储"垃圾"比特 $g(x)$. 第四个寄存器的作用很快会描述,假设它开始处于任意状态 y.

如以前一样,先应用一个可逆线路计算 f,导致状态 $(x,f(x),g(x),y)$. 下面,我们用受控非门把结果 $f(x)$ 按比特加到第四寄存器上,使机器进入状态 $(x,f(x),g(x),y\oplus f(x))$. 然而,计算 $f(x)$ 的所有步骤都是可逆的,并且不影响第四寄存器,故应用计算 f 的逆线路将得到状态 $(x,0,0,y\oplus f(x))$. 通常在描述函数的计算时将辅助的 0 略去,只把线路的动作写成

$$(x,y)\rightarrow(x,y\oplus f(x)) \tag{3.8}$$

一般地,这个修改后的计算 f 的电路就称为计算 f 的可逆电路,尽管原则上说可

能有许多其他可逆电路可以用来计算 f. 对具有多比特输出的函数，我们有如下引理.

引理　若 $f(x)$ 和 $f^{\perp}(x)$ 是具有多项式尺寸经典线路的置换(未必可逆线路)，则必存在不需辅助比特的多项式尺寸可逆线路计算 $x \to f(x)$.

证明是利用已介绍的可逆计算技术计算 $(x,0) \to (x,f(x)) \to (x \oplus f^{\perp}(f(x)),f(x)) = (0,f(x))$. 这个结果被第 5 章隐含地使用了.

进行可逆计算涉及多少额外资源？为分析这个问题，需要计算可逆电路中额外辅助比特的数目，并与经典模型中的门的数量进行比较. 应该明确，除了一个常数因子可逆电路的门的数量与一个不可逆电路相当. 这个因子代表模拟一个不可逆电路元件需要的 Fredkin 门的数量，加上退计算的因子 2，以及用于可逆计算的额外的与电路中比特数呈线性关系的受控非运算的开销. 类似地，要求的辅助比特的规模最多与不可逆电路中门的数量呈线性关系，因为每个不可逆电路的元件可以用固定数目的辅助比特来模拟. 作为结论，自然的复杂性类如 P 类和 NP 类不管是对可逆或不可逆的计算模型都是相同的. 对更细致的复杂性类如 PSPACE 类，情况并非如此简单，参看问题 3.9 和"历史和进一步阅读的材料"的更细致讨论.

练习 3.31(可逆半加器)　构造一个可逆电路，使得输入为两个比特 x 和 y，输出是 $(x,y,c,x \oplus y)$，其中 c 是 x 和 y 相加的进位.

Fredkin 门及其撞球计算机实现为可逆计算提供了一个漂亮的方案. 还有一类可逆逻辑门，Toffoli 门，对经典计算也是通用的. 虽然 Toffoli 门不像 Fredkin 撞球实现那样具有优雅的物理简单性，但是它对量子计算的研究更为重要. 1.4.1 节已经介绍了 Toffoli 门，但为方便起见，在这里复习一下它的性质.

Toffoli 门有三个输入比特，a，b 和 c. a 和 b 称为第一和第二控制比特，c 称为目标比特. 该门不改变两个控制比特，在两个控制比特都置位时，翻转目标比特，否则目标比特不变. Toffoli 门的真值表和电路表示如图 3.17 所示.

输入			输出		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

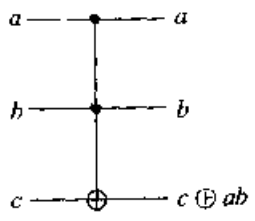


图 3.17　Toffoli 门的真值表和电路表示.

Toffoli 门怎样用于通用计算？设我们希望作 a 和 b 的与非运算，使用 Toffoli

门，则我们把 a 和 b 用作控制比特，把一个置为 1 的辅助比特送到目标比特，如图 3.18 所示，在目标比特将得到 a 和 b 的与非结果. 像 Fredkin 门的研究中一样，可以预期，用 Toffoli 门模拟与非门需要用到特殊的辅助输入，输出的一部分是垃圾比特.

可以用 Toffoli 门来实现扇出运算. 把一个辅助比特 1 输入到第一控制比特，把 a 输入到第二控制比特，就输出 $1, a, a$，如图 3.19 所示. 与非和扇出运算合起来具有计算通用性，这样就看出任意电路可以用一个由 Toffoli 门和辅助比特组成的可逆电路有效模拟，并且通过像对 Fredkin 门同样的方法，可以获得像退计算那样的其他技术.

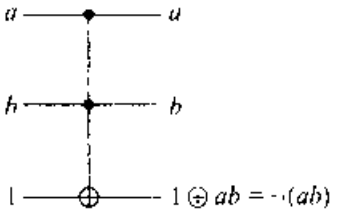


图 3.18 用一个 Toffoli 门实现一个与非门. 头两个比特表示与非门的输入，而第三个比特制备成有时称为辅助状态的标准状态 1. 与非门的输出在第三比特.

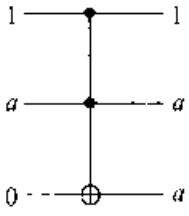


图 3.19 用 Toffoli 门实现的扇出运算. 第二个比特是扇出运算的输入，而其他两个比特是标准辅助状态. 扇出的输出出现在第二和第三比特.

研究可逆计算的动机是希望明白计算的能量要求. 显然无噪声撞球模型的操作不需要能量，基于 Toffoli 门的模型如何？这只能通过检查计算 Toffoli 门的特定模型来确定，第 7 章将考察几类这种实现，事实上，Toffoli 确实可以用不需要消耗任何能量的方式实现.

有一个严重的警告，这与计算可以不需要任何能量消耗的想法有关. 如前面已经介绍，计算的撞球模型对噪声高度敏感，许多其他可逆计算模型也是这样. 为消除噪声的影响，需要某种形式的纠错措施，这种纠错的办法通常涉及对系统的测量，以确定系统是按期望的方式运行，还是发生了差错. 由于计算机内存有限，存储着的用于纠错的测量结果最终必须擦除，以便为新的测量结果提供内存. 按照 Landauer 原理，这种擦除操作引起的相应能量消耗必须在统计总能量消耗时加以考虑. 在 12.4.4 节将更仔细地分析与纠错相联系的能耗.

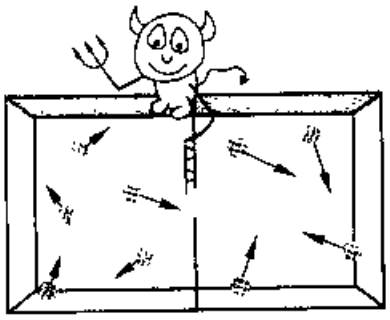
从对可逆计算的研究中可得出什么结论？有三个关键的思想. 首先，可逆性源于对每个比特信息的跟踪，不可逆性只发生在信息丢失或被擦除时. 其次，通过以可逆方式进行计算，我们消除了计算中的能量消耗. 最后，可逆计算可以有效进行，而且不产生其值依赖输入的垃圾比特，换句话说，如果一个不可逆电路计算函数 f，则存在一个作用为 $(x, y) \mapsto (x, y \oplus f(x))$ 的可逆电路，来对这个电路进行有效模拟.

这些结果对物理学、计算机科学以及量子计算与量子信息意味着什么？对一个关心散热的物理学家或硬件工程师而言，好消息是，原则上，通过将计算可逆化可以让计算没有热损耗，尽管实际中为了系统稳定和抗噪声还是需要消耗能量的. 在更基础的层次上，导致可逆计算的思想同样导致物理学基础中的一个世纪的老问题，著名的 Maxwell 妖(Maxwell's demon)问题的解决，这个问题的故事和它的解决在盒子 3.5 中简述. 从计算机科学家的角度看，可逆计算证实了在 Turing 机(因为使用它们或不使用它们给出的模型是多项式等价的)等计算模型中采用不可逆元件的合理性；而且，因为物理世界从根本上说是可逆的，所以基于计算的可逆模型的复杂性类比基于计算的不可逆模型的复杂性类更自然. 这个观点在问题 3.9 和"历史和进一步阅读的材料"中会再次提到. 从量子计算与量子信息的角度看，可逆计算极其重要. 为发挥量子计算的全部能力，任何经典的例程在量子计算中都必须以可逆和没有依赖经典输入的垃圾比特的方式下执行.

练习 3.32(从 Fredkin 门到 Toffoli 门以及逆过程)　模拟一个 Toffoli 门最少用多少 Fredkin 门？模拟一个 Fredkin 门最少用多少 Toffoli 门？

盒子 3.5　Maxwell 妖

热力学定律统治着在热力学平衡下一个物理系统能够做的工作，这些定律中的热力学第二定律说封闭系统的熵永远不会减少. 1871 年，James Clerk Maxwell 提出存在一个表面上违反这条定律的机器. 他假设了一个如下面的图中那样，可以减少初始条件下达到平衡的汽缸熵的小精灵. 汽缸中快和慢的分子被分隔成两半，小精灵呆在中间分隔壁的小门边上. 当快分子从左边靠近，小精灵就打开分隔壁上的门，让它通过，然后关上门. 这样做足够长时间以后，整个汽缸的熵会减少，这显然违反了热力学第二定律.



Maxwell 妖佯谬的解决办法在于小精灵必须测量在分隔壁之间移动的分子，以决定它们的速率，这个测量的结果必须存储在精灵的记忆中. 由于任何记忆空间都是有限的，精灵最终必须开始从它的记忆中擦除信息，以便可以有空间记忆新的测量结果. 由 Landauer 原理，这个擦除信息的动作会增加复合系统——精灵、汽缸和它们的环境——的熵. 实际上，完整的分析表明，Landauer 原理蕴含着，由于这个擦除信息动作引起的复合系统的熵增量至少是由于精灵行动引起复合系统熵的减少量，这就保证了热力学第二定律的遵守.

3.3 对计算科学的思考

本章的简短引论，不可能涉及像计算机科学这样一个内容丰富的领域中所有伟大思想的细节. 我们希望已经向读者传达了什么叫像计算机科学家那样思考，也提供了对理解计算非常重要的基本术语和一些基础性的概述. 作为本章的结束，我们简述一些更一般的问题，目的是提供量子计算与量子信息在整个计算机科学中的地位的一些看法.

我们的讨论一直围绕计算的 Turing 机模型. 计算的非经典模型，如大规模并行计算机、DNA 计算机和模拟计算机等，与标准的 Turing 机计算模型相比，计算能力如何？延伸一下，与量子计算相比呢？我们从并行计算结构开始. 现有的计算机绝大多数是在某个中央处理单元一次处理一条指令的串行计算机，与之对照，并行计算机可以一次处理一条以上的指令，对某些应用来说，可以节省可观的时间和金钱. 然而，当考虑效率问题时，并行处理并不能提供超越标准 Turing 机模型的根本好处，因为 Turing 机可以用多项式等价的物理资源——计算需要的总的时间和空间——来模拟并行计算机. 并行计算机带来的好处在时间方面，但它在计算需要的总的空间资源上却有损失，导致总体上来看，在计算模型的能力上没有本质变化.

大规模并行计算的一个有趣的特例是 DNA 计算技术. 一条 DNA 链(a strand of DNA)，脱氧核糖核酸，是一个分子(聚合体). 该分子由一连串四种以所载的碱基(base)区别的核苷(nucleotide)组成. 四种核苷分别记作 A(腺嘌呤)、C(胞嘧啶)、G(鸟嘌呤)和 T(胸腺嘧啶). 在特定条件下，碱基对形成互补(A 配 T，G 配 C)，两条链可以合成一个双链. 链的末端也是有区别且要互相匹配. 可以用化学技术增加以特定顺序开始或结束(多聚酶链式反应)的链的数量，按长度把链分开(凝胶体电泳)，把双链溶解成单链(改变温度和 PH 值)，读出链上的序列，对链在特定位置截断(限制酶)，也可检测试管中是否有特定的 DNA 序列. 可靠地使用这些技术的过程相当复杂，但基本的思想可以从下面的一个例子体现出来.

有向 Hamilton 路径问题是 3.2.2 节 Hamilton 圈问题的一个简单的和等难度的变形. 其目标是确定在一个 N 顶点的有向图 G 中，是否存在一条从特定的顶点 j_1 到 j_N 的路径，沿着边的允许方向，恰好经过每个顶点一次. 这个问题可以用 DNA 计算机按下面五个步骤来解决，其中 x_i 被选为碱基的惟一序列(面 $\bar{x}_i$ 是它们的补)，用 DNA 链 $x_i x_k$ 对边进行编码，用链 $\bar{x}_i\,\bar{x}_j$ 对顶点进行编码：(1)通过把代表顶点和边的所有可能的 DNA 链混合起来，组合出 G 的随机路径，并等待 DNA 链与互补核酸结合；(2)通过只扩增以 $\bar{x}_{j_1}$ 开始和以 $\bar{x}_{j_N}$ 结束的双链，留下从

j_1 开始和以 j_N 结束的路径；(3)按长度对链分离，选出长度为 N 的路径；(4)通过把 DNA 双链溶解为单链，并且依次与所有代表顶点的链结合并只过滤出那些能够结合的链，来选出经过每个顶点至少一次的路径；(5)检测是否有链经过选择步骤后存留下来. 如果是这样，那么存在这样的路径，否则不存在. 为保证答案以足够高的概率是正确的，x_j 可以选得包含很多碱基(约为 30)，在反应中使用大量(约为 10^{14} 或更多)的链.

还有一些基于这个基本想法的高级启发式方法. 当然，这样的穷举搜索方法只可用于能够有效产生所有可能路径的场合，因此，需要的分子数量随问题的规模(上述例子是顶点数)必然指数增长. DNA 分子相对微小并且容易合成，而且一个试管可容纳的海量 DNA 组合可以暂时避开指数复杂度的成本增加——大到几十个顶点规模. 但最终指数费用还是限制着这种方法的可用性. 因此，虽然 DNA 计算为解决某些问题提供了有吸引力和物理上可实现的计算模型，它还是一项经典计算技术，没有对 Turing 机从根本上提高.

模拟计算机(Analog computer)为进行计算提供了另外一套方案. 一台计算机是模拟的，当它采用的信息表示方式是基于连续的自由度，而不是 0 和 1. 例如，一个温度计就是一台模拟计算机. 模拟电路采用电阻、电容和放大器，也称为进行模拟计算. 这种机器在理想情况下具备无穷的资源，因为像位置和电压这样的连续变量可以存储无限的信息，但这只在没有噪声情况下成立. 有限程度的噪声使连续变量可以区分的状态减少为有限数量——从而将模拟计算机限制在有限容量的信息表示上. 实践中，噪声的限制使模拟计算机没有超过经典数字计算机，也就是 Turing 机的能力. 人们也许会怀疑量子计算机也不过就是模拟计算机，因为用连续参数来描述量子比特的状态，然而，事实上，量子计算机中噪声的效应可以被有效地数字化. 作为一个结论，量子计算机的计算优势甚至在有限噪声情况下仍得到保持.

噪声对数字计算机的影响如何？在计算研究的早期，噪声确实是问题. 在一些原始计算机中，真空管几分钟就出现一次故障. 即使是在今天，噪声对像调制解调器和硬盘这样的计算部件来说仍是一个问题. 人们为弄清如何用不可靠元件建造可靠计算机的问题投入了巨大的努力，von Neumann 证明仅需增加多项式规模的计算资源就可以做到这一点. 不过具有讽刺意味的是，现代计算机几乎完全没有用到那些结论. 因为现代计算机元件非常可靠，10^{-17} 甚至更低的差错率对现代电子元器件来说是很平常的. 出于这个原因，差错的发生很少，以致对付差错的额外努力被认为并不值得. 另一方面，我们将会发现量子计算机是非常脆弱的机器，看起来需要真正应用纠错技术.

不同的体系结构能够改变噪声的效应. 例如，如果忽略噪声，那么把计算机体系结构变成许多操作并行执行，并不会改变需要完成操作的数目，然而，并行系统

抗噪声的能力可能大大增强，因为噪声的影响积累的时间减少了. 因此，在现实的分析中，一个算法的并行版本可能比串行实现具有某些本质的优点. 体系结构设计是经典计算机的一个发展完善的领域. 在量子计算机方面却几乎没有任何类似的结果，但是噪声的研究已经提示给我们未来量子计算机体系结构的一些希望的特点，如高层次的并行化.

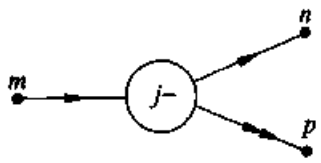
计算的第四种模型是分布式计算(distributed computation)，它是利用两个以上的空间分离的计算单元来解一个计算问题. 显然，因为它可以用 Turing 机有效模拟，所以这类计算模型不比 Turing 机模型更强大. 然而，分布式计算提出了一种有趣的新资源的挑战：在单元之间的通信费用高的情况下，如何最佳使用多计算单元？这个分布计算的问题随着计算机被高速网络连接起来变得特别有意义，虽然所有在网络上的计算机的总计算容量可能极其巨大，但利用这个潜力却是困难的. 大部分有趣的问题并不能很轻易地分解成可以独立求解的模块，而且可能要求不同计算子系统之间的频繁的全局通信，以交换中间结果或进行状态同步. 针对这些问题，已形成了通信复杂性(communication complexity)的研究领域，即通过量化解决问题的通信需求来处理这类问题. 当可以利用量子资源并且可以在分布式计算机之间交换量子资源时，有时通信的开销可以大大减少.

贯穿这些结论性的思想和整本书的一个反复出现的主题就是，尽管计算机科学和物理上的约束传统上是独立的，最终物理定律不仅对计算机如何实现，而且对那些类型的问题可以被解决还是有着重大影响. 量子计算与量子信息作为计算问题在物理上合理的替代模型，小心地保持了计算机科学的原则，同时又把计算机科学的概念带到物理学的前沿. 本书下面的任务是把这些来自完全不同领域的思想以及它们产生的令人兴奋的结果编织在一起.

问题 3.1（Minsky 机器） 一台 Minsky 机器由一组有限寄存器的集合 $r_1, r_2, \cdots, r_k$ 和一个程序组成，每个寄存器可以存储任意非负整数. 程序由两类命令中的一类组成. 第一类具有形式：

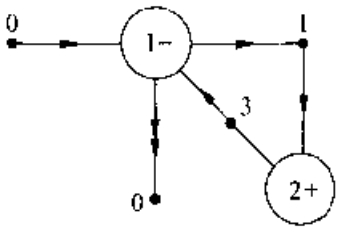


表明在程序中的 m 点，寄存器 r_j 增加 1，并且程序的执行前进到点 n. 第二类命令具有形式：



表明在程序中的 m 点，寄存器 r_j 如果包含一个正整数就减 1，并前进到程序的点

n;如果寄存器 r_j 是 0,简单地前进到程序中的 p 点. Minsky 机器的程序由这样一组命令组成,如形式:



程序的起始点和所有可能的停机点,习惯上都标为 0. 这个程序把寄存器 r_1 的内容加到寄存器 r_2 上,同时 r_1 本身减到 0.

(1) 证明所有(Turing)可计算函数均可用 Minsky 机器下计算,即给定一个可计算函数 $f(\cdot)$,存在一个 Minsky 机器的程序,使得当寄存器从状态 $(n,0,\cdots,0)$ 开始时,给出输出 $(f(n),0,\cdots,0)$.

(2) 根据定义,任意可用 Minsky 机器计算的函数,也能够用 Turing 机计算. 给出证明的梗概.

问题 3.2(向量游戏)　一个向量游戏由一组有限个同维整数坐标的向量给定,游戏从一个非负整数坐标向量 x 开始,往 x 上加上向量组中首个保持坐标非负性的向量. 重复这个过程,直到无法继续. 证明对任意的可计算函数 $f(\cdot)$,存在一个向量游戏,从向量 $(n,0,\cdots,0)$ 开始到达 $(f(n),0,\cdots,0)$(提示:证明一个 $k+2$ 维的向量游戏,可以模拟一台包含 k 个寄存器的 Minsky 机器).

问题 3.3(Fractran)　一个 Fractran 程序由一组正有理数 $q_1,\cdots,q_n$ 定义. 它在正整数 m 上的作用是用 $q_i m$ 代替 m,这里 i 是使 $q_i m$ 为整数的最小数. 如果没有 i 使 $q_i m$ 是整数,程序的执行就停止. 证明对任意的可计算函数 $f(\cdot)$,存在一个 Fractran 程序,从 2^n 开始到达 $2^{f(n)}$ 而不经过 2 的任何中间次幂(提示:利用前一个问题).

问题 3.4(动态系统的不可判定性)　Fractran 程序实质上是一个非常简单的动态系统,它把正整数变到正整数. 证明不存在算法,判定这样的动态系统是否到过 1.

问题 3.5(两比特可逆逻辑的非通用性)　假设我们试图仅用一比特和两比特可逆逻辑门和辅助比特建造电路,证明存在不能用这种方式计算的 Boolean 函数. 由此推断 Toffoli 门即使有辅助比特的帮助,也不能用单比特和两比特可逆门模拟.

问题 3.6(逼近 TSP 的难度)　令 $r\geqslant 1$,并且设存在一个 TSP 的近似算法,可以保证找到在因子 r 以内的 n 城市的最短旅行. 令 $G=(V,E)$ 是 n 顶点的任意图. TSP 的一个实例定义是,将城市与 V 中顶点对应,如果 (i,j) 是 G 一边,则定义城市 i 和 j 之间的距离为 1,否则距离定义为 $\lceil r\rceil|V|+1$. 证明如果把近似算法应用到 TSP 的这个实例,那么如果 G 存在 Hamilton 圈,它将给出 G 的一个 Hamilton 圈,

否则它将给出一个长度超过$\lceil r \rceil |V|$的旅行. 从 HC 的 NP 完全性可知,不存在这样的近似算法,除非 P=NP.

问题 3.7(可逆 Turing 机)

(1) 说明如何构造一个能够计算与普通 Turing 机同类函数的可逆 Turing 机(提示:也许采用多带结构会有帮助).

(2) 相对普通单带 Turing 机上计算函数 $f(x)$ 需要的时间 $t(x)$和空间 $s(x)$,给定你的可逆 Turing 机操作的空间和时间界.

* **问题 3.8**(找出难计算的函数类) 求一个自然的函数类,它满足 n 输入需要超多项式 Boolean 门计算.

问题 3.9(可逆 PSPACE = PSPACE) 容易证明带量词的可满足性(quantified satisfiability)问题 QSAT 是 PSPACE 完全的,即 PSPACE 中任何其他问题可以在多项式时间内归约为 QSAT. QSAT 的语言定义为 Boolean 公式 φ 的全集,φ 有 n 变量 $x_1,\cdots,x_n$,它的合取范式如下.

$$\exists_{x_1} \forall_{x_2} \exists_{x_3} \cdots \forall_{x_n} \varphi, \text{如果 } n \text{ 是偶数} \tag{3.9}$$

$$\exists_{x_1} \forall_{x_2} \exists_{x_3} \cdots \exists_{x_n} \varphi, \text{如果 } n \text{ 是奇数} \tag{3.10}$$

证明在多项式空间上操作的可逆 Turing 机可以解 QSAT,因此在多项式空间上进行可逆操作的计算机可以判定的语言类等同于 PSPACE.

问题 3.10(辅助比特和可逆计算的效率) 令 p_m 是第 m 个素数,给出一个当输入 m 和 n 且 $n>m$ 时,输出乘积 $p_m p_n$ 的可逆电路的框架,即$(m,n) \rightarrow (p_m p_n, g(m,n))$,其中 $g(m,n)$是电路使用的辅助比特的最终状态. 估计你所需辅助比特的数目,证明如果可以找到一个多项式规模的可逆电路,它使用 $O(\log(\log n))$辅助比特,则两个素数乘积的因子问题属于 P.

历史和进一步阅读的材料

计算机科学是一个包含许多有趣子领域的庞大领域,在非常有限的篇幅内不可能完整涉及. 我们只希望能借此机会推荐一些有普遍意义的题目和一些与本书内容有关的特殊主题,希望这些内容可以激发读者兴趣.

现代计算机科学可追溯到 1936 年 Turing 的论文[Tur36]. Church Turing 论题是 Church 在 1936 年[Chu36]首先叙述的,接着由 Turing 从不同的角度给出更完整的讨论. 几乎同时,其他作者也得到过类似的结论. 许多这类工作和关于历史的讨论可以在 Davis 编辑的书卷[Dav65]中找到. Church Turing 论题和不可判定性的富于启发性的讨论可以在 Hofstadter[Hof79]和 Penrose[Pen89]中找到.

算法设计方面有许多优秀著作,我们只列三本. 首先是 Knuth[Knu97,Knu98a,Knu98b]的经典系列,它们覆盖了计算机科学的很大一部分内容. 其次是 Cormen、

Leiserson 和 Rivest[CLR90]的非凡著作，这本巨著包含算法设计的许多领域的很好的材料. 最后是 Motwani 和 Raghavan[MR95]的书，对随机算法领域作了极好的综述.

现代计算复杂性理论特别受到 Cook[Coo71]和 Karp[Kar72]论文的影响. 俄国的 Levin[Lev73]也独立提出类似的想法，但不幸的是花了很长时间才传播到西方. Garey 和 Johnson[GJ79]的经典著作也对这个领域有巨大影响. 最近 Papadimitriou[Pap94]写了一部综述计算复杂性理论许多主要思想的优美作品. 本章中我们只考虑了语言之间一种类型的归约，多项式归约. 语言之间还有许多其他类型的归约. Ladner、Lynch 和 Selman[LLS75]给出这方面的一个早期综述. 后来归约的不同概念发展成一个称为结构复杂性的子领域，Balcázar、Diaz 和 Gabarró[BDG88a, BDG88b]对其作了综述.

对信息、能量耗散和计算之间联系的研究经历了一个很长的历史. 现代的工作开始于 Landauer 1961 年的论文[Lan61]，该论文首次提出了 Landauer 原理. Szilard[Szi29]的论文和 1949 年 Von Neumann 的演讲[von66]（第 66 页）曾得到接近于 Landaure 原理的结论，但没有完全抓住擦除信息需要耗散的实质.

可逆 Turing 机是 Lecerf[Lec63]和后来 Bennett[Ben73]很有影响的论文独立地提出的. Fredkin 和 Toffoli[FT82]引入计算的可逆电路模型. Barton 的 1978 年 5 月 MIT6.895 学期论文[Bar78]和 Ressler 的 1981 年的硕士论文[Res81]是两份有价值的历史文献，它们包含可逆 PDP-10 的设计，可逆逻辑对实现低功耗 CMOS 电路有潜在的重要性[YK95].

Maxwell 妖是一个有长而复杂历史的、让人着迷的话题，Maxwell 于 1871 年[Max71]提出. Szilard 于 1929 年发表了一篇关键的论文[Szi29]，它预示了许多最终解决 Maxwell 妖问题的细节. 1965 年 Feynman[FLS65b]解决了 Maxwell 妖问题的一种特殊情况，Bennett 在 Landauer 工作[Lan61]基础上，写了关于这个话题的两篇优美的文章[Ben82a, Ben87]，从而彻底地解决了这个问题. Leff 和 Rex[LR90]的论文集是关于 Maxwell 妖问题和解决这个问题的历史的一本很有意思的书.

DNA 计算是 Adleman 发明的，我们描述的有向 Hamilton 路径问题的解法就属于他[Adl94]. Lipton 也展示了如何在这个模型中解 3SAT 和可满足性问题[Lip95]. Adleman 在科学美国人杂志上的文章[Adl98]是一篇很好的科普文章. Winfree[Win98]给出 DNA 操作的通用性的一个有启发性的介绍. 要了解噪声情形下的可靠计算可以读 Winograd 和 Cowan 的书[WC67]. 第 10 章还会涉及这个话题. Hennessey、Goldberg 和 Patterson[HGP96]的书是计算机体系结构的一本好教材.

问题 3.1 到问题 3.4 展示了 Minsky 提出的（在他的关于计算机器的优美作品[Min67]中）Conway[Con72, Con86]发展的一条思路. Fractran 程序语言肯定是已知的最优美的通用计算模型之一，这可以从下面称为 PRIMEGAME[Con85]的例子看出.

PRIMEGAME 定义为如下的一串有理数：

$$\frac{17}{91},\frac{78}{85},\frac{19}{51},\frac{23}{38},\frac{29}{33},\frac{77}{29},\frac{95}{23},\frac{77}{19},\frac{1}{17},\frac{11}{13},\frac{13}{11},\frac{15}{2},\frac{1}{7},\frac{55}{1}$$

惊人的是，当 PRIMEGAME 从 2 开始时，出现的其他 2 的幂，即 $2^2,2^3,2^5,2^7,2^{11},2^{13},\cdots$，恰好是 2 的素数幂，指数依次是所有素数. 问题 3.9 是更一般的可逆计算空间资源需求的特例，参看 Bennett[Ben82] 和 Li、Tromp 与 Vitanyi[LV96,LTV98] 的论文.

第二部分

量子计算

第 4 章

量子线路

计算理论的研究传统上是纯数学的一个分支，几乎完全抽象. 这样会偏离主题. 计算机是物理的对象，而计算是物理的过程. 计算机计算的范围完全由物理定律而不是纯数学决定.

——*David Deutsch*

像数学一样，计算机科学和其他科学稍有差别. 计算机科学研究能被证明的人为规律，而不是永远无法彻底了解的自然规律.

——*Donald Knuth*

一条深刻真理的反面也许是另一条深刻真理.

— *Niels Bohr*

本书的第二部分从本章开始，详细介绍量子计算. 本章内容包括叙述量子计算的基本原理，建立量子线路的基本模块，描述复杂量子计算的通用语言. 在接下来的两章讲述从这些线路构造起来的两个已知的基本的量子算法. 第 5 章是量子 Fourier 变换及其在相位估计、求阶和因子问题中的应用；第 6 章是量子搜索算法及其在数据库搜索、计数和 NP 完全问题加速中的应用. 本书第二部分的最后一章，第 7 章讨论如何实验实现量子计算.

考虑到具有量子计算以外的广泛意义，量子计算的另外两个具有重要意义的主题：量子噪声和量子纠错将在本书第三部分中介绍.

本章引入两个主要思想. 首先详细说明量子计算的基本模型：量子线路模型；其次说明存在一小组通用门，即任何量子计算都可由这些门表出. 沿着这条思路，我们还要描述量子计算的许多其他基本结果. 4.1 节以对量子算法的总论开始，重点介绍已知的算法和它们结构背后的通用技术. 4.2 节将仔细研究单量子比特运算. 尽管这些运算都很简单，但单量子比特运算为建造各种例子和技术提供了丰富

的空间，因此对它们的深入理解非常重要. 4.3 节展示如何进行多量子比特受控酉(controlled unitary)运算. 4.4 节讨论量子线路模型中测量的描述. 这些内容接着被一起用到 4.5 节，来叙述和证明通用性定理. 4.6 节总结量子计算的所有基本运算，并且讨论这个模型可能的变形，还要讨论量子计算机与经典计算机计算能力的关系这一重要问题. 4.7 节以量子计算在实际量子系统的仿真方面的重要而有用的应用来结束本章.

本章或许是本书中读者参与最多的一章. 读者需要完成高密度的练习，有必要在此解释这种高强度参与的原因. 计算的量子线路模型的基本工具很容易理解，但如果要进一步面对更复杂的量子算法设计问题，就需要熟练掌握大量的简单结果和技巧. 出于这个原因，本章采用面向例子的方式，请读者来完成很多细节，以熟练掌握这个工具. 直接跳到 4.6 节，可以对量子计算的基本内容有一个稍微轻松，但多少有些肤浅的大概了解.

4.1 量子算法

量子计算机长处何在？我们经常感到沮丧，因为需要更多的计算机资源来解计算问题. 实际中，许多有趣的问题都不可能在一台经典计算机上求解，倒不是这些问题从根本上不可解，而是因为解它们需要天文数字的资源.

量子计算机引人入胜的前景在于，它可以使用新算法，解决那些在经典计算机上需要过多资源才能求解的问题. 当写作本书的时候，已经知道有两大类量子算法可以实践这个诺言. 第一类算法基于 Shor 的量子 Fourier 变换，包括解因子(factoring)问题和离散对数(discrete logarithm)问题的令人瞩目的算法. 这些算法提供了对最好的经典算法的惊人的指数加速. 第二类算法基于 Grover 的量子搜索(quantum searching)的算法. 这些算法提供略为逊色，但仍相当可观的对最好的经典算法二次(quadratic)加速. 量子搜索算法的重要性在于，经典算法中基于搜索技术应用非常广泛，这些应用中，许多都可以直接搬用比经典算法更快的量子算法.

图 4.1 是本书写作时有关量子算法知识的草图，还包括那些算法的应用的一些例子. 量子 Fourier 变换和量子搜索算法自然处在图的核心位置. 图中的量子计数(Quantum counting)算法特别有趣，这个算法是量子搜索和量子 Fourier 变换算法的巧妙结合，它可以比经典计算机更快地估计出搜索问题的解的数目.

量子搜索算法有许多潜在的应用，但这里只说明其中几个. 它可以比经典计算机更快地提取无序数据集中最小元的统计量，也可用于对 NP 类中的某些问题进行加速——特别是那些最好解决办法是直接搜索的问题. 最后，它可被用于加速像广泛使用的数据加密标准(data encryption standard，DES)那样的密码系统密钥的

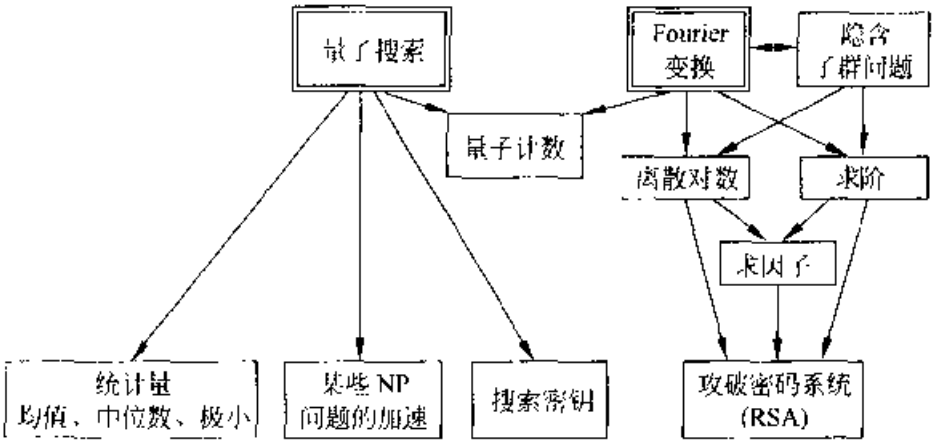


图 4.1　主要的量子算法以及它们的关系，还包括一些值得注意的应用.

搜索. 这些以及其他应用将在第 6 章说明.

量子 Fourier 变换也有许多有趣的应用，它可以用来解离散对数和因子问题. 这些结果又使得量子计算机能够用于破解许多正在使用的最流行的密码系统，包括 RSA 密码系统. Fourier 变换事实上和数学中的一个重要问题有密切关系，即求隐含子群(hidden subgroup)(求周期函数周期的一个推广)问题. 量子 Fourier 变换和它的一些应用，包括快速量子因子分解和离散对数算法将在第 5 章说明.

为什么所知比经典算法更好的量子算法如此之少？答案是想出一个好的量子算法是件困难的事. 这至少有两个原因. 第一，不管是经典的还是量子的算法，算法设计本身就不容易. 算法的发展历史告诉我们，即使对像两个数相乘这样简单的问题，也需要相当的独创性才能获得接近最优的算法. 发明好的量子算法更是面临双重困难，因为大家希望这些算法应该超过最好的现有的经典算法. 第二，相对量子世界而言，我们的直觉更适应经典世界. 如果用自然的直觉去思考问题，那么，我们想出的算法将是经典算法，所以想出好的量子算法需要特别的灵感和特别的技巧.

量子算法的进一步研究将推迟到下一章. 本章为描述量子算法提供有效和有力的语言，即量子线路语言，它包含描述计算过程的一组离散元件的集合. 这个工具将使我们能够用类似于需要的门的总数或线路深度等数量，来量化算法的费用，它也带来简化算法设计的丰富技巧，并较容易地从概念上认识算法.

4.2　单量子比特运算

量子计算工具箱的发展从一切量子系统中最简单的——单量子比特上的运算开始. 单量子比特门在 1.3.1 节已经引入，让我们很快地总结一下在那里所学的.

随着叙述的展开,"术语和记号"中的记号注释也许对读者有参考价值.

一个单量子比特是一个向量 $|\psi\rangle = a|0\rangle + b|1\rangle$,它有两个复参数 a, b,满足 $|a|^2 + |b|^2 = 1$. 量子比特上的运算必须保持该范数,由 2×2 酉矩阵给出. 其中,最重要的一些矩阵包括 Pauli 矩阵,这里再次列出如下.

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{4.1}$$

另外三个量子门将在后面扮演重要角色,分别是 Hadamard 门(记作 H),相位门(phase gate,记作 S)和 $\pi/8$ 门(记作 T):

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix} \tag{4.2}$$

需要记住的代数事实是 $H = (X+Z)/\sqrt{2}$ 和 $S = T^2$. 读者也许会问,为什么 T 门称为 $\pi/8$ 门,而定义中出现的却是 $\pi/4$. 这个门在历史上常被称为 $\pi/8$ 门,只是因为除了一个不重要的全局相位,T 等同于一个在对角线上是 $\exp(\pm i\pi/8)$ 的门

$$T = \exp(i\pi/8) \begin{bmatrix} \exp(-i\pi/8) & 0 \\ 0 & \exp(i\pi/8) \end{bmatrix} \tag{4.3}$$

不管怎样,这个名称从某些方面看相当令人遗憾,故我们常把这个门称为 T 门.

回忆一个处子状态为 $a|0\rangle + b|1\rangle$ 的单量子比特可显示为单位球面上的点 (θ, φ),其中 $a = \cos(\theta/2)$,$b = e^{i\varphi}\sin(\theta/2)$,并且因为状态的全局相位是不可观测的,$a$ 可以取为实数. 这称为 Bloch 球面表示. 向量 $(\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta)$ 称为 Bloch 向量. 为帮助直观理解,我们会常用到这个表示.

练习 4.1 练习 2.11 计算了 Pauli 矩阵的特征向量(如果还没有做这个练习,请现在就做),在 Bloch 球面上求出不同 Pauli 矩阵的归一化特征向量对应的点.

当出现在指数中时,Pauli 矩阵导出三类有用的酉矩阵,称为关于 $\hat{x}$,$\hat{y}$ 和 $\hat{z}$ 轴的旋转算子(rotation operator),如下式定义:

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} X = \begin{bmatrix} \cos\dfrac{\theta}{2} & -i\sin\dfrac{\theta}{2} \\ -i\sin\dfrac{\theta}{2} & \cos\dfrac{\theta}{2} \end{bmatrix} \tag{4.4}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y = \begin{bmatrix} \cos\dfrac{\theta}{2} & -\sin\dfrac{\theta}{2} \\ \sin\dfrac{\theta}{2} & \cos\dfrac{\theta}{2} \end{bmatrix} \tag{4.5}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix} \tag{4.6}$$

练习 4.2 令 x 为一实数,A 为一矩阵,满足 $A^2 = I$,证明

$$\exp(iAx) = \cos(x) I + i\sin(x) A \tag{4.7}$$

利用这一结果验证式(4.4)到式(4.6).

练习 4.3　证明除了一个全局相位，$\pi/8$ 门满足 $T=R_z(\pi/4)$.

练习 4.4　对某个 φ，把 Hadamard 门表示为旋转 R_x 和 R_z 以及 $e^{i\varphi}$ 的乘积.

若 $\hat{n}=(n_1,n_2,n_3)$ 为三维空间中的实单位向量，则我们通过下式定义关于 $\hat{n}$ 角度为 θ 的旋转，来推广前面的定义.

$$R_{\hat{n}}(\theta)\equiv \exp(-i\theta\hat{n}\cdot\sigma/2)=\cos\left(\frac{\theta}{2}\right)I-i\sin\left(\frac{\theta}{2}\right)(n_xX+n_yY+n_zZ) \tag{4.8}$$

其中 σ 表示 Pauli 矩阵的三元向量 (X,Y,Z).

练习 4.5　证明 $(\hat{n}\cdot\sigma)^2=I$，并以此验证式(4.8).

练习 4.6(旋转的 Bloch 球面解释)　$R_{\hat{n}}(\theta)$ 算子称为旋转算子的一个原因是如下要证明的事实. 假设一个单量子比特的状态由 Bloch 向量 $\boldsymbol{\lambda}$ 表示，则旋转 $R_{\hat{n}}(\theta)$ 在该状态上的作用，是绕 Bloch 球面的 $\hat{n}$ 轴转 θ 角. 这个事实解释了旋转矩阵中出现的看来特别神秘的因子 2.

练习 4.7　证明 $XYX=-Y$，并以此证明 $XR_y(\theta)X=R_y(-\theta)$.

练习 4.8　任意一个单量子比特酉算子可写成形式

$$U=\exp(i\alpha)R_{\hat{n}}(\theta) \tag{4.9}$$

其中 α 和 θ 是两个实数，$\hat{n}$ 是三维实单位向量.

(1) 证明这个事实；

(2) 求 α、θ 和 $\hat{n}$ 以得到 Hadamard 门 H；

(3) 求 α、θ 和 $\hat{n}$ 以得到相位门

$$S=\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix} \tag{4.10}$$

单量子比特上的任意的酉算子可以写成很多种形式，如旋转的组合，再加上一个该量子比特上的全局相移. 下述定理提供了一种表达任意单量子比特旋转的方法，它在后面受控算子的应用中特别有用.

定理 4.1(单量子比特的 z-y 分解)　设 U 是单量子比特上的酉算子，则存在实数 α,β,γ 和 δ，使得

$$U=e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta) \tag{4.11}$$

证明　由于 U 是酉的，U 的行和列是正交的，于是可知存在实数 α,β,γ 和 δ，使得

$$U=\begin{bmatrix}e^{i(\alpha-\beta/2-\delta/2)}\cos\dfrac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\dfrac{\gamma}{2}\\ e^{i(\alpha+\beta/2-\delta/2)}\sin\dfrac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\dfrac{\gamma}{2}\end{bmatrix} \tag{4.12}$$

从旋转矩阵和矩阵相乘的定义，立即可以得到式(4.11).

练习 4.9 解释为什么任意单量子比特上的酉算子可以写成式(4.12)的形式.

练习 4.10(旋转的 x-y 分解) 用 R_x 代替 R_z,给出相应于定理 4.1 的分解.

练习 4.11 设 $\hat{m}$ 和 $\hat{n}$ 是三维空间中不平行的实单位向量,证明任意单量子比特上的酉算子对适当的 α,β_k,γ_k,可以写成

$$U = e^{i\alpha}R_{\hat{n}}(\beta_1)R_{\hat{m}}(\gamma_1)R_{\hat{n}}(\beta_2)R_{\hat{m}}(\gamma_2)\cdots, \tag{4.13}$$

定理 4.1 的作用在子其如下特别的推论.如下一节将看到的,它是构造受控的多量子比特酉运算的关键.

推论 4.2 设 U 是单量子比特上的酉门,则存在单量子比特上的酉算子 A,B,C,使得 $ABC=I$ 且 $U=e^{i\alpha}AXBXC$,其中 α 为某个全局相位因子.

证明 仍采用定理 4.1 的记号,令 $A\equiv R_z(\beta)R_y(\gamma/2)$,$B\equiv R_y(-\gamma/2)R_z\times(-(\delta+\beta)/2)$,$C\equiv R_z((\delta-\beta)/2)$.注意

$$ABC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(-\frac{\gamma}{2}\right)R_z\left(-\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) = I \tag{4.14}$$

由于 $X^2=I$,并且由练习 4.7,可得

$$XBX = XR_y\left(-\frac{\gamma}{2}\right)XXR_z\left(-\frac{\delta+\beta}{2}\right)X = R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right) \tag{4.15}$$

于是

$$AXBXC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) \tag{4.16}$$

$$= R_z(\beta)R_y(\gamma)R_z(\delta) \tag{4.17}$$

因此 $U=e^{i\alpha}AXBXC$ 且 $ABC=I$,如所欲证.

练习 4.12 给出 Hadamard 门的 A,B,C 和 α.

练习 4.13(线路恒等式) 能以熟知的恒等式来简化线路非常有用,证明如下三个恒等式:

$$HXH = Z,\quad HYH = -Y,\quad HZH = X \tag{4.18}$$

练习 4.14 利用前面的练习证明除了一个全局相位,$HTH=R_x(\pi/4)$.

练习 4.15(单量子比特运算的组合) Bloch 球面为显示两个旋转组合的效果提供了一条很好的途径.

(1) 证明如果绕轴 $\hat{n}_1$ 旋转一个角 β_1,接着绕轴 $\hat{n}_2$ 旋转一个角 β_2,则总的旋转为如下给出的绕轴 $\hat{n}_{12}$ 转角 β_{12} 的旋转.

$$c_{12} = c_1c_2 - s_1s_2\hat{n}_1\cdot\hat{n}_2 \tag{4.19}$$

$$s_{12}\hat{n}_{12} = s_1c_2\hat{n}_1 + c_1s_2\hat{n}_2 - s_1s_2\hat{n}_2\times\hat{n}_1 \tag{4.20}$$

其中 $c_i=\cos(\beta_i/2)$,$s_i=\sin(\beta_i/2)$,$c_{12}=\cos(\beta_{12}/2)$ 和 $s_{12}=\sin(\beta_{12}/2)$.

(2) 证明若 $\beta_1=\beta_2$ 且 $\hat{n}_1=\hat{z}$,则这些等式可简化为

$$c_{12} = c^2 - s^2\hat{z}\cdot\hat{n}_2 \tag{4.21}$$

$$s_{12}\hat{n}_{12} = sc(\hat{x}+\hat{n}_2) - s'\hat{n}_2 \times \hat{z} \tag{4.22}$$

其中 $c=c_1$ 且 $s=s_1$.

图 4.2 给出常用单量子比特门的符号. 回忆量子线路的基本性质：时间前进自左向右，连线代表量子比特，而“/”用于指示量子比特束.

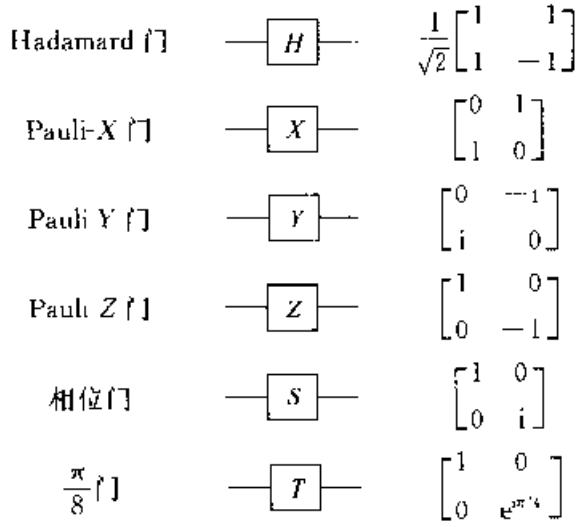


图 4.2　常用单量子比特的名称、符号和酉矩阵.

4.3　受控运算

“若 A 为真，则 B 亦为真”，不管是经典还是量子计算，这类受控运算(controlled operation)都是计算中最有用的运算之一. 本节说明，如何用从基本运算基础上建造起来的量子线路实现复杂的受控运算.

受控运算的原型是在 1.2.1 节遇到的受控非门，CNOT 门，它是具有分别称为控制量子比特(control qubit)和目标量子比特(target qubit)的双量子比特门，如图 4.3 所示. 相当于计算基，受控非门的作用由 $|c\rangle|t\rangle \to |c\rangle|t\oplus c\rangle$ 给出，即如果控制量子比特置为 $|1\rangle$，则目标量子比特翻转，否则目标量子比特保持不变. 于是，在|控制，目标〉基下，受控非门的矩阵表示为



图 4.3　受控非门的线路表示. 顶上的连线表示控制量子比特，底下的连线表示目标量子比特.

$$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix} \tag{4.23}$$

更一般地，设 U 是一个单量子比特上的任意酉运算，一个受控 U 运算为一个双量子比特运算，也具有控制量子比特和目标量子比特. 若控制量子比特置位，则 U 应用到目标量子比特上，否则目标量子比特保持不变，即 $|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle$. 受控 U 运算由图 4.4 中的线路表示.

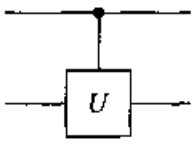
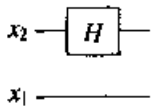
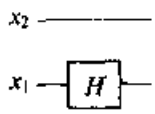


图 4.4 受控 U 运算. 顶上的连线表示控制量子比特，底下的连线表示目标量子比特. 若控制量子比特置位，则 U 应用到目标量子比特上，否则目标量子比特保持不变.

练习 4.16（多量子比特门的矩阵表示） 在计算基下，如下线路的 4×4 酉矩阵是什么？



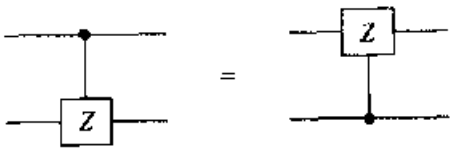
如下线路在计算基下的酉矩阵是什么？



练习 4.17（由受控 Z 门建造受控非门） 从一个受控 Z 门——即一个在计算基下的作用由如下酉矩阵表示——和两个 Hadamard 门构造一个受控非门，并指定控制量子比特和目标量子比特

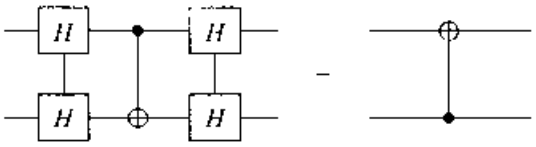
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

练习 4.18 证明下图



练习 4.19（受控非门在密度矩阵上的作用） 受控非门在密度矩阵 ρ 上的作用是重排矩阵元素的位置，故仅为一置换. 在计算基下清晰地写出它的作用.

练习 4.20(受控非门的基变换)　不像理想的经典门，理想的量子门没有（如电子工程师说的）高阻抗输入. 实际上，“控制”和“目标”的角色是随意的——它们的区分依赖于你认为该设备在哪组基下运算. 我们已经描述了受控非门相对计算基的行为，并且在这个描述中控制量子比特是不变的. 然而，如果考虑一组不同的基，则控制量子比特的确要变：我们将看到依赖于“目标”量子比特的状态，它的相位要翻转. 证明下图



引入基状态组 $|\pm\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$，利用这个线路恒等关系证明一个第一量子比特作为控制，第二量子比特作为目标的受控非门的作用为

$$|+\rangle|+\rangle\rightarrow|+\rangle|+\rangle \tag{4.24}$$

$$|-\rangle|+\rangle\rightarrow|-\rangle|+\rangle \tag{4.25}$$

$$|+\rangle|-\rangle\rightarrow|-\rangle|-\rangle \tag{4.26}$$

$$|-\rangle|-\rangle\rightarrow|+\rangle|-\rangle \tag{4.27}$$

因此，相对这组新基，目标量子比特的状态不变，而控制量子比特的状态在目标是 $|-\rangle$ 的时候翻转，否则保持不变，即在这组基下，目标和控制的角色实质上互换了.

我们紧接着的目标是弄清，如何仅用单量子比特运算和受控非门实现任意单量子比特的受控 U 门. 办法是基于推论 4.2 中给出的分解 $U=e^{i\alpha}AXBXC$ 的一个两步过程.

第一步是在控制量子比特控制下，在目标量子比特上相移 $e^{i\alpha}$. 即，若控制量子比特是 $|0\rangle$，则目标量子比特不变，而若控制量子比特是 $|1\rangle$，则在目标上应用相移 $e^{i\alpha}$. 仅用一个单量子比特酉门实现这一运算的线路，如图 4.5 右半部分所示. 为验证这个线路功能正确，我们需要注意右半部分线路的作用为

$$|00\rangle\rightarrow|00\rangle,\ |01\rangle\rightarrow|01\rangle,\ |10\rangle\rightarrow e^{i\alpha}|10\rangle,\ |11\rangle\rightarrow e^{i\alpha}|11\rangle \tag{4.28}$$

恰好是对左半部分受控运算所要求的.

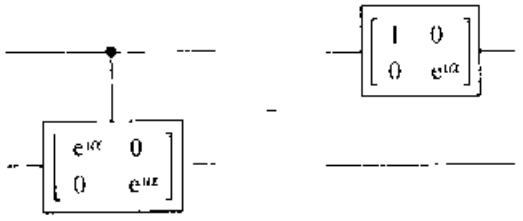


图 4.5　受控相移门及其双量子比特的等价线路.

如图 4.6 所示，我们现在可以来完成受控 U 运算的构造了. 为弄清为什么这个线路是正确的，回忆推论 4.2，U 可写成的 $U=e^{i\alpha}AXBXC$ 形式，其中 A,B,C 都是单量子比特运算，且满足 $ABC=I$. 设控制量子比特被置位，则 $e^{i\alpha}AXBXC=U$ 被应用到第二量子比特. 另一方面，若控制量子比特没有被置位，则运算 $ABC=I$ 被用到第二量子比特，即没有变化. 因此该线路实现了受控 U 运算.

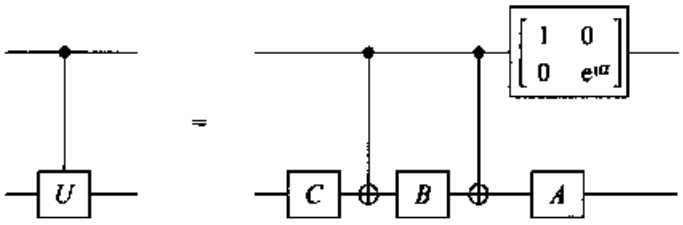


图 4.6 单量子比特的受控 U 运算的线路实现，α,A,B 和 C 满足 $U=\exp(i\alpha)AXBXC, ABC=I$.

现在我们知道，如何用单量子比特置位为条件，但对多量子比特如何设置条件呢？我们遇到过多量子比特设置条件的例子，如 Toffoli 门. 这个门在前两个控制量子比特满足都置 1 的条件时，使第三目标量子比特翻转. 更一般地，设有 $n+k$ 量子比特，并且 U 是一个 k 量子比特酉算子，则按下式，定义受控运算 $C^n(U)$

$$C^n(U)\mid x_1x_2\cdots x_n\rangle\mid\phi\rangle=\mid x_1x_2\cdots x_n\rangle\mid U^{x_1x_2\cdots x_n}\mid\phi\rangle \qquad (4.29)$$

其中 U 的指数中的 $x_1x_2\cdots x_n$ 表示比特 $x_1,x_2,\cdots,x_n$ 的积，即若前 n 量子比特全为 1，则算子 U 应用到后 k 量子比特，否则，什么也不做. 鉴于这类条件运算非常有用，我们引入专门的线路符号来表示它们，如图 4.7. 下面为简单起见，假设 $k=1$. 对 k 更大的情形本质上可以用同样的方法处理，不过 $k\geqslant 2$ 时，我们尚不清楚如何进行 k 量子比特上的任意运算.

假设 U 是单量子比特的酉算子，且 V 是使 $V^2=U$ 的酉算子，则运算 $C^2(U)$ 可用图 4.8 所示的线路实现.

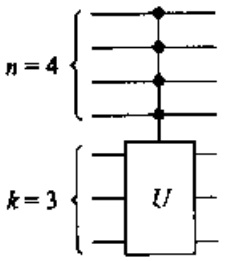


图 4.7 $C^n(U)$ 运算线路表示 $n=4$，$k=3$ 的例子，其中 U 是 k 量子比特上的一个酉算子.

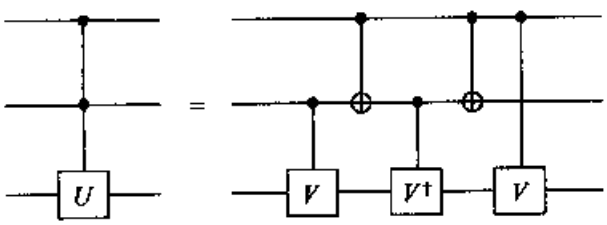


图 4.8 $C^2(U)$ 的线路，其中 V 是满足 $V^2=U$ 的任意酉算子. $V\equiv(1-i)(I+iX)/2$ 的特殊情形对应 Toffoli 门.

练习 4.21　验证图 4.8，实现 $C^2(U)$ 的运算.

练习 4.22　证明一个 $(C^2(U))$ 门(对任意单量子比特酉算子 U)可至多用八个单量子比特门和六个受控非门构造出来.

练习 4.23　仅用受控非门和单量子比特门构造一个 $U=R_x(\theta)$ 和 $U=R_y(\theta)$ 的 $C^1(U)$ 门.你能够把所需的单量子比特门的数量减到三个或两个吗?

所熟知的 Toffoli 门是 $C^2(U)$ 运算的极重要的特例，即 $C^2(X)$. 定义 $V\equiv(1-i)(I+iX)/2$，并注意到 $V^2=X$，可知图 4.8 给出了以单或双量子比特运算形式的 Toffoli 门实现. 从经典的角度看，这是一个了不起的结果，因为在问题 3.5 中，曾看到仅用单和双经典比特可逆门，不足以实现 Toffoli 门，或者更一般地，实现通用计算. 与之对照，在量子情形，我们看到单量子比特和双量子比特可逆门可以实现 Toffoli 门，而且最终我们将证明它们足以实现通用计算.

最终我们将证明，任意一个酉算子可以仅由 Hadamard、相位、受控非门和 $\pi/8$ 门组合来实现，这实现是个任意好的近似. 由于 Toffoli 门非常有用，值得看一下它是如何用这组门建造的. 图 4.9 是仅由 Hadamard、相位、受控非门和 $\pi/8$ 门组成的 Toffoli 门的一个线路.

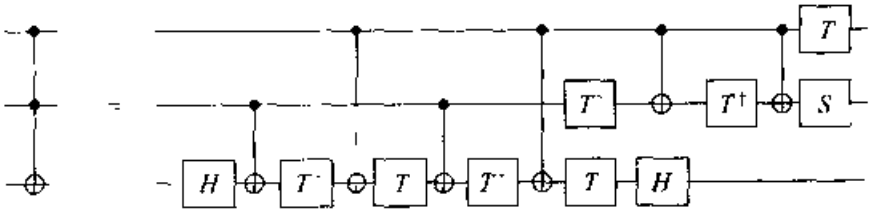


图 4.9　用 Hadamard、相位、受控非门和 $\pi/8$ 门实现的 Toffoli 门.

练习 4.24　验证图 4.9 实现了 Toffoli 门.

练习 4.25(Fredkin 门的构造)　回忆 Fredkin(受控交换，controlled-swap)门进行的运算

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.30}$$

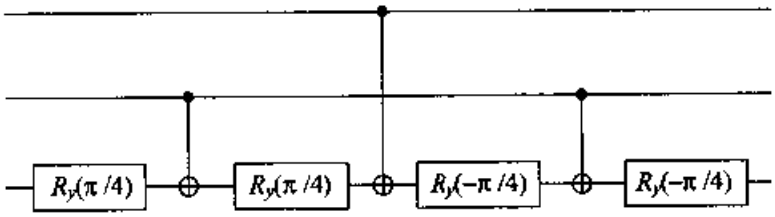
(1) 给出一个用三个 Toffoli 门构造的 Fredkin 门(提示：想想这个交换门的结构——可以每次控制一个门).

(2) 证明第一个和最后一个 Toffoli 门可以用受控非门代替.

(3) 用图 4.8 所示线路代替中间的 Toffoli 门,来得到仅用六个双量子比特门构造的 Fredkin 门.

(4) 有更简单的仅用五个双量子比特门的结构吗?

练习 4.26 证明如下线路



与 Toffoli 门的差别仅是相对相位. 即,该线路把$|c_1,c_2,t\rangle$变为$e^{i\delta(c_1,c_2,t)}|c_1,c_2,t\oplus c_1c_2\rangle$,其中$e^{i\delta(c_1,c_2,t)}$是某个相对相位因子. 这类门在实验实现中有时有用,它可以实现除了一个相对相位外与 Toffoli 门相同的门,但比直接实现 Toffoli 门容易得多.

练习 4.27 仅用受控非门和 Toffoli 门,来构造一个执行如下变换的量子线路.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{4.31}$$

这类部分循环置换(cyclic permutation)运算将在后面第 7 章用到.

如何利用已有的全部门对任意单量子比特酉运算 U 实现 $C^n(U)$门? 图 4.10 给出了一个能做到这一点的特别简单的线路. 这个线路分成三段,并使用不多的 $n-1$ 量子比特工作单元,它们的开始和结束都处在$|0\rangle$状态. 设控制量子比特处在计算基中的$|c_1,c_2,\cdots,c_n\rangle$状态. 线路的第一段是将控制位 $c_1,c_2,\cdots,c_n$以可逆方式"与"起来,得到乘积 $c_1c_2\cdots c_n$. 为此,线路中第一个门用一个 Toffoli 门把 c_1 和 c_2 "与"起来,把第一工作量子比特变为状态$|c_1c_2\rangle$,下一个 Toffoli 门把 c_3 和 c_1c_2 "与"起来,把第二工作量子比特的状态变为$|c_1c_2c_3\rangle$. 继续这样使用 Toffoli 门,直到最后工作量子比特处于状态$|c_1c_2\cdots c_n\rangle$. 第二段线路是,以最后工作量子比特被置 1 为条件,执行目标量子比特上的一个 U 运算,即当且仅当 c_1 到 c_n 都置位,应

用 U. 最后一部分线路只是逆转第一部分的步骤，把所有工作量子比特还原为它们的初态 $|0\rangle$. 于是组合起来的结果就是，当且仅当控制量子比特 c_1 到 c_n 都置位，把酉算子 U 应用到目标量子比特上. 正如所期望的.

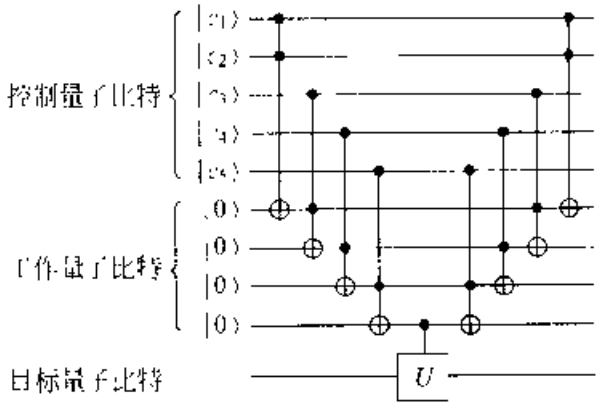


图 4.10　对 $n=5$ 实现 $C^n(U)$ 运算的网络.

练习 4.28　对 $U=V^2$，其中 V 是酉的，类似于图 4.10 构造 $C^3(U)$ 门，但不用工作量子比特，可以用受控 V 门和受控 $V^\dagger$ 门.

练习 4.29　不使用工作量子比特，求出一个包含 $O(n^2)$ Toffoli 门、受控非门和单量子比特门的可实现 $C^n(X)$ 门 $(n>3)$ 的线路.

练习 4.30　设 U 是一个单量子比特酉运算，不使用工作量子比特，求一个包含 $O(n^2)$ Toffoli 门、受控非门和单量子比特门，实现 $C^n(U)$ 门 $(n>3)$ 的线路.

我们所考虑的受控门中，条件动态发生在控制量子比特都置为 1 的情况. 当然 1 并没有任何特殊之处，考虑当控制位置为 0 条件发生的动态常常也是有用的. 例如，设希望实现当第一（控制）量子比特置为 0 条件下，第二（目标）量子比特翻转的双量子比特门，图 4.11 中我们为这个门引入一个线路符号和等价的用已知门构成的线路. 一般地，用空的圆圈符号表示一个量子比特被置为 0，而用实圆圈表示一个量子比特被置为 1.

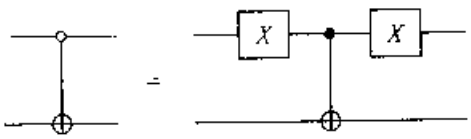


图 4.11　当第一量子比特为 0 时，在第二量子比特上进行的非门运算的受控操作.

图 4.12 给出了比这样约定的更进一步的，包含三个控制量子比特的例子. 运算 U 在第一和第三量子比特置为 0，第二量子比特置为 1 时，应用到目标量子比

特.通过考查右边的线路,容易验证它实现了期望的运算.更一般地,通过在适当位置插入 X 门,很容易在条件位置 1 和置 0 的线路之间转换,如图 4.12 所示.

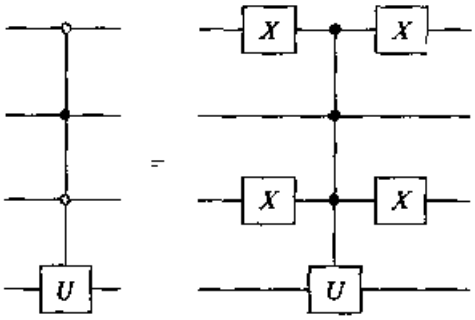


图 4.12 受控 U 运算及其等价的用我们已知如何完成基本运算的线路.在第一和第三量子比特置 0,第二量子比特置 1 条件下,第四量子比特应用 U.

有时会有用的另一约定是,允许受控非门具有多个目标量子比特,如图 4.13 所示.这个符号自然表示当控制量子比特为 1 时,其他所有标有⊕的量子比特都翻转,否则没有任何变化.我们会在第 10 章看到,它在构造置换等经典函数,在量子纠错线路的解码器或编码器中用起来很方便.

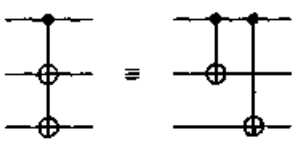


图 4.13 具有多目标量子比特的受控非门.

练习 4.31(更多的线路恒等式) 令下标表示算子作用的量子比特,并令 C 是量子比特 1 为控制、量子比特 2 为目标的受控非门,证明如下恒等式:

$$CX_1C = X_1X_2 \tag{4.32}$$

$$CY_1C = Y_1X_2 \tag{4.33}$$

$$CZ_1C = Z_1 \tag{4.34}$$

$$CX_2C = X_2 \tag{4.35}$$

$$CY_2C = Z_1Y_2 \tag{4.36}$$

$$CZ_2C = Z_1Z_2 \tag{4.37}$$

$$R_{z,1}(\theta)C = CR_{z,1}(\theta) \tag{4.38}$$

$$R_{z,2}(\theta)C = CR_{z,2}(\theta) \tag{4.39}$$

4.4 测 量

量子线路采用的最后一个元素就是测量,它有时是隐含的.在我们的线路中,用仪表符号表示计算基中(2.2.5 节)的投影测量,如图 4.14 所示.在量子线路的

理论中，习惯上不用特殊符号表示更一般的测量，因为如第 2 章所述，这些测量总可以由酉变换加上辅助量子比特，再连接投影测量表出.



图 4.14　单量子比特上投影测量的符号. 在这个线路中没有对测量结果的进一步运算，但在一般量子线路中可能会以前半部分的测量结果为条件，对后一半量子线路进行改变. 这样一个经典信息的使用以双线绘出(这里没画).

量子线路有两个重要的原理值得记住. 这两个原理都相当显然，然而，它们非常有用，值得尽早强调. 第一个原理是经典的条件运算可以用量子条件运算代替.

推迟测量原理(principle of deferred measurement)　总可以把测量从量子线路的中间步骤移到线路的末端；如果测量的结果被用子线路的某些阶段，则经典的条件运算可以被条件量子运算代替.

通常，量子测量在量子线路中作为一个中间步骤，并且测量结果被用作控制后续量子门的条件，例如图 1.13 的隐形传态线路就是这样. 不过，这些测量总可以移到线路的末端，图 4.15 说明了，如何通过用相应的量子条件运算代替所有经典条件运算来完成这一点(当然，对这个进行隐形传态的线路的部分解释将不适用，因为从 Alice 到 Bob 没有经典信息的传送，但明显地，两个量子线路的整体作用完全相同，这正是关键所在).

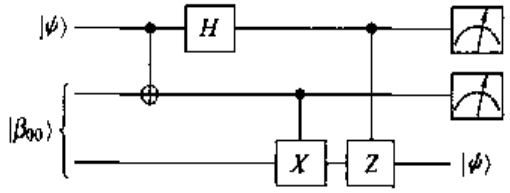


图 4.15　测量放在最后而不是在线路中间的量子隐形传态线路. 像图 1.13 那样，顶上两个量子比特属于 Alice，底下的一个属于 Bob.

第二个原理甚至更明显而且惊人地有用.

隐含测量原理(principle of implicit measurement)　不失一般性，量子线路中任何未终结的量子连线(未被测量的量子比特)总可以假设为被测量.

为什么这是对的？假想有一个仅包含两个量子比特的量子线路，并且只有第一量子比特在线路末端被测量，则这时观测得到的统计量完全由第一量子比特的约化密度矩阵决定. 然而，如果第二量子比特上也进行过测量，则该测量能够改变第一量子比特上测量的统计值，这将非常令人奇怪. 读者将在练习 4.32 中，通过证

明第一量子比特的约化密度矩阵不受第二量子比特上测量的影响，来证明这一点.

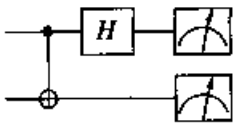
当读者认识到测量在量子线路中的角色时，记住它在量子和经典世界之间扮演的界面角色也是很重要的. 测量一般被视为一个不可逆运算，它毁掉了量子信息而代之以经典信息. 不过在一些仔细设计的情况下，这并不一定总是对的，隐形传态和量子纠错都生动地说明了这一情况. 隐形传态和量子纠错的共同之处在于，两种情况的测量都没有揭示量子状态的任何信息. 的确，第 10 章将看到这是测量的一个普遍的特点——为使一个测量是可逆的，它一定不能揭示被测量子状态的任何信息.

练习 4.32 设 ρ 是描述双量子系统的密度矩阵，假设在计算基中执行对第二量子比特的测量，令 $P_0 = |0\rangle\langle 0|$ 和 $P_1 = |1\rangle\langle 1|$ 分别是第二量子比特上到状态 $|0\rangle$ 和 $|1\rangle$ 的投影，令 ρ' 是测量后，由一个不了解测量结果的观测者分配给系统的密度矩阵. 证明

$$\rho' = P_0 \rho P_0 + P_1 \rho P_1 \tag{4.40}$$

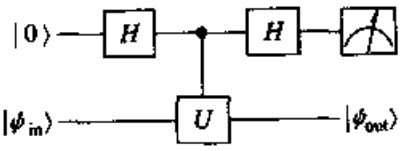
再证明第一量子比特的约化密度矩阵不受测量的影响，即 $\mathrm{tr}_2(\rho) = \mathrm{tr}_2(\rho')$.

练习 4.33(在 Bell 基中的测量) 我们对量子线路规定的测量模型，限于针对计算基，然而，我们常在其他标准正交状态组定义的基中执行测量. 为执行这样的测量，只需要从我们希望在其中进行测量的基酉变换到计算基，再进行测量. 例如，证明图

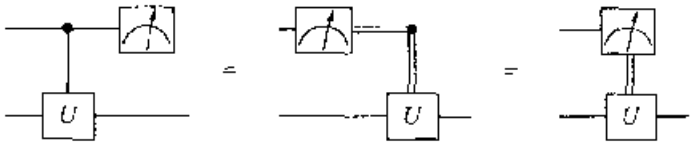


执行了在 Bell 态下的测量. 更精确地，证明这个线路导致相应的 POVM 元是到四个 Bell 态的投影的测量，并求出相应的测量算子是什么.

练习 4.34(测量一个算子) 设我们有一个具有特征值 ± 1 的单量子比特上的算子 U，于是 U 既是 Hermite 的又是酉的，故可以看作既是一个可观测量又是一个量子门. 假设我们希望测量可观测量 U，即我们希望获得指示两个特征值之一的测量结果，并将测量后的状态带到相应的特征向量. 用一个量子线路如何实现？证明下面的线路实现了 U 的一个测量.



练习 4.35(与控制可交换的测量) 推迟测量原理的一个结论是，当被测量量子比特是一个量子门的控制量子比特时，测量量子比特和量子门可以交换，即：



(在图中双线代表经典比特)证明第一个等式. 右边的等式只是为方便,测量结果以经典方式控制量子门的符号来表示.

4.5　通用量子门

如 3.1.2 节所看到的,一个门组成的小集合(如与、或、非)可以用来计算任意的经典函数,我们说这样一个门的集合对经典计算是通用的. 事实上,因为 Toffoli 门对经典计算是通用的,所以量子线路包含经典线路. 对量子计算有相应的通用性结果. 一组门称为是对量子计算是通用的,如果用这组门的量子线路可以以任意精度近似任意的酉运算. 现在描述量子计算的三个通用性构造步骤,这些可以层层推进,最后证明可用 Hadamard、相位、受控非门和 $\pi/8$ 门以任意精度近似任意酉运算. 读者也许会问为什么会出现相位门,因为它可以用两个 $\pi/8$ 门构造出来;原因是它在容错结构中的自然作用,将在第 10 章中描述.

第一个步骤显示任意酉算子可以精确地表为一些酉算子的乘积,其中每个酉算子的作用只在一个由两个计算基态张成的子空间上是不平凡的. 第二个步骤是把第一个步骤和酉算子结合起来,这酉算子如前一节所述,可以精确地用单量子比特门和受控非门表出. 第三个步骤包含第二个步骤与一个证明,即单量子比特运算可以用 Hadamard、相位和 $\pi/8$ 门以任意精度近似. 这也就蕴含任意酉运算可以被 Hadamard、相位、受控非门和 $\pi/8$ 门以任意精度近似.

上述构造过程几乎没有涉及效率问题——为产生一个给定的酉变换需要多少(多项式或指数数量的)门的问题. 4.5.4 节将证明存在酉变换需要指数量级的门来近似. 当然,量子计算的目的是寻找能有效进行有意义的酉变换的类.

练习 4.36　构造一个把双比特数 x 和 y 进行模 4 加的量子线路,即线路可以完成 $|x,y\rangle \mapsto |x,x+y \bmod 4\rangle$ 的变换.

4.5.1　两级酉门(two-level unitary gate)是通用的

考虑一个作用在 d 维 Hilbert 空间上的酉矩阵 U. 本节将说明怎样将 U 分解成两级酉矩阵的乘积,即只不平凡地作用在向量的一个或两个分量上的酉矩阵. 这个分解背后的本质思想可以从 U 是 3×3 矩阵的情况看出,设 U 具有形式

$$U=\begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix} \tag{4.41}$$

我们将找出两级酉矩阵 $U_1,\cdots,U_3$，使得

$$U_3U_2U_1U=I \tag{4.42}$$

于是

$$U=U_1^{\dagger}U_2^{\dagger}U_3^{\dagger} \tag{4.43}$$

其中 U_1，U_2 和 U_3 是两级酉矩阵，容易验证它们的逆 $U_1^{\dagger}$，$U_2^{\dagger}$ 和 $U_3^{\dagger}$ 也是两级酉矩阵. 因此如果能证明式(4.42)，则就说明了如何将 U 分解为两级酉矩阵的乘积. 用下述过程来构造 U_1：若 $b=0$，则置

$$U_1\equiv\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{4.44}$$

若 $b\neq 0$，则置

$$U_1\equiv\begin{bmatrix} \dfrac{a^*}{\sqrt{|a|^2+|b|^2}} & \dfrac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \dfrac{b}{\sqrt{|a|^2+|b|^2}} & \dfrac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{4.45}$$

注意两种情况下，U_1 均为一个两级酉矩阵，并且做乘法，得到

$$U_1U=\begin{bmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{bmatrix} \tag{4.46}$$

关键点在左边列的中间项是 0. 矩阵的其他项用加上“′”的符号表示，它们的实际值并不重要.

类似地，找出一个两级矩阵 U_2，使得 U_2U_1U 左下角的项为 0，即若 $c'=0$，则我们置

$$U_2\equiv\begin{bmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{4.47}$$

而若 $c'\neq 0$，则我们置

$$U_2\equiv\begin{bmatrix} \dfrac{a'^*}{\sqrt{|a'|^2+|c'|^2}} & 0 & \dfrac{c'^*}{\sqrt{|a'|^2+|c'|^2}} \\ 0 & 1 & 0 \\ \dfrac{c'}{\sqrt{|a'|^2+|c'|^2}} & 0 & \dfrac{-a'}{\sqrt{|a'|^2+|c'|^2}} \end{bmatrix} \tag{4.48}$$

两种情况下，做矩阵乘法都得到

$$U_2U_1U=\begin{bmatrix}1 & d'' & g''\\ 0 & e'' & h''\\ 0 & f'' & j''\end{bmatrix} \tag{4.49}$$

由于 U,U_1,U_2 是酉的，可导出 U_2U_1U 也是酉的，又因为 U_2U_1U 的第一行的模必须为 1，所以 $d''=g''=0$. 最后，置

$$U_3\equiv\begin{bmatrix}1 & 0 & 0\\ 0 & e''^* & f''^*\\ 0 & h''^* & j''^*\end{bmatrix} \tag{4.50}$$

容易验证 $U_3U_2U_1U=I$，于是 $U=U_1^\dagger U_2^\dagger U_3^\dagger$，是 U 的两级酉分解.

更一般地，设 U 作用在 d 维空间上. 则类似于 3×3 的情况，可以找到两级酉矩阵 $U_1,\cdots,U_{d-1}$，使得 $U_{d-1}U_{d-2}\cdots U_1U$ 左上角为 1，而第一列和第一行的其他元素均为 0. 接着对 $U_{d-1}U_{d-2}\cdots U_1U$ 的右下角的 $(d-1)\times(d-1)$ 子酉阵重复这个过程，依此类推，最后可把 $d\times d$ 酉矩阵写成

$$U=V_1\cdots V_k \tag{4.51}$$

其中矩阵 V_j 是两级矩阵，而 $k\leqslant(d-1)+(d-2)+\cdots+1=d(d-1)/2$.

练习 4.37　求变换

$$\frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & i & -1 & -i\\ 1 & -1 & 1 & -1\\ 1 & -i & -1 & i\end{bmatrix} \tag{4.52}$$

的一个两级酉矩阵分解. 这是量子 Fourier 变换的一个特例，下一章将作仔细研究.

上述结果的一个推论是，n 量子比特系统上的任意酉矩阵可以写成至多 $2^{n-1}(2^n-1)$ 个两级酉矩阵的乘积. 对特定的酉矩阵，找到有效得多的分解也是可能的，但如读者将要证明的，确实存在矩阵，它不能分解为少于 $d-1$ 个两级酉矩阵的乘积.

练习 4.38　证明存在 $d\times d$ 酉矩阵 U，它不能分解为少于 $d-1$ 个两级酉矩阵的乘积.

4.5.2　单量子比特门和受控非门是通用的

证明了 d 维 Hilbert 空间上的任意酉矩阵可以写成两级酉矩阵的乘积形式，现在来证明，单量子比特门和受控非门可以实现 n 量子比特状态空间上的任意两级酉运算. 这些结果合在一起就可以看到，单量子比特门和受控非门可以实现 n 量

子比特上的任意酉运算，于是它们对量子计算来说是通用的.

设 U 是一个 n 量子比特量子计算机上的两级酉矩阵. 特别地设 U 在计算机基态 $|s\rangle$ 和 $|t\rangle$ 张成的空间上的作用是不平凡的，其中 $s=s_1\cdots s_n$ 和 $t=t_1\cdots t_n$ 是 s 和 t 的二进制展开. 令 $\tilde{U}$ 是 U 的一个 2×2 的不平凡子酉阵，$\tilde{U}$ 可视为单量子比特上的酉算子.

现在的目标是基于单量子比特门和受控非门，构造一个实现 U 的线路. 为此，我们需要使用 Gray 码. 设有两个不同的二进制数 s 和 t. 连接 s 和 t 的一个 Gray 码是，以 s 开头以 t 结束的一组二进制数，使得相邻的数恰好有一位不同. 例如，对 $s=101001$ 和 $t=110011$，有 Gray 码

$$\begin{matrix}1&0&1&0&0&1\\1&0&1&0&1&1\\1&0&0&0&1&1\\1&1&0&0&1&1\end{matrix}\tag{4.53}$$

令 g_1 到 g_m 为连接 s 和 t 的 Gray 码的元，且 $g_1=s, g_m=t$. 注意总可以找到满足 $m\leqslant n+1$ 的 Gray 码，因为 s 和 t 最多有 n 个位置不同.

量子线路实现 U 的基本想法是通过一系列的门实现状态变换 $|g_1\rangle\rightarrow|g_2\rangle\rightarrow\cdots\rightarrow|g_{m-1}\rangle$，然后进行受控 $\tilde{U}$ 门运算，目标量子比特处在 g_{m-1} 和 g_m 不同的那一位，接着还原第一阶段的运算，进行变换 $|g_{m-1}\rangle\rightarrow|g_{m-2}\rangle\rightarrow\cdots\rightarrow|g_1\rangle$. 以上每个步骤用本章中前面提供的运算都很容易实现，最后的结果就是 U 的一个实现.

实现的更确切的描述如下. 第一步是交换 $|g_1\rangle$ 和 $|g_2\rangle$ 的状态. 设 $|g_1\rangle$ 和 $|g_2\rangle$ 的第 i 位值不同，则我们通过第 i 量子比特的一个受控比特翻转来完成交换，条件是 $|g_1\rangle$ 和 $|g_2\rangle$ 的其他位的量子比特都相同. 接下来用一个受控运算来交换 $|g_2\rangle$ 和 $|g_3\rangle$. 依此类推，直到交换了 $|g_{m-2}\rangle$ 和 $|g_{m-1}\rangle$. 这 $m-2$ 个运算的效果是完成如下运算

$$|g_1\rangle\rightarrow|g_{m-1}\rangle \tag{4.54}$$

$$|g_2\rangle\rightarrow|g_1\rangle \tag{4.55}$$

$$|g_3\rangle\rightarrow|g_2\rangle \tag{4.56}$$

$$\cdots\cdots$$

$$|g_{m-1}\rangle\rightarrow|g_{m-2}\rangle \tag{4.57}$$

计算基的所有其他状态在这一连串运算中都保持不变. 第二步，设 g_{m-1} 和 g_m 的第 j 位不同，在 g_{m-1} 和 g_m 其他位量子比特相同的条件下，进行以第 j 量子比特为目标的受控 $\tilde{U}$ 运算. 最后，用还原性的交换运算来完成 U 的运算：交换 $|g_{m-1}\rangle$ 和 $|g_{m-2}\rangle$，接着交换 $|g_{m-2}\rangle$ 和 $|g_{m-3}\rangle$，依此类推，直到交换 $|g_2\rangle$ 和 $|g_1\rangle$.

下面用一个例子进一步说明这个过程. 假设希望实现一个两级酉变换

$$U=\begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix} \tag{4.58}$$

这里 a,b,c 和 d 是使得 $\tilde{U}\equiv\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ 为酉矩阵的任意复数. 注意 U 的作用只在状态 $|000\rangle$ 和 $|111\rangle$ 上是不平凡的. 可写出连接 000 和 111 的 Gray 码：

$$\begin{matrix} A & B & C \\ 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{matrix} \tag{4.59}$$

从这里可以得出需要的电路，如图 4.16 所示. 前两个门对状态进行转换，把 $|000\rangle$ 与 $|011\rangle$ 交换. 接着运算 $\tilde{U}$ 以第二和第三量子比特是 $|11\rangle$ 为条件，应用到状态 $|011\rangle$ 和 $|111\rangle$ 的第一量子比特. 最后，还原状态，让状态 $|011\rangle$ 与 $|000\rangle$ 交换.

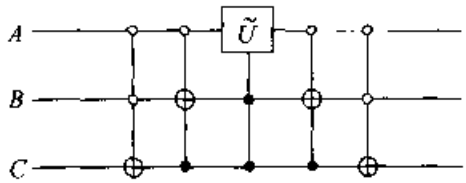


图 4.16　实现由式(4.58)定义的两级酉运算的线路.

回到一般情形，我们知道为实现两级酉运算 U 需要至多 $2(n-1)$ 个受控运算来交换 $|g_1\rangle$ 与 $|g_{m-1}\rangle$，然后再返回. 每个这样的受控运算可以用 $O(n)$ 个单量子比特和受控非门实现，受控 $\tilde{U}$ 也需要 $O(n)$ 个门. 因此，实现 U 需要 $O(n^2)$ 个单量子比特和受控非门. 在前一节看到，在 n 量子比特的 2^n 维状态空间上的任意酉矩阵可以写成 $O(2^{2n})=O(4^n)$ 个两级酉运算的乘积. 将这些结果合在一起，可知 n 量子比特上的任意酉运算可以用包含 $O(n^2 4^n)$ 个单量子比特门和受控非门的线路来实现. 显然，这个结构并没有导出非常有效的量子线路，然而，在 4.5.4 节将证明酉运算需要指数数目的门来实现，所以该结构接近最优. 于是，显然为寻找快速量子算法，必须采取与通用性结构不同的方法.

练习 4.39 求一个用单量子比特运算和受控非门的量子线路，实现变换

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{bmatrix} \tag{4.60}$$

其中 $\tilde{U} \equiv \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ 是任意的 2×2 酉矩阵.

4.5.3 通用运算的一个离散集合

前节证明了，受控非门和单量子比特酉运算一起构成量子计算的一个通用集合，但没有已知直接方法以抗噪声方式实现所有这些门. 幸运的是本节将找出一个门的离散集合来执行通用量子计算，并且第 10 章将证明，如何利用量子纠错码以抗差错方式执行这些门的运算.

1. 酉算子的近似

显然，门的一个离散集合不可能精确实现任意的酉运算，因为酉运算的集合是连续的. 然而，可以用一个离散集合去近似任意的酉运算. 为明白这是怎样进行的，首先需要研究近似酉运算意味着什么. 设 U 和 V 是在同一状态空间上的两个酉算子，U 是希望实现的目标酉算子，而 V 是实际中实现的一个酉算子. 定义当用 V 实现 U 时的误差为

$$E(U,V) \equiv \max_{|\psi\rangle} || (U-V)|\psi\rangle || \tag{4.61}$$

其中最大运算取遍状态空间中所有归一化量子状态 $|\psi\rangle$. 盒子 4.1 中证明这个误差的度量具有如下解释：如果 $E(U,V)$ 小，则对任意初态 $|\psi\rangle$，在状态 $V|\psi\rangle$ 上进行的测量将给出对 $U|\psi\rangle$ 的测量近似的测量统计值. 更确切地，我们证明如果 M 是任意 POVM 中的一个 POVM 元，且 P_U（或 P_V）是得到这个输出结果的概率，如果 U（或 V）应用到开始状态 $|\psi\rangle$，则

$$|P_U - P_V| \leqslant 2E(U,V) \tag{4.62}$$

因此如果 $E(U,V)$ 小，则不管进行 U 或 V 运算，测量结果均以相似概率出现. 盒子 4.1 中也证明，如果执行一系列的门运算 $V_1,\cdots,V_m$ 来近似另外一系列门 $U_1,\cdots,U_m$，则误差至多以线性相加，即

$$E(U_m U_{m-1}\cdots U_1, V_m V_{m-1}\cdots V_1) \leqslant \sum_{j=1}^{m} E(U_j,V_j) \tag{4.63}$$

式(4.62)和式(4.63)的近似结果极为有用. 假设希望完成一个包含 m 个门 U_1 到 U_m 的量子线路，不幸的是，只能用门 V_j 去近似门 U_j. 为了使从近似线路得

到的输出结果在正确概率的一个容许量 $\Delta>0$ 之内，根据式(4.62)和式(4.63)的结果，只要保证 $E(U_j,V_j)\leqslant\Delta/(2m)$ 就可以了.

2. Hadamard 门＋相位门＋受控非门＋π/8 门的通用性

我们现在有了很好的基础来研究用门的离散集合来近似任意的酉运算. 考虑门的两个不同的离散集合，它们都是通用的. 第一个集合，通用门的标准集合，由 Hadamard 门、相位门、受控非门、π/8 门组成. 在第 10 章将为这些门提供容错设计，这些设计也提供异常简单的通用结构. 第二个集合是 Hadamard 门、相位门、受控非门和 Toffoli 门. 这些门也都可采用容错结构，不过，这些门的通用性证明和容错设计有点不太吸引人.

盒子 4.1　近似量子线路

设一个量子系统的初态是 $|\psi\rangle$，并设我们要么进行酉运算 U，要么进行酉运算 V. 接着进行测量. 令 M 是一个与测量相联系的 POVM 元，且令 P_U(或 P_V)是进行运算 U(或 V)获得相应输出结果的概率，则

$$|P_U-P_V|=|\langle\psi|U^\dagger MU|\psi\rangle-\langle\psi|V^\dagger MV|\psi\rangle| \tag{4.64}$$

令 $|\Delta\rangle\equiv(U-V)|\psi\rangle$，利用简单的代数计算和 Cauchy-Schwarz 不等式，可得

$$|P_U-P_V|=|\langle\psi|U^\dagger M|\Delta\rangle+\langle\Delta|MV|\psi\rangle| \tag{4.65}$$

$$\leqslant|\langle\psi|U^\dagger M|\Delta\rangle|+|\langle\Delta|MV|\psi\rangle| \tag{4.66}$$

$$\leqslant||\Delta\rangle||+||\Delta\rangle|| \tag{4.67}$$

$$\leqslant 2E(U,V) \tag{4.68}$$

不等式 $|P_U-P_V|\leqslant 2E(U,V)$ 定量地表示了，当误差 $E(U,V)$ 小时，测量输出的结果的差别也小.

假设用门的一个序列 $V_1,V_2,\cdots,V_m$ 来近似某个门的另外一个序列 $U_1,U_2,\cdots,U_m$，则事实上，整个不精确门的序列引起的误差最多是单个门误差的和，即

$$E(U_mU_{m-1}\cdots U_1,V_mV_{m-1}\cdots V_1)\leqslant\sum_{j=1}^{m}E(U_j,V_j) \tag{4.69}$$

为证明这一点，我们从 $m=2$ 的情况开始. 注意对某个状态 $|\psi\rangle$ 有

$$E(U_2U_1,V_2V_1)=||(U_2U_1-V_2V_1)|\psi\rangle|| \tag{4.70}$$

$$=||(U_2U_1-V_2U_1)|\psi\rangle-(V_2U_1-V_2V_1)|\psi\rangle|| \tag{4.71}$$

利用三角不等式 $||a\rangle+|b\rangle||\leqslant||a\rangle||+||b\rangle||$，得到

$$E(U_2U_1,V_2V_1)\leqslant||(U_2-V_2)U_1|\psi\rangle||+||V_2(U_1-V_1)|\psi\rangle|| \tag{4.72}$$

$$\leqslant E(U_2,V_2)+E(U_1,V_1) \tag{4.73}$$

正如所期望的. 对 m 的一般情况可以从归纳法得到.

通用性的证明可以从如下开始，Hadamard 门和 $\pi/8$ 门可以用来以任意精度近似任意单量子比特酉运算. 考虑 T 门和 HTH 门，T 除了一个不要紧的全局相位，和一个 Bloch 球面上绕 $\hat{z}$ 轴的 $\pi/4$ 弧度旋转相当，而 HTH 是一个 Bloch 球面上绕 $\hat{x}$ 的 $\pi/4$ 弧度旋转相当(练习 4.14). 这两个运算组合起来，除了一个全局相位，得到

$$\exp\left(-\mathrm{i}\frac{\pi}{8}Z\right)\exp\left(-\mathrm{i}\frac{\pi}{8}X\right)=\left[\cos\frac{\pi}{8}I-\mathrm{i}\sin\frac{\pi}{8}Z\right]\left[\cos\frac{\pi}{8}I-\mathrm{i}\sin\frac{\pi}{8}X\right] \tag{4.74}$$

$$=\cos^2\frac{\pi}{8}I-\mathrm{i}\left[\cos\frac{\pi}{8}(X+Z)+\sin\frac{\pi}{8}Y\right]\sin\frac{\pi}{8} \tag{4.75}$$

这是一个 Bloch 球面绕单位向量 $\hat{n}$，转过 θ 角的一个旋转，其中 $\hat{n}$ 与 $n=\left(\cos\frac{\pi}{8},\sin\frac{\pi}{8},\cos\frac{\pi\mathrm{i}}{8}\right)$ 对应，θ 由 $\cos(\theta/2)\equiv\cos^2\frac{\pi}{8}$ 定义，即仅利用 Hadamard 门和 $\frac{\pi}{8}$ 门可以构造出 $R_{\hat{n}}(\theta)$. 进而可证明这个 θ 是 2π 的无理倍数. 证明这后一个事实超出了我们的讨论范围，参看“历史和进一步阅读的材料”.

下面证明反复迭代 $R_{\hat{n}}(\theta)$ 可以以任意精度近似任意旋转 $R_{\hat{n}}(\alpha)$. 为此，令 $\delta>0$ 是希望的精度，且令 N 是一个比 $2\pi/\delta$ 大的整数. 定义 θ_k，使得 $\theta_k\in[0,2\pi)$，且 $\theta_k=(k\theta)\bmod 2\pi$. 于是鸽笼原理蕴含，在 $1,\cdots,N$ 范围内存在不同的 j 和 k，使得 $|\theta_k-\theta_j|\leqslant 2\pi/N<\delta$. 不失一般性假设 $k>j$，于是我们有 $|\theta_{k-j}|<\delta$. 因为 $j\neq k$ 且 θ 是 2π 的无理倍数，必有 $\theta_{k-j}\neq 0$. 可知当 l 变化时，$\theta_{l(k-j)}$ 可填满区间 $[0,2\pi)$，所以序列中相邻的数的距离不超过 δ. 因此可导出对任意的 $\epsilon>0$，存在 n，使得

$$E(R_{\hat{n}}(\alpha),R_{\hat{n}}(\theta)^n)<\frac{\epsilon}{3} \tag{4.76}$$

练习 4.40 对任意的 α 和 β，证明

$$E(R_{\hat{n}}(\alpha),R_{\hat{n}}(\alpha+\beta))=|1-\exp(\mathrm{i}\beta/2)| \tag{4.77}$$

并以此论证式(4.76).

现在可以来论证任意的单量子比特运算，可以用 Hadamard 门和 $\pi/8$ 门以任意精度近似. 简单的代数计算表明，对任意的 α

$$HR_{\hat{n}}(\alpha)H=R_{\hat{m}}(\alpha) \tag{4.78}$$

其中 $\hat{m}$ 是 $\left(\cos\frac{\pi}{8},-\sin\frac{\pi}{8},\cos\frac{\pi}{8}\right)$ 方向上的单位向量，因此

$$E(R_{\hat{m}}(\alpha),R_{\hat{m}}(\theta)^n)<\frac{\epsilon}{3} \tag{4.79}$$

但由练习 4.11，除了一个不要紧的全局相移，单量子比特上的任意酉运算 U 可以写成

$$U=R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta) \tag{4.80}$$

于是结果式(4.76)和式(4.79)以及式(4.63)中的不等式链蕴含对适当的正整数 n_1、n_2、n_3，有

$$E(U, R_{\hat{x}}(\theta)^{n_1} HR_{\hat{n}}(\theta)^{n_2} HR_{\hat{n}}(\theta)^{n_3}) < \varepsilon \tag{4.81}$$

即对于给定的任意单量子比特酉算子 U 和任意的 $\varepsilon > 0$，可以用一个只由 Hadamard 门和 $\pi/8$ 门组成的量子线路在 ε 范围内近似.

因为 $\pi/8$ 门和 Hadamard 门可使我们近似任意的单量子比特酉算子，故从 4.5.2 节的论证可知，可以按如下方式近似任意的 m 门量子线路. 给定一个包含 m 个受控非或单量子比特酉门的量子线路，可以用 Hadamard 门、受控非门和 $\pi/8$ 门(以后我们看到相位门使容错近似成为可能，但对当前的通用性论证，它们不是严格必要的). 如果希望对整个线路具有 ε 精度，可以通过用上述近似，对每个单量子比特酉算子在精度 ε/m 内近似，利用式(4.63)不等式链获得整体线路的 ε 精度.

这个利用一组离散门近似量子线路的过程的效率如何？这是个重要的问题. 例如假设近似一个任意的单量子比特酉算子到 ε 距离，需要离散集合中的 $\Omega(2^{1/\varepsilon})$ 个门，那么近似上一段考虑的 m 门量子线路就需要 $\Omega(m2^{m/\varepsilon})$ 个门，随原线路规模呈指数增长. 幸运的是，收敛速率比这要好得多. 从直观上看，可以认为 θ_i 或多或少以一种一致的方式填充区间 $[0, 2\pi)$，于是近似任意单量子比特门应该大约用离散集合中 $\Theta(1/\varepsilon)$ 个门. 如果我们用这个数来估计近似任意单量子比特门需要的门的数目，则近似 m 门量子线路到 ε 精度，需要的门数将是 $\Theta(m^c/\varepsilon)$. 这个数目随原线路的规模二次增长，对许多应用来说是够了.

不过相当引人瞩目的是，可以证明有快得多的收敛速率. 附录 C 中证明的 Solovay-Kitaev 定理蕴含，任意单量子比特门可以用离散集合中的 $O(\log^c(1/\varepsilon))$ 个门近似到 ε 精度，其中 c 是接近于 2 的常数. 于是 Solovay-Kitaev 定理蕴含，要在 ε 精度内近似一个包含 m 个受控非门和单量子比特酉门的线路，需要离散集合中 $O(m\log^c(m/\varepsilon))$ 个门. 这个数目随原线路规模多重对数增长，实际上对所有应用大概都是可以接受的.

总之，我们证明了在只用一组离散门就能够有好的精度来模拟一个给定的线路，此线路包含受控非和任意单量子比特酉门，在此意义下，Hadamard 门、相位门、受控非门和 $\pi/8$ 门对量子计算是通用的. 而且，在仿真需要增加的资源对 $\log(m/\varepsilon)$ 是多项式的意义下，仿真是有效的，其中，m 是原线路中的门数，ε 是仿真的期望精度.

练习 4.41　本练习和下两个练习通过构造证明 Hadamard 门、相位门、受控非门和 Toffoli 门是通用的. 证明图 4.17 所示线路在两个测量输出都是 0 时，把 $R_z(\theta)$ 运算应用到第三(目标)量子比特，其中 $\cos\theta = 3/5$，否则把 Z 应用到目标量子比特. 证明两个测量结果都是 0 的概率是 5/8，并说明如何反复使用该线路和 $Z = S^2$ 门，来让应用 $R_z(\theta)$ 门的概率接近 1.

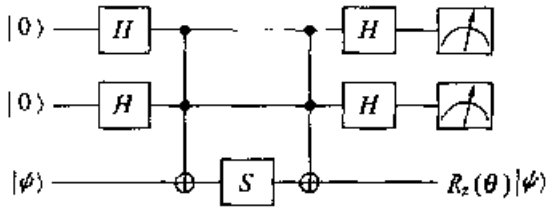


图 4.17 设两个测量结果都是 0，则这个电路把 $R_z(\theta)$ 应用到目标，其中 $\cos\theta = 3/5$. 如果是其他测量结果，则把 Z 应用到目标.

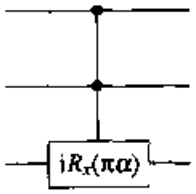
练习 4.42(θ 的无理性) 设 $\cos\theta = 3/5$，我们用反证法证明 θ 是 2π 的无理倍数.

(1) 利用 $e^{i\theta} = (3+4i)/5$ 的事实，证明若 θ 是有理的，则必存在一个正整数 m，使得 $(3+4i)^m = 5^m$.

(2) 证明对所有 $m>0$，$(3+4i)^m = 3+4i \bmod 5$，并得出不存在 m，使得 $(3+4i)^m = 5^m$ 的结论.

练习 4.43 利用上两个练习的结果证明，Hadamard 门、相位门、受控非门和 Toffoli 门对量子计算是通用的.

练习 4.44 证明只要 α 是无理的，如下定义的三量子比特门对量子计算就是通用的.



练习 4.45 设 U 是用 H，S，受控非门和 Toffoli 门构造的一个 n 量子比特量子线路. 证明 U 具有形式 $2^{-k/2}M$，其中 k 是某个整数，M 是只有复整数元的 $2^n \times 2^n$ 矩阵. 对以 $\pi/8$ 门代替 Toffoli 门的情形，重复本练习.

4.5.4 近似任意酉门一般是难的

我们看到 n 量子比特上的酉变换可以由一小组基本门构造，这样做总是有效的吗？即给定 n 量子比特上的酉变换 U，是否存在 n 多项式规模的线路来近似 U？这个问题的答案是否定的：事实上，大多数酉变换不是很有效. 理解这一点的一个途径是考虑如下问题：需要多少门来产生 n 量子比特的任意状态？简单的计数论证显示这一般需要指数量级的运算，于是立即可知酉运算需要指数量级的运算. 为验证这一点，设有 g 类不同的门，每个门至多有 f 个输入量子比特. 这两个数 f 和 g 是计算硬件所定的，可视为常数. 设有一个包含 m 个门的量子线路，初态为计算

基态$|0\rangle^{\otimes n}$，对线路中的任一特定门，共有至多$\binom{n}{f}=O(n^q)$种可能，因此可推知用m门至多计算出$O(n^{mq})$个不同的状态。

设我们希望以距离ε近似一个特殊状态$|\psi\rangle$。证明的思路是用一组半径均为ε的小块来覆盖所有可能状态的集合(图4.18)，并证明需要的块数随n双指数增长，与m个门能够计算的不同状态的指数数目比较，就可以得出结论。需要注意的第一事实是，n量子比特状态向量的空间可以视为就是单位$(2^{n+1}-1)$球。为验证这一点，设n量子比特具有幅度$\psi_j=X_j+iY_j$，其中X_j和Y_j分别是第j个幅度的实部和虚部。量子状态的归一化条件可以写成$\sum_j(X_j^2+Y_j^2)=1$，这正是一个点在2^{n+1}维实空间单位球面的条件，即单位$(2^{n+1}-1)$球。类似地，$|\psi\rangle$附近半径为ε的表面积，近似与半径为ε的$(2^{n+1}-2)$球的体积相等。利用对半径为r的k-球的表面积公式$S_k(r)=2\pi^{(k+1)/2}r^k/\Gamma((k+1)/2)$和对半径为$r$的$k$-球的体积$V_k(r)=2\pi^{(k+1)/2}r^{k+1}/[(k+1)\Gamma((k+1)/2)]$，我们看到需要覆盖状态空间的块数为

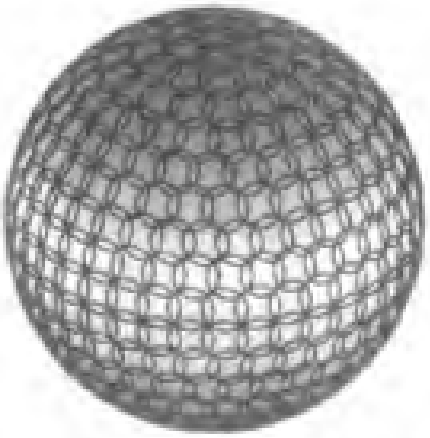


图4.18 用固定半径的小块覆盖所有可能状态。

$$\frac{S_{2^{n+1}-1}(1)}{V_{2^{n+1}-2}(\varepsilon)}=\frac{\sqrt{\pi}\,\Gamma\left(2^n-\frac{1}{2}\right)(2^{n+1}-1)}{\Gamma(2^n)\varepsilon^{2^{n+1}-2}} \tag{4.82}$$

其中Γ是阶乘函数的常用推广，但因为$\Gamma(2^n-1/2)\geqslant\Gamma(2^n)/2^n$，于是覆盖空间的块数至少为

$$\Omega\left(\frac{1}{\varepsilon^{2^{n+1}-2}}\right) \tag{4.83}$$

回忆m个门可以达到的块数为$O(n^{6m})$，于是为达到所有的ε小块，必须要有

$$O(n^{6m})\geqslant\Omega\left(\frac{1}{\varepsilon^{2^{n+1}-2}}\right) \tag{4.84}$$

所以

$$m=\Omega\left(\frac{2^n\log(1/\varepsilon)}{\log(n)}\right) \tag{4.85}$$

即，存在n量子比特的一组状态，需要$\Omega(2^n\log(1/\varepsilon)/\log(n))$次运算近似到距离$\varepsilon$以内。这对$n$来说是指数的，因此在第3章引入的计算机复杂性的意义下，这是"难"的。进而这直接意味着存在n量子比特上的酉变换U，需要一个用$\Omega(2^n\log(1/\varepsilon)/\log(n))$个运算的线路来近似，该线路实现运算$V$，使得$E(U,V)\leqslant\varepsilon$。

与之对照，利用通用结构和 Solovay-Kitaev 定理可知，n 量子比特上的任意酉运算可以用 $O(n^2\,4^n\log^c(n^2\,4^n/\varepsilon))$ 个门近似到 ε 距离. 因此，在结构的多项式因子范围内，我们给出的构造是最优的，但不幸的是，它没有解决确定哪类酉运算，可在量子线路模型中可有效地计算的问题.

4.5.5 量子计算复杂性

第 3 章描述了经典计算机上的计算复杂性理论，它对解计算问题的资源需求进行分类. 不奇怪，人们对发展量子计算复杂性理论，并且把它和经典计算复杂性理论联系起来有浓厚的兴趣. 尽管这个方向还非常初步，不过对未来的研究者来说，这无疑将是一个成果极其丰富的方向. 我们只限于表述量子复杂性类的一个结果，它把量子复杂性 BQP 类和经典的 PSPACE 类联系起来. 这里对这一结果的讨论相当不正规，更多的细节请参考本章末“历史和进一步阅读的材料”引用的 Bernstein 和 Vazirani 的论文.

回忆第 3 章 PSPACE 类定义，为 Turing 机上用多项式空间规模和任意长时间可解的判定问题类. BQP 类实质上是量子复杂性类，由多项式规模量子线路内的，并且误差在有界概率内的可解的判定问题组成. 稍微正式一点看，我们说一个语言 L 属于 BQP 类，如果存在一族多项式规模的量子线路来判定该语言，且判定过程为，以至少 3/4 概率接受该语言中的串，以至少 3/4 概率拒绝不在该语言中的串. 在实践中，这意味着量子线路以二进制串为输入，并且试图决定它们是否是语言的元素. 在线路的末端，测量一个量子比特，用 0 指示串接受，用 1 指示拒绝. 通过对串进行几次测试，就可以判定它是否在 L 中. 我们可以有很高的概率判定一个给定串是否在 L 中.

当然，一个量子线路是一个固定的实体，并且任意给定的量子线路只能判定 L 中的某个有限长度的串. 出于这个原因，BQP 类的定义中采用了一个线路族，对每个可能的长度，在线路族中有一个不同的线路. 我们在已描述的接受/拒绝准则的基础上，再增加两条限制. 首先，线路的规模只能随输入串 x 的大小以多项式方式增大，对于 x 我们试图判定是否有 $x\in L$. 其次，要求在类似于 3.1.2 节描述的意义下，线路是一致生成的. 这个一致性要求提出的原因是，在实践中，给定某个长度 n 的输入串 x，人们必须构造出能够判定 x 是否在 L 中的一个量子线路. 为此就需要一组确切的指令——一个算法——来建造线路. 因此，要求量子线路是一致生成的，即存在一个 Turing 机，它可以有效输出量子线路的一个描述. 这个限制看起来是相当技术性的，并且在实践中几乎总是得到满足的，但它确实使我们避免了像 3.1.2 节中那样的佯谬(读者也许会问，在一致性要求中采用的是量子 Turing 机，还是经典 Turing 机，是否要紧，事实上没有关系——参看“历史和进一步阅读的材料”).

量子计算复杂性类中最重要的结果之一是，$\mathrm{BQP}\subseteq\mathrm{PSPACE}$. 显然

BPP⊆BQP，其中 BPP 类是在经典Turing 机上，以有界误差概率，在多项式时间可解判定问题的经典复杂性类. 因此我们有包含链 BPP⊆ BQP⊆ PSPACE. 证明 BQP≠BPP——显然这将意味着量子计算机比经典计算机更强大——将缠含 BPP≠PSPACE. 然而，目前尚不清楚是否有 BPP≠PSPACE，证明这一点将是计算机科学中的一大突破. 于是证明量子计算机比经典计算机更强大，对经典的计算复杂性将有非常重要的价值，不幸的是，这也意味着提供这样一个证明可能相当困难.

为什么 BQP⊆PSPACE 是对的？下面是证明的直观概述(关于严格的证明请参看“历史和进一步阅读的材料”). 设有一台 n 量子比特量子计算机，并且进行一项包含 $p(n)$个门的计算，其中 $p(n)$是 n 的多项式. 设量子线路初始状态为$|0\rangle$. 我们将说明，如何在一台经典计算机上得到用多项式空间来计算它最终处于状态 $|y\rangle$的概率. 设在量子计算机上执行的门运算依次为 $U_1, U_2, \cdots, U_{p(n)}$，则最终处于状态$|y\rangle$的概率为

$$\langle y \mid U_{p(n)} \cdots U_2 U_1 \mid 0 \rangle \tag{4.86}$$

的模 平方，这个量在经典计算机上可以用多项式空间估计. 基本的思路是在式(4.86) 的每一项中插入完备性关系 $\sum_x |x\rangle\langle x| = I$，得 到

$$\begin{aligned}\langle y \mid U_{p(n)} \cdots U_2 U_1 \mid 0 \rangle = \sum_{x_1, \cdots, x_{p(n)-1}} & \langle y \mid U_{p(n)} \mid x_{p(n)-1} \rangle \langle x_{p(n)-1} \mid \\ & \times U_{p(n)-1} \cdots U_2 \mid x_1 \rangle \langle x_1 \mid U_1 \mid 0 \rangle\end{aligned} \tag{4.87}$$

已知出现在这个和中的每个西门都是诸如 Hadamard 门、受控非门等，显然，和中的每项可以在经典计算机上仅用多项式空间计算就能得到高精度. 因此这个和整体上可以用多项式空间计算，因为和的每一项可以在加完后被擦除. 当然，这个算法相当慢，因为和中包含的指数量级的项需要分别计算并且加起来，不过，仅消耗了多项式规模的空间，因此 BQP⊆ PSPACE.

可用类似的过程在经典计算机上模拟任意的量子计算，而不管量子计算的长度. 因此，不限时间和空间时，量子计算机可解的问题类不超过经典计算机可解的问题类. 换个说法，这意味着量子计算机不违反 Church-Turing 论题，即任意算法过程可用 Turing 机模拟. 当然，量子计算机可能比经典计算机有效得多，因此概率 Turing 机有效模拟任意算法过程，对强 Church-Turing 论题构成了挑战.

4.6　计算的量子线路模型的总结

本书中“量子计算机”一词与计算的量子线路模型是同义词. 本章详细阐述了量子线路、它们的基本要素、通用类的门以及一些应用. 在讨论更复杂的应用之前，让我们总结一些计算的量子线路模型的一些关键要素.

(1) 经典资源. 量子计算机包括两部分,经典部分和量子部分. 原则上,计算机不需要经典部分,但实践中如果允许部分计算以经典方式进行,某些任务的完成将容易得多. 例如,许多量子纠错方案(第 10 章)为使效率最高,可能会涉及经典计算. 尽管原则上经典计算总可以在一台量子计算机上进行,不过在经典计算机上进行会更方便些.

(2) 适当的状态空间. 量子线路在某个数目为 n 的量子比特组上进行操作,因此状态空间是 2^n 维复 Hilbert 空间. 积形式 $|x_1,\cdots,x_n\rangle$,其中 $x_i=0,1$ 的状态称为计算机的计算基态. $|x\rangle$ 表示一个计算基态,其中 x 是二进制表示为 $x_1\cdots x_n$ 的数.

(3) 将状态置子计算基中的能力. 假设任何的计算基态 $|x_1\cdots x_n\rangle$ 可以在至多 n 步内制备出来.

(4) 进行量子门运算的能力. 门可以随意应用到量子比特的任意子集,并且可以实现一组通用门. 例如,在量子计算机上可以把受控非门用到任何一对量子比特上. Hadamard 门、相位门、受控非门和 $\pi/8$ 门构成一组可以近似任意酉运算的门,因此是一组通用门. 还存在其他的通用类.

(5) 在计算基中测量的能力. 计算机中可以进行在计算基中的一个或多个量子比特的测量.

在同样的问题要求同样资源的意义下,量子计算的量子线路模型等价于历史上提出过的许多计算模型. 作为说明基本思想的简单例子,人们可能会问,基子三级量子系统进行设计,而不是基于两级量子系统,是否能带来什么计算上的好处. 当然,虽然用三级量子系统(qutrit)可能会比两级系统略微有些优点,但是它们的任何差别从理论角度看都是可以忽略的. 更不明显的例子是计算的量子 Turing 机模型,即经典 Turing 机的量子推广,业已证明它等价于基于量子线路的模型. 本书不考虑那个计算模型,但有兴趣更多地学习量子 Turing 机的读者,可以参考本章末的"历史和进一步阅读的材料".

尽管量子线路模型具有简单性,也很吸引人,但了解对它可能的批评、修改和扩充是有用的. 例如,量子线路关子状态空间和初始条件的基本假设的合理性,无论如何不是显然的. 到目前为止,一切都是针对有限维状态空间表述的. 使用无穷维状态空间会带来好处吗? 假设计算机的初态不是必须为一个计算基态,我们知道自然中的许多系统"更愿意"处于许多系统的高度纠缠状态. 可以利用这种偏好获得额外的计算能力吗? 如果能让某些特定计算访问特定状态,或许比从计算基态开始容易得多. 同样道理,在多重量子比特基中进行有效纠缠测量的能力,或许和进行纠缠酉运算一样有用. 的确,有可能利用这种测量,来完成在量子线路模型中不可解的任务.

量子线路模型的物理学基础的详细考察和论证合理性的尝试,超出了现在的

讨论范围，而且事实上超出了已知的范围. 通过提出这些问题，我们希望引人量子线路模型的完备性问题，并且再次强调信息是物理性的基本观点. 在建立信息处理模型的尝试中，我们总是企图回到基本的物理定律. 就本书而言，我们的讨论将限于计算的量子线路模型，它提供了内容丰富且非常有力的计算模型，即利用量子力学性质，来完成没有经典先例的惊人的信息处理任务. 是否存在超过量子线路模型的物理上合理的计算模型，是一个令人着迷的尚未解决的问题.

4.7 量子系统的仿真

也许……我们需要一套关于量子自动机的理论. ……量子状态空间的容量远大于经典状态空间：相对于一个具有 N 状态的经典系统，其量子版本允许容纳 c^N 个状态. 两个经典系合起来的状态数是 N_1 与 N_2 的乘积，而在量子情形却是指数增长 $c^{N_1 N_2}$. ……这些粗略估计表明，系统的量子行为可能比其经典仿真复杂得多.

——*Yu Manin (1980)*[Man80]，*见文献[Man99]中的英文译文*

一个甲烷分子的量子力学计算需要 10^{42} 个格点. 假使在每个点上只进行 10 次基本运算，并且计算在极低的 $T=3\times10^{-3}$K 温度下进行，我们仍需要用 19 世纪全球所生产的能量.

——*R. P. Poplavskii (1975)*[Pop75] *Manin 的引文*

物理学能够被通用计算机模拟吗？……物理世界服从量子力学，因此正确的问题是量子物理学的仿真……对一个包含 R 个粒子大系统的完整量子力学描述需要太多的变量，用具有与 R 成比例的元件数的普通计算机模拟这样的系统是不可能的……但可以用量子计算机元件模拟. 量子系统能够被经典通用(假设是概率型)计算机在概率意义下模拟吗？……如果计算机是我们到目前为止所描述的经典类型……答案无疑是否定的.

——*Richard P. Feynman(1982)*[Fey82]

让我们用量子线路模型的一个有趣和有用的应用来结束本章. 计算的最重要的实际应用的例子之一是物理系统的仿真. 例如，一个新建筑的工程设计中，有限元分析和建模被用于保证安全，同时使费用最小化. 汽车借助计算机辅助设计，可以制造得重量轻，结构优良，外形吸引人，价格不贵. 现代航空学工程非常依赖对飞机设计的计算流体力学仿真. 核武器不再试爆(对大部分地区)，而彻底由计算建模进行测试. 这样的例子很多，因为预测性的仿真有极宽的实际应用范围. 我们从仿真问题的一些例子开始，接着给出仿真的量子算法和一个说明性的例子，最后以这

一应用的前景展望作结束.

4.7.1 仿真原理

仿真的本质在于,得到刻画统治系统动态行为的物理定律的微分方程解.可举出一些例子,这里只列出很少的几个,如 Newton 定律

$$\frac{\mathrm{d}}{\mathrm{d}t}\left(m\frac{\mathrm{d}x}{\mathrm{d}t}\right)=F \tag{4.88}$$

Poisson 方程

$$-\nabla\cdot(k\nabla u)=Q \tag{4.89}$$

电磁向量波动方程

$$\nabla\cdot\nabla E=\epsilon_0\mu_0\frac{\partial^2 E}{\partial t^2} \tag{4.90}$$

和扩散方程

$$\nabla^2\psi=\frac{1}{a^2}\frac{\partial\psi}{\partial t} \tag{4.91}$$

仿真的目标相当普遍:给定系统的初始状态,在某个时间/位置时,它是什么状态?解常常是通过用一个数字表示近似状态,然后对微分方程进行空间和时间上的离散化,使得某个过程的承载着从开始到终了的状态信息迭代而得到.重要之处在于,这个过程的误差是有界的,并且增长的速率不会超过迭代次数的一个小的方次.但是,并不是所有动态系统都可以有效地模拟:一般只有能被有效表示的系统可以被有效模拟.

用经典计算机模拟量子系统是可能的,但一般而言不是很有效.许多简单量子系统的动态行为服从 Schrödinger 方程

$$\mathrm{i}\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\psi\rangle=H|\psi\rangle \tag{4.92}$$

我们将看到把 $\hbar$ 放入 H 中是方便的,本节剩下的内容将使用这个约定.对于一个研究空间中实际粒子(而不是我们所研究的像量子比特那样的抽象系统)的物理学家感兴趣的典型 Hamilton 量,这个方程可简化为

$$\mathrm{i}\frac{\partial}{\partial t}\psi(x)=\left[-\frac{1}{2m}\frac{\partial^2}{\partial x^2}+V(x)\right]\psi(x) \tag{4.93}$$

其中使用了称为位置表示的约定 $\langle x|\psi\rangle=\psi(x)$,这是一个非常类似于式(4.91)的椭圆形方程.因此仅仅仿真 Schrödinger 方程并不是模拟量子系统中面临的特殊困难,那么困难在哪里?

模拟量子系统的关键挑战是,必须求解的微分方程为指数数目.对按 Schrödinger 方程演化的一个量子比特,必须求解两个微分方程;对两个量子比特,是四个方程;且对 n 量子比特,是 2^n 个方程.有时具有洞察力的近似可以减少

方程个数，从而使这种量子系统的经典仿真成为可行. 然而，有许多物理上有意义的量子系统，人们尚不知道它们的这类近似.

练习 4.46(量子系统复杂性的指数增长)　令 ρ 是描述 n 量子比特状态的一个密度矩阵，证明对 ρ 的描述需要 4^n-1 个独立实数.

有物理背景的读者或许会同意，许多重要的量子系统的经典仿真是不可行的. 这些系统包括 Hubbard 模型，这是一个相互作用的具有 Hamilton 量

$$H = \sum_{k=1}^{n} V_0 n_{k,\uparrow} n_{k,\downarrow} + \sum_{k,\text{neighbors},\sigma} t_{kl} c_{k\sigma}^{\dagger} c_{l\sigma} \tag{4.94}$$

的 fermi 模型. 它对超导、磁力、Ising 模型和许多其他研究有用，此时 H 为

$$H = \sum_{k=1}^{n} \boldsymbol{\sigma}_k \cdot \boldsymbol{\sigma}_{k+1} \tag{4.95}$$

这些模型的解可以给出许多物理属性的结果，如绝缘常数、传导率和材料的磁化系数等. 量子电动力学(QED)和量子色动力学(QCD)的更为复杂的模型，可以用来计算如质子质量等常数.

量子计算机可以有效模拟量子系统，它们没有有效经典仿真，直观上，出于和任意量子线路可以由一组通用的量子门构造的原因，这样做是可能的. 而且，正如存在不能被有效近似的酉运算，原则上可以想象，也可能有不能在量子计算机上有效模拟的量子系统. 当然，我们相信这样的系统在自然界中实际上是不能实现的，否则我们将利用它们进行超越量子线路模型的信息处理.

4.7.2　量子仿真算法

经典仿真从简单的微分方程解的实现开始，例如一阶 $\mathrm{d}y/\mathrm{d}t = f(y)$ 所知的解的实现是 $y(t+\Delta t) \approx y(t) + f(y)\Delta t$. 类似地，量子情形关心的是 $\mathrm{i}\hbar|\psi\rangle/\mathrm{d}t = H|\psi\rangle$，对时不变的 H，就是

$$|\psi(t)\rangle = \mathrm{e}^{-\mathrm{i}Ht/\hbar}|\psi(0)\rangle \tag{4.96}$$

因为 H 指数通常极难求(也许它是稀疏的，但仍是指数规模的)，所以好的出发点是考虑 $|\psi(t+\Delta t)\rangle \approx (I - \mathrm{i}H\Delta t|\psi(t)\rangle)$ 的一阶解. 这是可解的，因为对许多 Hamilton 量 H 可以直接利用量子门，来有效近似 $I - \mathrm{i}H\Delta t$. 不过，这样的一阶解一般来说非常不充分.

有效近似式(4.96)的解到高阶对许多类 Hamilton 量是可能的. 例如，在大多数物理系统中，Hamilton 量可写作许多局部相互作用的和的形式. 特别地，对一个 n 粒子系统，有

$$H = \sum_{k=1}^{L} H_k \tag{4.97}$$

其中 H_k 最多作用在常数 c 数目的子系统上，而 L 是 n 的一个多项式. 例如，项 H_k

常常只是两体相互作用如 X_jX_k 和单体 Hamilton 量如 X_j. Hubbard 和 Ising 模型都具有这种形式的 Hamilton 量. 这种局部性在物理上相当合理，并且，在许多系统中，大多数相互作用随距离或能量差的增大而衰减. 有时还存在其他附加的全局对称约束，如粒子的统计特性等，我们将很快涉及它们. 重要的是虽然 e^{-iHt} 难以计算，作用在小得多的子系统上的 e^{-iH_kt} 却可以直接用粒子线路来近似. 但由于 $[H_j,H_k]\neq 0$，一般地 $e^{-iHt}\neq\prod_k e^{-iH_kt}$，那么 e^{-iH_kt} 怎样用于得出 e^{-iHt}？

练习 4.47 对 $H=\sum_k^L H_k$，证明如果对所有的 j 和 k，$[H_j,H_k]=0$，则对所有的 t，$e^{-iHt}=e^{-iH_1t}e^{-iH_2t}\cdots e^{-iH_Lt}$.

练习 4.48 H_k 最多包含 c 个粒子的限制，蕴含和式(4.97)中 L 有 n 的多项式上界.

量子仿真算法的核心是如下的渐近近似定理.

定理 4.3(Trotter 公式) 令 A 和 B 是 Hermite 算子，则对任意实数 t，有

$$\lim_{n\to\infty}(e^{iAt/n}e^{iBt/n})^n=e^{i(A+B)t} \tag{4.98}$$

注意，式(4.98)即使对 A 和 B 不对易的情形也是成立的，更有趣的也许是，它可以推广到对应于一般量子运算的某些半群的生成子. 我们将在第 8 章 8.4.1 节描述这样的生成子("Lindblad 形")，现在只考虑 A 和 B 是 Hermite 矩阵的情形.

证明 由定义

$$e^{iAt/n}=I+\frac{1}{n}iAt+O\left(\frac{1}{n^2}\right) \tag{4.99}$$

于是

$$e^{iAt/n}e^{iBt/n}=I+\frac{1}{n}i(A+B)t+O\left(\frac{1}{n^2}\right) \tag{4.100}$$

可得到

$$(e^{iAt/n}e^{iBt/n})^n=e^{i(A+B)t/n}+O\left(\frac{1}{n^2}\right) \tag{4.101}$$

可导出

$$\lim_{n\to\infty}(e^{iAt/n}e^{iBt/n})^n=\lim e^{i(A+B)t}+O\left(\frac{1}{n}\right)=e^{i(A+B)t} \tag{4.102}$$

修改 Trotter 公式，可以导出进行量子仿真的高阶近似方法. 例如，利用与上述证明类似的推导，可以证明

$$e^{i(A+B)\Delta t}=e^{iA\Delta t}e^{iB\Delta t}+O(\Delta t^2) \tag{4.103}$$

类似地

$$e^{i(A+B)\Delta t}=e^{iA\Delta t/2}e^{iB\Delta t}e^{iA\Delta t/2}+O(\Delta t^3) \tag{4.104}$$

量子仿真算法的框架如下，并且盒子 4.2 给出模拟一维非相对论 Schrödinger 方程的例子.

算法　量子仿真

输入　(1) 作用在 N 维系统上的 Hamilton 量 $H=\sum_k H_k$，其中每个 H_k 作用在规模独立于 N 的小的子系统上；(2) 系统在 $t=0$ 时刻的初态 $|\psi_0\rangle$；(3) 正的非零精度 δ；(4) 获得期望状态的时间 t_f.

输出　状态 $|\tilde{\psi}(t_f)\rangle$，使得 $|\langle\tilde{\psi}(t_f)|\mathrm{e}^{-\mathrm{i}Ht_f}|\psi_0\rangle|^2\geqslant 1-\delta$.

运行时间　$O(\mathrm{poly}(1/\delta))$ 数目的操作.

过程　选择一个表示，使得 $n=\mathrm{poly}(\log N)$ 量子比特的状态 $|\tilde{\psi}\rangle$ 能近似系统状态，且算子 $\mathrm{e}^{-\mathrm{i}H_k\Delta t}$ 有有效的量子线路近似. 选择一个近似方法(参看式(4.103)～(4.105))和 Δt，使得期望误差是可接受的(并且对某个整数 j，$j\Delta t=t_f$)，为迭代构造一个相应的量子线路 $U_{\Delta t}$，并且执行：

(1) $|\tilde{\psi}_0\rangle\leftarrow|\psi_0\rangle$；$j=0$　　//状态初始化

(2) $\rightarrow|\tilde{\psi}_{j+1}\rangle=U_{\Delta t}|\tilde{\psi}_j\rangle$　　//迭代更新

(3) $\rightarrow j\leftarrow j+1$；转到(2)直到 $j\Delta t\geqslant t_f$　　//循环

(4) $\rightarrow|\tilde{\psi}(t_f)\rangle=|\tilde{\psi}_j\rangle$　　//最终结果

练习 4.49(Baker-Campbell-Hausdorf 公式)　证明

$$\mathrm{e}^{(A+B)\Delta t}=\mathrm{e}^{A\Delta t}\mathrm{e}^{B\Delta t}\mathrm{e}^{-\frac{1}{2}[A,B]\Delta t^2}+O(\Delta t^3) \tag{4.105}$$

并且再证明式(4.103)和式(4.104).

练习 4.50　令 $H=\sum_{k=1}^{L}H_k$，且定义

$$U_{\Delta t}=[\mathrm{e}^{-\mathrm{i}H_1\Delta t}\mathrm{e}^{-\mathrm{i}H_2\Delta t}\cdots\mathrm{e}^{-\mathrm{i}H_L\Delta t}][\mathrm{e}^{-\mathrm{i}H_L\Delta t}\mathrm{e}^{-\mathrm{i}H_{L-1}\Delta t}\cdots\mathrm{e}^{-\mathrm{i}H_1\Delta t}] \tag{4.106}$$

(1) 证明 $U_{\Delta t}=\mathrm{e}^{-2\mathrm{i}H\Delta t}+O(\Delta t^3)$.

(2) 利用盒子 4.1 的结果，证明对某个常数 α，任意正整数 m，有

$$E(U_V^m,\mathrm{e}^{-2\mathrm{i}mH\Delta t})\leqslant m\alpha\Delta t^3 \tag{4.107}$$

盒子 4.2　Schrödinger 方程的量子仿真

量子仿真的方法和局限性可以通过如下例子说明. 这个例子来自物理学家的传统模型，而不是抽象的量子比特模型. 考虑在一根直线上的运动的具有一维势能 $V(x)$ 的一个单粒子，其 Hamilton 量为

$$H=\frac{p^2}{2m}+V(x) \tag{4.108}$$

其中 p 是动量算子而 x 是位置算子. x 的特征值是连续的，而系统状态 $|\psi\rangle$ 处于无穷维 Hilbert 空间，在基 x 下，可以写成

$$|\psi\rangle=\int|x\rangle\langle x|\psi\rangle\mathrm{d}x \tag{4.109}$$

实践中，只对某个有限区域感兴趣，设其为区域 $-d \leqslant x \leqslant d$. 而且，可以选择离散步长 Δx 与系统的最短波长相比足够小，使得

$$|\tilde{\psi}\rangle = \sum_{k=-d/\Delta x}^{d/\Delta x} a_k |k\Delta x\rangle \tag{4.110}$$

成为 $|\psi\rangle$ 的一个好的物理近似. 这个状态可以用 $n=\lceil \log(2d/\Delta x+1)\rceil$ 量子比特表示，我们直接用 n 量子比特的计算基 $|k\rangle$ 替换基 $|k\Delta x\rangle$（x 算子的一个本征态）. 注意这个仿真只需要 n 量子比特，而经典仿真不得不用 2^n 个复数来保存信息，于是用量子计算机进行仿真，可带来资源的指数性节省.

$|\tilde{\psi}(t)\rangle = e^{-iHt}|\tilde{\psi}(0)\rangle$ 的计算必须利用式(4.103)～(4.105)的一个近似，因为一般来说 $H_1 = V(x)$ 与 $H_0 = p^2/(2m)$ 不对易. 于是我们一定要计算 $e^{-iH_1\Delta t}$ 和 $e^{-iH_0\Delta t}$，因为 $|\tilde{\psi}\rangle$ 是在 H_1 的本征基表出的，$e^{-iH_1\Delta t}$ 形如

$$|k\rangle \to e^{-iV(k\Delta x)\Delta t}|k\rangle \tag{4.111}$$

的一个对角变换. 这个计算是直接的，因为可以计算 $V(k\Delta t)\Delta t$（又见问题 4.1）. 第二项的计算也很简单，因为 x 和 p 是由量子 Fourier 变换 $U_{FFT}xU_{FFT}^{\dagger} = p$ 联系起来的共轭变量，于是 $e^{-iH_0\Delta t} = U_{FFT}e^{-ix^2\Delta t/2m}U_{FFT}^{\dagger}$，为计算 $e^{-iH_0\Delta t}$，执行

$$|k\rangle \to U_{FFT}e^{-ix^2/2m}U_{FFT}^{\dagger}|k\rangle \tag{4.112}$$

U_{FFT} 的构造将在第 5 章讨论.

4.7.3 一个说明性的例子

我们描述的量子仿真过程集中在模拟局部相互作用的 Hamilton 量，然而，这并不是一个根本性的要求. 如下面例子说明的，甚至对不平凡地作用在大系统的，所有或几乎所有部分的 Hamilton 量，有效的量子仿真仍是可能的.

设我们有作用在 n 量子比特上的 Hamilton 量

$$H = Z_1 \otimes Z_2 \otimes \cdots \otimes Z_n \tag{4.113}$$

尽管这是一个涉及整个系统的相互作用，然而事实上可以被有效模拟. 我们期望的是一个对任意 Δt 实现 $e^{-iH\Delta t}$ 的简单的量子线路，图 4.19 给出 $n=3$ 时精确地做到这一点的一个线路. 主要的灵感是，虽然 Hamilton 量涉及系统中的全部量子比特，但属于经典方式：如果 n 量子比特在计算基中的奇偶校验结果是偶数，则应用到系统中的相移是 $e^{-i\Delta t}$；否则相移将是 $e^{i\Delta t}$. 因此，首先经典地计算奇偶校验结果（把结果存储在一个辅助量子比特中），然后以其为条件进行适当的相移，接着逆转奇偶校验的计算（擦除辅助单元），就可简单地实现 H 的仿真. 这个办法显然不只适用于 $n=3$，对任意的 n 都适用.

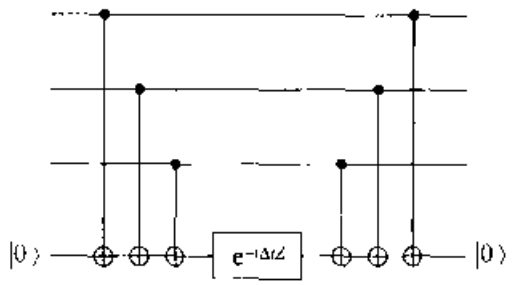


图 4.19　对时间 Δt 模拟 Hamilton 量 $H=Z_1\otimes Z_2\otimes Z_3$ 的量子线路.

进而，对上述过程进行推广，可以模拟更复杂的 Hamilton 量. 特别地，可以有效模拟任何具有形式

$$H=\bigotimes_{k=1}^{n}\sigma_{c(k)}^{k} \tag{4.114}$$

的 Hamilton 量，其中 $\sigma_{c(k)}^{k}$ 是作用在第 k 量子比特上的 Pauli 矩阵(或单位阵)，$c(k)\in\{0,1,2,3\}$ 定出 $\{I,X,Y,Z\}$ 中的一个. 单位运算作用的量子比特可以忽略，而 X 和 Y 项可以用单量子比特门变换成 Z 运算. 这使我们得到一个形如式(4.113)的 Hamilton 量，可以用上述过程进行模拟.

练习 4.51　构造一个 Hamilton 量

$$H=X_1\otimes Y_2\otimes Z_3 \tag{4.115}$$

的量子线路，模拟对任意的 Δt 执行酉变换 $e^{-i\Delta tH}$.

利用这个过程，可以模拟一大类包含非局部项的 Hamilton 量，也可以模拟具有形式 $H=\sum_{k=1}^{L}H_k$ 的 Hamilton 量，其中对单个 H_k 的惟一要求是具有张量积结构，并且要求 L 是粒子总数 n 的多项式. 更一般地，全部的要求是，存在有效的线路来模拟每个单独的 H_k. 例如，Hamilton 量 $H=\sum_{k=1}^{n}X_k+Z^{\otimes n}$ 很容易用上述技术进行模拟，这样的 Hamilton 量通常不会出现在自然界. 不过，它们为量子算法提供了一个可能和有潜在价值的应用前景.

4.7.4　量子仿真的展望

量子仿真算法非常类似于经典方法，但也有根本的差别. 量子算法的每一步迭代必须用新状态彻底替换老状态，如果不对算法做重大改动，无法从中间步骤获得(不平凡的)信息，因为状态是量子的. 而且，必须巧妙选择最终的测量，以获得期望的结果，因为测量会干扰量子状态. 当然，量子仿真可以重复以获得统计量，但我们希望算法至多重复多项式次数. 可能会出现仿真可以有效进行，但没有办法进行期望的测量的情况.

而且确实存在不能有效模拟的 Hamilton 量. 4.5.4 节曾看到，存在量子计算

机不能有效近似的酉变换. 作为推论,不是所有的 Hamilton 量的演化都可以在量子计算机上有效模拟,因为一旦如此,所有的酉变换都应可以被有效近似.

另外一个困难的问题,也是一个有趣的问题,是平衡过程的仿真. 具有 Hamilton 量 H 的一个系统与温度为 T 的环境相连,一般而言会趋于 Gibbs 态的热力学平衡,$\rho_{\text{therm}}=e^{-H/k_BT}/Z$,其中 k_B 是 Boltzmann 常数,而 $Z=\text{tr}e^{-H/k_BT}$ 是通常的划分函数的归一化因子,保证 $\text{tr}(\rho)=1$. 这个平衡发生的过程还不是很清楚,尽管我们知道某些条件:环境必须很大,与 H 本征态能量匹配的粒子数目不为零,而且环境和系统的耦合应该是弱的. 对任意的 H 和 T 得到 ρ_{therm},对经典计算机而言,一般是指数困难的问题. 用量子计算机能有效求解这个问题吗?我们还不知道.

另一方面,如上面我们谈到的,许多有趣的量子问题的确可以用量子计算机有效仿真,甚至当它们和这里的简单算法相比,有额外的约束时也可以. 这些系统涉及来源于粒子统计学的全局对称性. 在日常的世界中,我们习惯于区分不同的粒子,如可以跟踪一个网球场上的网球,保存每个球的信息. 这个可以保持对象谁是谁的能力,是经典对象的一个一般特征——通过连续测量一个经典粒子的位置,可以在每个时刻跟踪它,从而可以惟一地区分每个粒子. 然而,这对量子力学行不通,因为我们不能精确地跟踪单个粒子的运动. 如果两个粒子本质不同,如光子和电子,那么我们可以通过测量它们的电荷正负性,来区分谁是谁. 但对相同粒子,如两个电子,研究发现,它们本质上是不可区分的.

粒子的不可区分性,在具有两种表现形式的系统的状态向量上增加了一条约束. 根据实验,自然界的粒子有两种类型,称为 Bose 子和 Fermi 子. Bose 子系统的状态向量对任意两个成员的置换是不变的,反映出它们的本质不可区分性;与之对照,Fermi 子系统的状态向量对任意两个成员的互换都改变符号. 两种系统都可以在量子计算机上有效模拟. 怎样进行的细节已经超出了本书的范围,不过这个过程相当直接. 给定一个不对称的初态,可以在仿真开始之前进行对称化. 仿真使用的算法可以被设计得保持相应的对称性,甚至允许得到高阶误差项. 对这个问题和其他问题感兴趣的读者,可以在本章末的"历史和进一步阅读的材料"中找到参考资料.

问题 4.1(可计算的相移) 令 m 和 n 是正整数,设 $f:\{0,\cdots,2^m-1\}\to\{0,\cdots,2^n-1\}$ 是一个从 m 比特到 n 比特的经典函数. 可以如 3.2.5 节所述,用 T 个 Toffoli 门进行可逆计算. 即函数 $(x,y)\to(x,y\oplus f(x))$ 可以用 T 个 Toffoli 门实现. 给出一个用 $2T+n$ 个(或更少)单、双和三量子比特门来实现,定义为

$$|x\rangle\to\exp\left(\frac{-2i\pi f(x)}{2^n}\right)|x\rangle \tag{4.116}$$

的酉运算的量子线路.

问题 4.2 求 $C^n(X)$ 门的一个深度为 $O(\log n)$ 的结构(评注:线路的深度是门应用到线路中,形成的不同时间步的数目. 这个问题的关键点在于,有可能通过在同一时间步中并行性地应用许多门,来并行化 $C^n(X)$ 的结构).

问题 4.3(不同的通用性结构)　设 U 是一个 n 量子比特上的酉矩阵,定义 $H \equiv \mathrm{i}\ln(U)$. 证明

(1) H 是 Hermite 的,其特征值在 0 到 2π 范围内.

(2) H 可以写成

$$H = \sum_g h_g g \tag{4.117}$$

其中 h_g 是实数且和展布在 Pauli 矩阵 $\{I, X, Y, Z\}$ 的所有 n 重张量积 g 上.

(3) 对某个正整数 k,令 $\Delta = 1/k$. 说明怎样用 $O(n)$ 个单和双量子比特运算,实现酉运算 $\exp(-\mathrm{i}h_g g\Delta)$.

(4) 证明

$$\exp(-\mathrm{i}H\Delta) = \prod_g \exp(-\mathrm{i}h_g g\Delta) + O(4^n \Delta^2) \tag{4.118}$$

其中乘积是对任意固定次序的 Pauli 矩阵的 n 重张量积 g 取的.

(5) 证明

$$U = \left[\prod_g \exp(-\mathrm{i}h_g g\Delta)\right]^k + O(4^n \Delta) \tag{4.119}$$

(6) 说明如何用 $O(n16^n/\varepsilon)$ 个单或双量子比特运算近似 U 到距离 $\varepsilon > 0$ 以内.

问题 4.4(最小 Toffoli 结构)

(1) 实现 Toffoli 门的双量子比特门的最小数目是多少?

(2) 实现 Toffoli 门的单量子比特门和受控非门的最小数目是多少?

(3) 实现 Toffoli 门的单量子比特门和受控 Z 门的最小数目是多少?

问题 4.5　构造 n 量子比特上的一族 Hamilton 量 $\{H_n\}$,使得模拟 H_n 要求 n 的超多项式数目的运算(评注:这个问题看来相当困难).

问题 4.6(具有预先纠缠的通用性)　受控非门和单量子比特门构成量子逻辑门的一个通用性集合. 证明一个不同的通用性资源集合可由单量子比特酉运算,在 Bell 态下测量量子比特对的能力和将四量子比特制备成纠缠态的能力组成.

第 4 章的总结　量子线路

- **通用性**:n 量子比特上任意的酉运算,可以用单量子比特门和受控非门精确地实现.
- **一个离散集合的通用性**:Hadamard 门、相位门、受控非门和 $\pi/8$ 门. 在 n 量子比特上任意的酉运算,可以用仅由这些门组成的线路近似到任意精度 $\varepsilon > 0$,这意味着它们对量子计算是通用的. 这个清单中用 Toffoli 门代替 $\pi/8$,仍给出一个通用性族.

• **并非所有酉运算都可以有效地实现**：存在 n 量子比特上的酉运算，用门的任何有限集合近似到 ε 的距离，都需要 $\Omega(2^n \log(1/\varepsilon)/\log(n))$ 个门.

• **仿真**：对 Hamilton 量 $H=\sum_k H_k$，给定 $|\psi(0)\rangle$，量子计算机可以有效模拟 e^{-iHt} 的演化，且近似 $|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$. 这里 H 是多项式数目的项 H_k 的和. 对 H_k 可以构造有效的量子线路.

历史和进一步阅读的材料

本章的逻辑门结构参考了很多材料. Barenco、Bennett、Cleve、DiVincenzo、Margolus、Shor、Sleator、Smolin 和 Weinfurter 的论文[BBC+95]是本章许多线路结构和单量子比特门与受控非门通用性证明的来源. Beckman、Chari、Devabhaktuni 和 Preskill 的论文[BCDP96]是关于量子线路灵感的另外一个有用的来源. DiVincenzo[DiV98]提供了一个雅致而容易理解的引论. 测量和控制量子比特终端可以交换的事实是 Griffiths 和 Niu[GN96]指出的.

两级酉运算的通用性证明属于 Reck、Zeilinger、Bernstein 和 Bertani[RZBB94]. 受控非门和单量子比特门的通用性是 DiVincenzo[DiV95b]证明的. 练习 4.44 中的通用性的 G 门有时称为 Deutsch 门[Deu89]. Deutsch、Barenco 和 Ekert[DBE95]以及 Lioyd[Llod95]独立地证明，几乎任意的双量子比特逻辑门都是通用性的. 门序列引起的误差至多是单个门误差的和的结果是 Bernstein 和 Vazirani[BV97]证明的. 我们所集中讨论的，特别的通用性门集合——Hadamard 门、相位门、受控非门和 $\pi/8$ 门，在 Boykin、Mor、Pulver、Roychowdhury 和 Vatan[BMP+99]中被证明是通用的，该文献还包含由 $\cos(\theta/2)\equiv\cos^2(\pi/8)$ 是 π 的无理倍数的一个证明. 4.5.4 节中的界基于 Knill 的论文[Kni95]，该论文对用量子线路近似任意酉运算的难度进行了极为详细的研究. 特别地，Knill 得到了比我们更严格和更一般的界，并且他的分析还可以用到门的连续集而不仅是我们所考虑的有限集. 4.6 节中使用非计算基初始状态以获得超过量子线路模型能力的建议是 Daniel Gottesman 和 Michael Nielsen(私人通信)给出的.

计算的量子线路模型属于 Deutsch[Deu89]，并且由 Yao[Yao93]进行了发展，后一篇论文还证明计算的量子线路模型等价于量子 Turing 机模型. 量子 Turing 机模型是 Benioff[Ben80]在 1980 年引入的，并由 Deutsch[Deu85]和 Yao[Yao93]进行了发展，其现代定义由 Bernstein 和 Vazirani[BV97]给出，后两篇文章也迈出了建立对应于精度计算复杂性理论的量子计算复杂性理论的步子. 特别地，包含关系 BQP$\subseteq$PSPACE

和一些稍强的结果是 Bernstein 和 Vazirani 证明的. Knill 和 Laflamme[KL98]发展出量子和经典计算复杂性之间的一些迷人的联系. 其他有关量子计算复杂性的有趣工作包括 Adleman、Demarrais 和 Huang 的论文[ADH97]，以及 Watrous 的论文[Wat99]，后一篇论文在交互证明系统的背景下，给出量子计算机比经典计算机更强大的证据.

量子计算机或许会比经典计算机在模拟量子系统方面更有效，是 Manin[Man80]在 1980 年宣布的，并由 Feynman[Fey82]在 1982 年独立地进行了更细致的考查. 后来 Abrams 和 Lloyd[AL97]，Boghosian 和 Taylor[BT97]，Sornborger 和 Stewart[SS99]，Wiesner[Wie96]以及 Zalka[Zal98]进行了更为详细的研究. Trotter 公式属于 Trotter[Tro59]，并且还被 Chernoff[Che68]证明，尽管西算子的简单形式相当古老，可追溯到 Sophus Lie 的时代. 第三个更老一些的 Baker Campbell-Hausdorff 公式版本，即式(4.104)，自 Sornborger 和 Stewart[SS99]给出. Abrams 和 Lloyd[AL97]给出了一个在量子计算机上模拟多体 Fermi 子系统的过程. Terhal 和 DiVincenzo[TD98]讨论了量子系统到 Gibbs 态平衡的模拟. 盒子 4.2 中模拟 Schrödinger 方程的方法属于 Zalka[Zal98]和 Wiesner[Wie96].

练习 4.25 属于 Vandersypen，且与 Chau 和 Wilczek[CW95]有关. 练习 4.45 属于 Boykin、Mor、Pulver、Roychowdhury 和 Vatan[BMP+99]. 问题 4.2 属于 Gottesman. 问题 4.6 属于 Gottesman 和 Chuang[GC99].

从非计算基态出发可能得到超过量子线路模型的计算能力的建议(第 4.6 节)是 Daniel Gottesman 和 Michael Nielsen(私人通信)提出的.

CHAPTER 5
第 5 章
量子 Fourier 变换及其应用

如果你建造的是量子计算机，那么每个间谍都会想得到它，我们的密码都会失效，他们会读我们的电子邮件，直到我们用量子加密来阻止他们.

——*Jennifer 和 Peter Shor*

我们阅读电子邮件时，间谍和他们的量子计算机是多么讨厌；不过请放心，他们还不知道怎样分解 12 或 15 呢.

——*Volker Strassen*

计算机编程是一种艺术形式，正如诗歌和音乐的创作.

——*Donald Knuth*

迄今为止，量子计算最引人入胜的发现在于，量子计算机可以有效地完成某些在经典计算机上做不到的任务. 例如，截止到本书写作的时候，用最好的已知的经典算法，所谓数域筛(field sieve)，人们认为求 n 比特整数的素因子分解需要 $\exp(\Theta(n^{1/3}\log^{2/3} n))$ 个操作. 这个算法对被分解数的规模是指数的，因此因子问题一般被视为在经典计算机上不可解的问题：即使对中等长度的数，因子问题也很快变得不可能. 与之对照，量子算法可用 $O(n^2 \log n \log\log n)$ 次操作完成同样的任务，即量子计算机求一个数的因子可指数式地快于已知的最好经典算法. 这个结果本身就很重要，但最令人激动的方面是它引出的问题：还有哪些在经典计算机上不可解的问题，可以在量子计算机上有效求解？

本章阐述量子 Fourier 变换，它是量子因子分解和许多其他有趣量子算法的关键部分. 从 5.1 节开始讲的量子 Fourier 变换是，进行量子力学幅度的 Fourier 变换的有效量子算法，它并没有加速计算经典数据的 Fourier 变换的经典任务，但它的一个重要任务是相位估计，即近似酉算子在某些场合的特征值. 这将在 5.2 节描述. 这允许我们求解若干其他有趣的问题，包括 5.3 节涉及的求阶问题

(order-finding problem)和因子问题(factoring problem). 如第 6 章所述,相位估计还可以和量子搜索算法结合起来,去求解搜索问题的解个数的计数(counting solution)问题. 5.4 节以量子 Fourier 变换如何用于求解隐含子群问题(hidden subgroup problem)的讨论结束本章,该问题是相位估计和求阶问题的推广. 它的一个特殊情况——离散对数(discrete logarithm)问题有有效量子算法,离散对数问题是另一被认为在经典计算机上不可解的问题.

5.1　量子 Fourier 变换

一个好的想法具有这么一种能力,用与问题本意不同的方式来简化和解决问题.

— Robert Tarjan

数学或计算机科学中解决问题的最重要的方法之一,是把问题变换为其他解为已知的问题. 有些这类变换出现得非常频繁,并且用于非常多的不同场合,以致形成了对这些变换自身的研究领域. 量子计算的一项伟大发现就是,某些这样的变换在量子计算机上的计算,可以比在经典计算机上快得多,这个发现使我们能针对量子计算机建立快速算法.

离散 Fourier 变换就是这类变换之一. 按通常的数学记号,离散 Fourier 变换以一个复向量 $x_0,\cdots,x_{N-1}$ 为输入,其中向量的长度 N 是固定参数,输出的数据是如下定义的复向量 $y_0,\cdots,y_{N-1}$:

$$y_k \equiv \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} x_j e^{2\pi ijk/N} \tag{5.1}$$

量子 Fourier 变换是与它严格相同的变换,尽管量子 Fourier 变换的记号与传统记号有些不同. 量子 Fourier 变换定义为,在一组标准正交基 $|0\rangle,\cdots,|N-1\rangle$ 上的一个线性算子,在基态上的作用为

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle \tag{5.2}$$

等价地,对任意状态的作用可写作

$$\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle \tag{5.3}$$

其中幅度 y_k 是幅度 x_j 的离散 Fourier 变换值. 虽然从定义并不能直接看出这是一个酉变换,但它确实是酉的,因此可以作为量子计算机上的动态过程实现. 我们将通过构造计算 Fourier 变换的具体酉量子线路,来说明 Fourier 变换的酉性. 直接证明 Fourier 变换的酉性也很容易.

练习 5.1 给出式(5.2)式定义的线性变换是酉变换的直接证明.

练习 5.2 具体计算 n 量子比特状态$|00\cdots 0\rangle$的 Fourier 变换.

下面取 $N=2^n$,其中 n 是某个整数,且基 $0\rangle,\cdots,2^n-1\rangle$是 n 量子比特的量子计算机的计算基. 我们需要把状态 j 写成二进制形式 $j=j_1j_2\cdots j_n$,更正式地,$j=j_1 2^{n-1}+j_2 2^{n-2}+\cdots+j_n 2^0$. 为方便起见,用记号 $0.j_lj_{l+1}\cdots j_m$ 表示二进制分数 $j_l/2+j_{l+1}/4+\cdots+j_m/2^{m-l+1}$.

通过简单的代数计算,可给出量子 Fourier 变换的有用的积形式:

$$|j_1,\cdots,j_n\rangle \rightarrow \frac{(|0\rangle+e^{2\pi i 0.j_n}|1\rangle)(|0\rangle+e^{2\pi i 0.j_{n-1}j_n}|1\rangle)\cdots(|0\rangle+e^{2\pi i 0.j_1j_2\cdots j_n}|1\rangle)}{2^{n/2}} \tag{5.4}$$

这个积形式非常有用,甚至可以把它作为量子 Fourier 变换的定义. 这里我们简单的解释一下,这个表示允许我们构造有效计算量子 Fourier 变换的一个量子线路,给出量子 Fourier 变换酉性的证明,并为基于量子 Fourier 变换的算法提供灵感. 作为一项附带的回报,在练习中可以得到经典的快速 Fourier 算法.

式(5.4)的积表示与式(5.2)的等价性,可由简单的代数运算得到

$$|j\rangle \rightarrow \frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1}e^{2\pi ijk/2^n}|k\rangle \tag{5.5}$$

$$=\frac{1}{2^{n/2}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}e^{2\pi ij\left(\sum_{l=1}^{n}k_l2^{-l}\right)}|k_1\cdots k_n\rangle \tag{5.6}$$

$$=\frac{1}{2^{n/2}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}\bigotimes_{l=1}^{n}e^{2\pi ijk_l2^{-l}}|k_l\rangle \tag{5.7}$$

$$=\frac{1}{2^{n/2}}\bigotimes_{l=1}^{n}\left[\sum_{k_l=0}^{1}e^{2\pi ijk_l2^{-l}}|k_l\rangle\right] \tag{5.8}$$

$$=\frac{1}{2^{n/2}}\bigotimes_{l=1}^{n}\left[|0\rangle+e^{2\pi ij2^{-l}}|1\rangle\right] \tag{5.9}$$

$$=\frac{(|0\rangle+e^{2\pi i 0.j_n}|1\rangle)(|0\rangle+e^{2\pi i 0.j_{n-1}j_n}|1\rangle)\cdots(|0\rangle+e^{2\pi i 0.j_1j_2\cdots j_n}|1\rangle)}{2^{n/2}} \tag{5.10}$$

积形式(5.4)使推导量子 Fourier 变换的有效线路变得容易. 图 5.1 就给出了一个这样的线路,门 R_k 表示酉变换

$$R_k\equiv\begin{bmatrix}1 & 0\\ 0 & e^{2\pi i/2^k}\end{bmatrix} \tag{5.11}$$

为证明图 5.1 所示的线路是计算量子 Fourier 变换,考虑当$|j_1\cdots j_n\rangle$为输入时的过程. Hadamard 门应用到第一量子比特产生状态

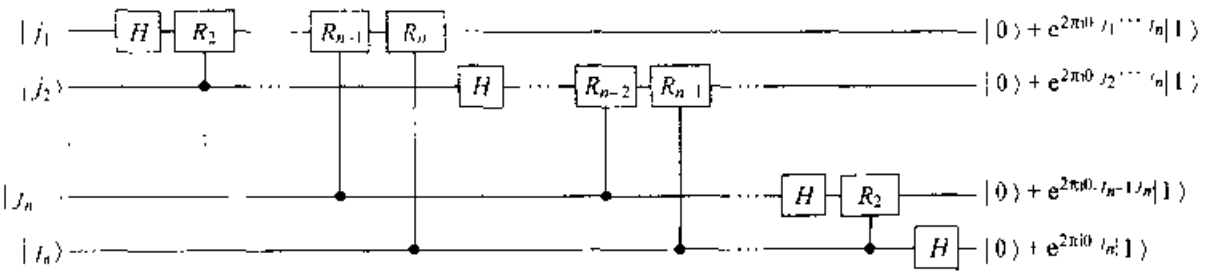


图 5.1　量子 Fourier 变换的有效线路. 这个线路从量子 Fourier 变换的积形式(5.4)很容易推导. 这里没有给出线路末端逆转量子比特顺序的交换门和输出的 $1/\sqrt{2}$ 归一化因子.

$$\frac{1}{2^{1/2}}(|0\rangle+e^{2\pi i 0.j_1}|1\rangle)|j_2\cdots j_n\rangle \tag{5.12}$$

因为当 $j_1=1$ 时，$e^{2\pi i 0.j_1}=-1$，否则为 $+1$. 应用受控 R_2 门产生状态

$$\frac{1}{2^{1/2}}(|0\rangle+e^{2\pi i 0.j_1 j_2}|1\rangle)|j_2\cdots j_n\rangle \tag{5.13}$$

继续应用受控 R_3 门，R_4 直到 R_n 门，每一个门都在第一个 $|1\rangle$ 的系数的相位上增加一个附加比特. 到这个过程的最后，我们有状态

$$\frac{1}{2^{1/2}}(|0\rangle+e^{2\pi i 0.j_1 j_2\cdots j_n}|1\rangle)|j_2\cdots j_n\rangle \tag{5.14}$$

下面对第二量子比特执行类似过程. Hadamdard 门使状态为

$$\frac{1}{2^{2/2}}(|0\rangle+e^{2\pi i 0.j_1 j_2\cdots j_n}|1\rangle)(|0\rangle+e^{2\pi i 0.j_2}|1\rangle)|j_3\cdots j_n\rangle \tag{5.15}$$

应用受控 R_2 直到 R_{n-1} 门，产生状态

$$\frac{1}{2^{2/2}}(|0\rangle+e^{2\pi i 0.j_1 j_2\cdots j_n}|1\rangle)(|0\rangle+e^{2\pi i 0.j_2\cdots j_n}|1\rangle)|j_3\cdots j_n\rangle \tag{5.16}$$

对每个量子比特继续这样的操作，导出最终状态

$$\frac{1}{2^{n/2}}(|0\rangle+e^{2\pi i 0.j_1 j_2\cdots j_n}|1\rangle)(|0\rangle+e^{2\pi i 0.j_2\cdots j_n}|1\rangle)\cdots(|0\rangle+e^{2\pi i 0.j_n}|1\rangle) \tag{5.17}$$

用交换运算(参考 1.3.4 节给出的一个线路描述)逆转量子比特的顺序，图 5.1 为清晰起见略去了这些交换. 经过交换运算，量子比特的状态为

$$\frac{1}{2^{n/2}}(|0\rangle+e^{2\pi i 0.j_n}|1\rangle)(|0\rangle+e^{2\pi i 0.j_{n-1}j_n}|1\rangle)\cdots(|0\rangle+e^{2\pi i 0.j_1 j_2\cdots j_n}|1\rangle) \tag{5.18}$$

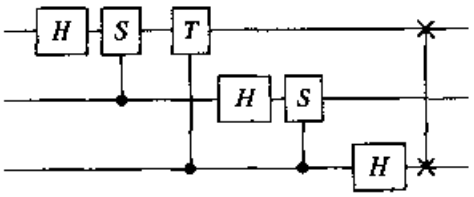
与式(5.4)比较，可以看到这正是量子 Fourier 变换期望的输出. 该结构也证明量

子 Fourier 变换是酉的，因为线路中每个门都是酉的. 盒子 5.1 给出一个三量子比特上量子 Fourier 变换的具体线路.

这个线路用了多少个门？从第一量子比特上的 Hadamdard 门和 $n-1$ 个条件旋转开始——共 n 个门，接着是第二量子比特上的一个 Hadamdard 门和 $n-2$ 个条件旋转，共计 $n+n-1$ 个门. 依次类推，可以看到需要 $n+(n-1)+\cdots+1=n(n+1)/2$ 个门，再加上交换涉及的门. 至多需要 $n/2$ 交换，且每个交换可以用三个受控非门完成. 因此，这个线路提供了进行量子 Fourier 变换的一个 $\Theta(n^2)$ 算法.

盒子 5.1 三量子比特量子 Fourier 变换

为具体起见，我们来看一个三量子比特量子 Fourier 变换的具体例子：



回忆 S 和 T 是相位门和 $\pi/8$ 门(参考名词和记号). 这个实例中量子 Fourier 变换用 $\omega=e^{2\pi i/8}=\sqrt{i}$ 的矩阵表示为

$$\frac{1}{\sqrt{8}}\begin{bmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7\\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6\\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5\\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4\\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3\\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2\\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1\end{bmatrix} \tag{5.19}$$

与之对照，计算 2^n 个元的离散 Fourier 变换的最好经典算法，如快速 Fourier 变换(FFT)，要用 $\Theta(n2^n)$ 个门，即在经典计算机上需要的运算指数式多于在量子计算机的量子 Fourier 变换.

表面上这看起来好极了，因为 Fourier 变换是实际中很多数据处理应用的关键步骤. 例如，在计算机语音识别的应用中，音素识别的第一步是对数字化声音进行 Fourier 变换. 我们可以用量子 Fourier 变换来加速这些 Fourier 变换的计算吗？不幸的是，我们还不知道如何才能做到这一点. 原因在于，量子计算机的幅度不能通过测量直接访问，因此，没办法确定原状态的 Fourier 变换的幅度. 更糟糕的是，

一般没有制备待变换的原状态的有效办法. 因此，寻找量子 Fourier 变换的用途比我们希望的更微妙. 本章和第 6 章我们开发了几个算法，它巧妙运用了量子 Fourier 变换.

练习 5.3(经典快速 Fourier 变换)　在一个经典计算机上进行一个包含 2^n 个复数向量的 Fourier 变换，验证基于式(5.1)的直接方法进行 Fourier 变换，需要 $\Theta(2^{2n})$ 个基本算术运算. 找出基于式(5.4)的运算方法，将这个数量降低到 $\Theta(n2^n)$ 个.

练习 5.4　给出受控 R_k 门到单量子比特门和受控非门的一个分解.

练习 5.5　给出进行逆量子 Fourier 变换的一个量子线路.

练习 5.6(量子 Fourier 变换的近似)　量子 Fourier 变换的量子线路结构，表面上需要用到的门的个数为量子比特数目指数的量级，然而，多项式规模的量子线路永远也不需要这样的精度. 例如，令 U 是 n 量子比特上的理想 Fourier 变换，而 V 是以精度 $\Delta = 1/p(n)$ 完成受控 R_k 门得到的结果，$p(n)$ 是某个多项式. 证明误差 $E(U,V) \equiv \max_{\psi} \| (U-V)|\psi\rangle \|$ 的大小是 $\Theta(n^2/p(n))$，因此每个门的多项式精度对保证输出状态的多项式精度是足够了.

5.2　相位估计

Fourier 变换是称为相位估计(phase estimation)的一般过程的关键，而相位估计又是许多量子算法的关键. 设酉算子 U 具有一个特征值为 $e^{2\pi i\varphi}$ 的特征向量 $|u\rangle$，而 φ 的值是未知的. 相位估计算法的目的是要估计 φ. 为进行估计，假定可以制备状态 $|u\rangle$，并且可以进行受控 U^{2^j} 运算的黑箱(black box，有时称为 oracle)，j 是适当的非负整数. 黑箱的使用表明，相位估计过程本身不是一个完整的量子算法，而是一种和其他子程序结合后，可以完成有意义计算任务的子程序或模块. 在相位估计的特定的应用中，确实是在这样做. 我们会描述这些黑箱运算是如何进行的，并把它们和相位估计过程结合起来，完成真正有用的任务. 不过现在我们要暂时把它们想象为黑箱.

量子相位估计使用两个寄存器. 第一个寄存器包含初态为 $|0\rangle$ 的 t 量子比特. 如何选择 t 和两件事有关：希望精确估计 φ 的位数和相位估计过程希望的成功概率. t 对这两个量的依赖可从下面分析中自然得出.

第二个寄存器初态为 $|u\rangle$，且包含存储 $|u\rangle$ 所需要数目的量子比特. 相位估计分两个阶段. 首先，应用图 5.2 所示的线路. 该线路从对第一寄存器应用 Hadamard 门开始，接着应用受控 U 门到第二寄存器，U 以 2 的幂次自乘. 容易看出第一寄存器的最终状态是

$$\frac{1}{2^{t/2}}(|0\rangle+e^{2\pi i 2^{t-1}\varphi}|1\rangle)(|0\rangle+e^{2\pi i 2^{t-2}\varphi}|1\rangle)\cdots(|0\rangle+e^{2\pi i 2^{0}\varphi}|1\rangle)$$
$$=\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1}e^{2\pi i\varphi k}|k\rangle \tag{5.20}$$

在这个描述中忽略了第二寄存器，因为它在计算过程中始终处于状态$|u\rangle$.

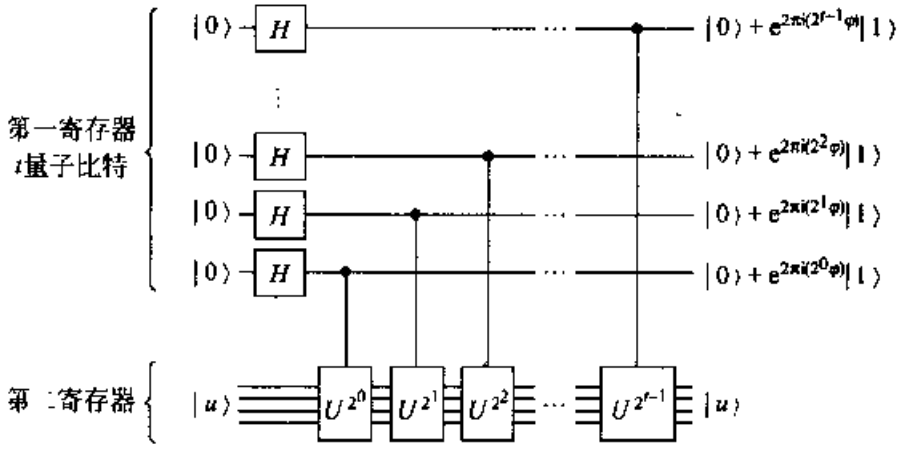


图 5.2 相位估计的第一阶段. 右边略去了归一化因子 $1/\sqrt{2}$.

练习 5.7 通过证明图 5.2 中那样的受控 U 运算把状态$|j\rangle|u\rangle$变到$|j\rangle U^j|u\rangle$，可以获得对图 5.2 中线路更多的了解，现在就证明这一点（注意这并不依赖于$|u\rangle$是 U 的本征态）.

相位估计的第二阶段是应用逆 Fourier 变换到第一寄存器. 这可以通过反转上节 Fourier 变换的线路做到（练习 5.5），并且可在 $O(t^2)$ 步内完成. 相位估计的第三也是最后的阶段是，通过在计算基中的测量读出第一寄存器状态. 我们将证明这给出 φ 的一个相当好的估计，算法的整体框架在图 5.3 给出.

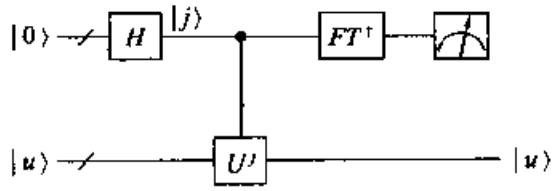


图 5.3 相位估计的全过程的框架. 顶上 t 量子比特（如常用的情形，"/"表示线束）是第一寄存器，而底下的量子比特是第二寄存器，其量子比特数目为进行 U 所需的. $|u\rangle$是 U 的特征值为 $e^{2\pi i\varphi}$ 的一个本征态. 测量的输出是 φ 的输确到 $t-\left\lceil \log\left(2+\frac{1}{2\varepsilon}\right)\right\rceil$比特，成功概率至少为 $1-\varepsilon$ 的近似.

为更清晰地理解为什么相位估计可行，假设 φ 恰好可以表为 t 比特，即 $\varphi = 0.\varphi_1 \cdots \varphi_t$. 则相位估计第一阶段的结果状态式(5.20)，可重写为

$$\frac{1}{2^t}(|0\rangle + e^{2\pi i \cdot \varphi_t}|1\rangle)(|0\rangle + e^{2\pi i \cdot \varphi_{t-1}\varphi_t}|1\rangle)\cdots(|0\rangle + e^{2\pi i \cdot \varphi_1\varphi_2\cdots\varphi_t}|1\rangle) \tag{5.21}$$

相位估计的第二阶段是应用逆 Fourier 变换. 通过比较上式和 Fourier 变换的积形式(式(5.4))，我们看到第二阶段的输出状态是积状态 $|\varphi_1\cdots\varphi_t\rangle$. 在计算基中的测量精确给出 φ.

总之，给定相应的特征向量 $|u\rangle$，相位估计算法使我们能估计酉算子 U 的一个特征值的相位 φ. 这个过程核心的一个本质特点是进行逆 Fourier 变换

$$\frac{1}{2^{t/2}}\sum_{j=0}^{2^t-1} e^{2\pi i\varphi j}|j\rangle|u\rangle \rightarrow |\tilde{\varphi}\rangle|u\rangle \tag{5.22}$$

的能力，其中 $|\tilde{\varphi}\rangle$ 表示测量时，可作为 φ 的好的估计器的一个状态.

5.2.1　性能和要求

上述分析适合 φ 可以精确地展成 t 比特二进制数的理想情况. 如果不是这样会如何？事实上我们描述的过程将会以很高概率，产生 φ 的一个相当不错的近似，如式(5.22)所示. 为证明需要仔细的操作.

令 b 是 $0\sim 2^t-1$ 内的一个整数，它使得 $b/2^t = 0.b_1\cdots b_t$ 成为在小于 φ 的数中 φ 的 t 比特最佳近似. 即，φ 和 $b/2^t$ 之间的差 $\delta \equiv \varphi - b/2^t$ 满足 $0 \leqslant \delta \leqslant 2^{-t}$. 我们要证明，在相位估计过程的最后做的观察产生一个接近 b 的结果，从而以高的概率精确估计 φ. 应用逆量子 Fourier 变换到状态式(5.20)上，产生状态

$$\frac{1}{2^t}\sum_{k,l=0}^{2^t-1} e^{\frac{-2\pi i k l}{2^t}} e^{2\pi i\varphi k}|l\rangle \tag{5.23}$$

令 α_l 为 $|(b+l)(\mathrm{mod}2^t)|$ 的幅度

$$\alpha_l = \frac{1}{2^t}\sum_{k=0}^{2^t-1}(e^{2\pi i(\varphi-(b+l)/2^t)})^k \tag{5.24}$$

这是一个几何级数的和，故

$$\alpha_l = \frac{1}{2^t}\left(\frac{1-e^{2\pi i(2^t\varphi-(b+l))}}{1-e^{2\pi i(\varphi-(b+l)/2^t)}}\right) \tag{5.25}$$

$$= \frac{1}{2^t}\left(\frac{1-e^{2\pi i(2^t\delta-l)}}{1-e^{2\pi i(\delta-l/2^t)}}\right) \tag{5.26}$$

设最终输出的结果为 m，对得到满足 $|m-b|>e$ 的 m 的概率给出估界，其中 e 是刻画容许误差的一个正整数，观察到这样的 m 的概率如下

$$p(|m-b|>e)=\sum_{2^{t-1}<l\leqslant-(e+1)}|a_l|^2+\sum_{e+1\leqslant l\leqslant 2^{t-1}}|a_l|^2 \tag{5.27}$$

但对任意实数 θ，有 $|1-\exp(i\theta)|\leqslant 2$，故

$$|a_l|\leqslant\frac{2}{2^t|1-e^{2\pi i(\delta-l/2^t)}|} \tag{5.28}$$

由初等几何或微积分可知，当 $-\pi\leqslant\theta\leqslant\pi$ 时，$|1-\exp(i\theta)|\geqslant 2|\theta|/\pi$. 但当 $-2^{t-1}<l\leqslant 2^{t-1}$ 时，我们有 $-\pi\leqslant 2\pi(\delta-l/2^t)\leqslant\pi$. 因此

$$|a_l|\leqslant\frac{1}{2^{t+1}(\delta-l/2^t)} \tag{5.29}$$

结合式(5.27)和式(5.29)，得

$$p(|m-b|>e)\leqslant\frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)}\frac{1}{(l-2^t\delta)^2}+\sum_{l=e+1}^{2^{t-1}}\frac{1}{(l-2^t\delta)^2}\right] \tag{5.30}$$

又 $0\leqslant 2^t\delta\leqslant 1$，就得到

$$p(|m-b|>e)\leqslant\frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)}\frac{1}{l^2}+\sum_{l=e+1}^{2^{t-1}}\frac{1}{(l-1)^2}\right] \tag{5.31}$$

$$\leqslant\frac{1}{2}\sum_{l=e}^{2^{t-1}-1}\frac{1}{l^2} \tag{5.32}$$

$$\leqslant\frac{1}{2}\int_{e-1}^{2^{t-1}-1}dl\,\frac{1}{l^2} \tag{5.33}$$

$$=\frac{1}{2(e-1)} \tag{5.34}$$

假设我们希望近似 φ 到精度 2^{-n}，即我们选择 $e=2^{t-n}-1$. 通过在相位估计算法中利用 $t=n+p$ 量子比特，我们从式(5.34)看到，获得精确到这个精度的近似概率至少为 $1-1/2(2^p-2)$. 因此为了以至少 $1-\varepsilon$ 的成功概率精确到 n 比特，得到 φ，我们选择

$$t=n+\left\lceil\log\left(2+\frac{1}{2\varepsilon}\right)\right\rceil \tag{5.35}$$

为使用相位估计算法，需要制备 U 的本征态 $|u\rangle$. 若不知怎样制备这样一个本征态会如何？设代替 $|u\rangle$ 的是某个其他状态 $|\psi\rangle$，把这个状态按 U 的本征态集合展开，得到 $|\psi\rangle=\sum_c c_u|u\rangle$. 设本征态 $|u\rangle$ 具有特征值 $e^{2\pi i\varphi_u}$. 直观上，运行相位估计算法的结果会给出一个接近 $\sum_u c_u|\tilde{\varphi}_u\rangle|u\rangle$ 的输出状态，其中 $\tilde{\varphi}_u$ 是相位 φ_u 的一个很好的近似. 于是，可以预见，第一寄存器的读数将是 φ_u 的一个很好的近似，其中 u 是以 $|c_u|^2$ 概率随机选取的. 这个严格化的论证留作练习 5.8. 这个过程允许我们以在算法中引入一些附加的随机性为代价，避免制备(可能未知的)本征态.

练习 5.8　设相位估计算法把状态 $|0\rangle|u\rangle$ 变为状态 $|\tilde{\varphi}_u\rangle|u\rangle$，使得给定输入 $|0\rangle\left(\sum_u c_u|u\rangle\right)$ 时，算法的输出为 $\sum_u c_u|\tilde{\varphi}_u\rangle|u\rangle$. 证明如果 t 按照式(5.35)选择，则在相位估计算法最后精确到 n 比特测量 φ_u 的概率，至少是 $|c_u|^2(1-\varepsilon)$.

为什么相位估计有意义？就其本身而言，从物理上看，相位估计解决了不平凡和有趣的问题：如何估计一个酉算子相应于给定特征向量的特征值. 不过它的真正用途在于，如下面各节所述的其他可以归结为相位估计的问题. 相位估计算法总结如下.

算法　量子相位估计

输入　(1)对整数 j 进行受控 U^j 运算的黑箱；(2)U 的具有特征值 $e^{2\pi i\varphi_u}$ 的本征态 $|u\rangle$；(3)初始化为 $|0\rangle$ 的 $t=n+\left\lceil\log\left(2+\frac{1}{2\varepsilon}\right)\right\rceil$ 个量子比特.

输出　对 φ_u 的 n 比特近似 $\tilde{\varphi}_u$.

运行时间　$O(t^2)$ 个操作和一个受控 U^j 门的黑箱，成功的概率至少是 $1-\varepsilon$.

过程

(1) $|0\rangle|u\rangle$　　// 初态

(2) $\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|u\rangle$　　// 产生叠加

(3) $\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle U^j|u\rangle$　　// 应用黑箱

$= \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}e^{2\pi ij\varphi_u}|j\rangle|u\rangle$　　// 黑箱的结果

(4) $\rightarrow |\tilde{\varphi}_u\rangle|u\rangle$　　// 应用逆 Fourier 变换

(5) $\rightarrow |\tilde{\varphi}_u\rangle$　　// 测量第一寄存器

练习 5.9　令 U 是一个特征值为 ± 1 的酉变换，作用在一个状态 $|\psi\rangle$ 上. 利用相位估计过程，构造一个量子线路，使 $|\psi\rangle$ 坍缩到 U 的两个本征空间之一，并给出最终状态在哪个空间的一个经典指示器. 与练习 4.34 的结果进行比较.

5.3　应用：求阶和因子问题

相位估计过程可用来解决各种有趣的问题. 现在描述这些问题中最有趣的两个：求阶问题(order-finding problem)和因子问题. 这两个问题实际上是等价的，因此在 5.3.1 节我们说明解求阶问题的一个量子算法，而在 5.3.2 节说明求阶问题还蕴含求因子问题的能力.

为了解因子分解和求阶的量子算法，需要一点数论的背景知识. 所有用到的材料都收集在附录 D 中. 下两节给出的描述中我们集中在问题的量子方面，为读懂仅需要对模算术(modular arithmetric)比较熟悉. 我们引用的数论理论结果的细节证明可以在附录 D 中找到.

至少出于三方面的原因，求阶和因子问题的快速量子算法有价值. 首先，在我们看来最重要的，是它们为量子计算机可能比经典计算机更强大的观点提供了证据，并且对强 Church Turing 论题提出可信的挑战. 其次，这两个问题对不管是经典的，还是量子的任何新算法，都具有值得去证实的内在价值. 最后，从实践观点看最重要的，求阶和因子分解的有效算法可用来破解 RSA 公钥密码系统(附录 E).

5.3.1 应用：求阶

对满足 $x< N$，且无公因子的正整数 x 和 N，x 模 N 的阶定义为最小正整数 r，使得 $x^r=1(\mathrm{mod}\ N)$. 求阶问题就是对特定的 x 和 N 确定阶. 因为没有已知的，用给定问题的 $O(L)$ 比特的多项式规模资源算法求解该问题，人们相信求阶问题在经典计算机上是一个困难的问题，其中 $L\equiv\lceil\log(N)\rceil$ 是给定 N 所需要的比特数. 本节说明怎样用相位估计得到求阶的一个有效量子算法.

练习 5.10 证明 $x=5$ 模 $N=21$ 的阶是 6.

练习 5.11 证明 x 的阶满足 $r\leqslant N$.

求阶的量子算法恰好是把相位估计算法应用到酉算子

$$U|y\rangle\equiv|xy(\mathrm{mod}\ N)\rangle \tag{5.36}$$

其中 $y\in\{0,1\}^L$(注意这里和下面，当 $N\leqslant y\leqslant 2^L-1$ 时，约定 $xy(\mathrm{mod}\ N)$ 就是 y. 即，U 的作用仅当 $0\leqslant y\leqslant N-1$ 时是不平凡的). 简单的计算表明，对整数 $0\leqslant s\leqslant r-1$ 定义的状态

$$|u_s\rangle\equiv\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi isk}{r}\right]|x^k\bmod N\rangle \tag{5.37}$$

是 U 的本征态，因为

$$U|u_s\rangle=\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi isk}{r}\right]|x^{k+1}\bmod N\rangle \tag{5.38}$$

$$=\exp\left[\frac{2\pi is}{r}\right]|u_s\rangle \tag{5.39}$$

利用相位估计，使我们以高精度得到相应的特征值 $e^{(2\pi is/r)}$，再花一点功夫就可以得到阶 r.

练习 5.12 证明 U 是酉的(提示：x 与 N 互质，于是有模 N 的逆).

应用相位估计过程有两个重要的要求：必须有对任意整数 j 实现受控 U^{2^j} 操作的有效过程，且必须能够有效制备具有不平凡特征值的本征态 $|u\rangle$ 或至少是这样的本征态的一个叠加. 第一个要求用称为求模幂(modular exponentiation)的过程来满足，用这个过程，我们能够实现整个受控 U^{2^j} 运算的序列，以应用到用 $O(L^3)$ 个门的相位估计过程，如盒子 5.2 所描述的.

盒子 5.2　求　模　幂

在求阶算法中，如何计算相位估计算法的受控 U^{2^j} 运算的序列？即我们希望计算变换

$$|z\rangle|y\rangle \rightarrow |z\rangle U^{z_{t-1}2^{t-1}}\cdots U^{z_1 2^0}|y\rangle \tag{5.40}$$

$$= |z\rangle|x^{z_{t-1}2^{t-1}}\times\cdots\times x^{z_1 2^0}y(\mathrm{mod}\ N)\rangle \tag{5.41}$$

$$= |z\rangle|x^z y(\mathrm{mod}\ N)\rangle \tag{5.42}$$

因此相位估计中用的受控 U^{2^j} 运算的序列等价于，用一个求模幂 $x^z(\mathrm{mod}\ N)$ 乘以第二寄存器的内容，其中 z 是第一寄存器的内容. 这个运算可以轻易地用可逆计算的技术来完成. 基本思路是以可逆方式对第二寄存器中的 z 计算函数 $x^z(\mathrm{mod}\ N)$，并用退计算的技巧在完成计算后，擦除第三寄存器的内容. 计算求模幂的算法分两个阶段. 第一阶段通过 x 的平方对 N 取模，用带模乘法计算 $x^2(\mathrm{mod}\ N)$，然后通过 x^2 的平方对 N 取模计算 $x^4(\mathrm{mod}\ N)$，并一直进行下去，对所有直到 $t-1$ 的 j 计算 $x^{2^j}(\mathrm{mod}\ N)$. 我们采用 $t=2L+1+\lceil \log(2+1/(2\epsilon))\rceil = O(L)$，所以总共 $t-1=O(L)$ 个平方运算，每个需要 $O(L^2)$ 规模的费用(这个费用假设了用人们孩童时代所学的熟知的乘法算法来实现平方)，第一阶段总的费用是 $O(L^3)$. 第二阶段的算法基于我们已经注意的事实

$$x^z(\mathrm{mod}\ N) = (x^{z_{t-1}2^{t-1}}(\mathrm{mod}\ N))(x^{z_{t-2}2^{t-2}}(\mathrm{mod}\ N))\cdots(x^{z_1 2^0}(\mathrm{mod}\ N)) \tag{5.43}$$

通过进行每个代价为 $O(L^2)$ 的 $t-1$ 个带模乘法，可以看到这个乘积可用 $O(L^3)$ 个门计算. 这对我们的目的是足够有效的，但可以有更有效的算法(参看“历史和进一步阅读的材料”). 利用 3.2.5 节的技术，可直接构造一个带有 t 比特寄存器和 L 比特寄存器用 $O(L^3)$ 个门的可逆电路，使当从 (z,y) 状态开始时输出为 $(z,x^z y(\mathrm{mod}\ N))$. 该电路可以转换为用 $O(L^3)$ 门计算变换 $|z\rangle|y\rangle \rightarrow |z\rangle|x^z y(\mathrm{mod}\ N)\rangle$ 的量子线路.

第二个要求需要一定技巧：为制备 $|u_r\rangle$，要求我们知道 r，这不可能. 幸运的是，有一个聪明的观察，可以使我们回避制备 $|u_r\rangle$ 的问题，即

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1} |u_s\rangle = |1\rangle \tag{5.44}$$

在进行相位估计的过程中，如果第一寄存器用 $t=2L+1+\left\lceil \log\left(2+\frac{1}{2\varepsilon}\right)\right\rceil$ 个量子比特(参考图 5.3)，并把第二寄存器制备成 $|1\rangle$ 状态——其构造是平凡的——则可知对每个在 0 到 $r-1$ 范围内的 s，我们都将以不小于 $(1-\varepsilon)/r$ 的概率，得到相位 $\varphi\approx s/r$ 的精确到 $2L+1$ 比特的估计. 求阶算法的框架如图 5.4.

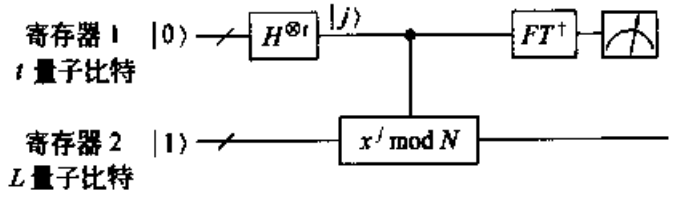


图 5.4 求阶算法的量子线路. 第二寄存器初始化为状态 $|1\rangle$，但如果用练习 5.14 的方法，它可以初始化为 $|0\rangle$. 利用 5.3.2 节的归约，这个线路还可以用作因子分解

练习 5.13 证明式(5.44)$\left($提示：$\sum_{s=0}^{r-1}\exp(-2\pi isk/r) = r\,\delta_{k0}\right)$，即证明

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1} e^{2\pi isk/r} |u_s\rangle = |x^k \bmod N\rangle \tag{5.45}$$

练习 5.14 若我们将第二寄存器初始化为 $|1\rangle$，在逆 Fourier 变换之前，求阶算法产生的量子状态是

$$|\psi\rangle = \sum_{j=0}^{2^t-1} |j\rangle U^j |1\rangle = \sum_{j=0}^{2^t-1} |j\rangle |x^j \bmod N\rangle \tag{5.46}$$

证明如果我们把 U^j 替换为酉变换 V，V 计算

$$V|j\rangle|k\rangle = |j\rangle|k + x^j \bmod N\rangle \tag{5.47}$$

且让第二寄存器从 $|0\rangle$ 开始，将得到同样的状态. 同时说明如何仍用 $O(L^3)$ 个门构造 V.

1. 连分式展开(continued fraction expression)

求阶到相位估计的归约可由从描述相位估计算法的结果 $\varphi\approx s/r$ 中如何得到期望答案 r 而完成. 我们只知道 φ 近似到 $2L+1$ 位，但我们预先还知道它是一个有理数——两个有界整数之比——而且如果能计算出离 φ 最近的这样的分数，或许可以得到 r. 值得注意的是，完成这个任务的有效算法是存在的，称为连分式算法. 这个方法的原理的一个例子在盒子 5.3 给出. 该算法满足我们要求的原因是如下定理，它在附录 D 中被证明.

定理 5.1　设 s/r 是一个使得

$$\left|\frac{s}{r}-\varphi\right|\leqslant\frac{1}{2r^2} \tag{5.48}$$

的有理数. 则 s/r 是 φ 的连分式的一个渐近值，且因此可以用连分式算法在 $O(L^4)$ 个运算之内计算.

由于 φ 是 s/r 精确到 $2L+1$ 位的一个近似，从 $r\leqslant N\leqslant 2^L$ 可知，$|s/r-\varphi|\leqslant 2^{-2L-1}\leqslant 1/2r^2$，因此定理成立.

总之，给定 φ，连分式算法可有效地产生出没有公因子的数 s' 和 r'，使得 $s'/r'=s/r$，数 r' 是阶的候选对象. 可以通过计算 $x^{r'} \bmod N$，看结果是否为 1，来检查它是否为阶. 如果是，则 r' 是 x 模 N 的阶，我们的任务就完成了.

2. 性能

什么情况下这里的求阶算法会失败？有两种可能性. 首先，相位估计的结果可能给出 s/r 的一个糟糕的估计. 但这样的概率至多为 ε，并且可以通过线路规模的可忽略的增大来减小. 其次，s 和 r 可能有公因子. 这时连分式算法返回的 r' 是 r 的一个因子，而非 r 本身. 幸运的是，至少有三种办法可以解决这个问题.

最直接的办法或许是注意到在 $0\sim r-1$ 内随机选取的 s，实际上 s 和 r 很可能是互质(co-prime)的，在这种情况下连分式算法必然返回 r. 为明确这一点，注意由问题 D. 1，小于 r 的素数的数目至少为 $r/2\log r$，因此 s 是素数的机会至少是 $1/2\log(r)>1/2\log(N)$. 故重复算法 $2\log(N)$ 次，将会以高的概率得到一个相位 s/r，使得 s 和 r 互质，于是用连分式算法可得到期望的 r.

盒子 5.3　连分式算法

连分式算法的思想是只用整数把实数描述为如下形式

$$[a_0,\cdots,a_M]\equiv a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\cdots+\cfrac{1}{a_M}}}} \tag{5.49}$$

其中 $a_0,\cdots,a_M$ 是正整数(对量子计算的应用假设也允许 $a_0=0$)，我们定义这个连分式的第 m 个渐近值($0\leqslant m\leqslant M$)为 $[a_0,\cdots,a_m]$. 连分式算法是一个确定任意实数连分式的方法，通过下面的例子很容易明白. 设我们试图把 31/13 分解为连分式. 第一步是把 31/13 分成整数的分数部分

$$\frac{31}{13}=2+\frac{5}{13} \tag{5.50}$$

下面把分数部分倒过来，得到

$$\frac{31}{13}=2+\frac{1}{\frac{13}{5}} \tag{5.51}$$

这些步骤——分开接着倒转——应用到 13/5，得出

$$\frac{31}{13}=2+\frac{1}{2+\frac{3}{5}}=2+\frac{1}{2+\frac{1}{\frac{5}{3}}} \tag{5.52}$$

下面分开和倒转 5/3

$$\frac{31}{13}=2+\frac{1}{2+\frac{1}{1+\frac{2}{3}}}=2+\frac{1}{2+\frac{1}{1+\frac{1}{\frac{3}{2}}}} \tag{5.53}$$

连分式分解现在终止了，因为

$$\frac{3}{2}=1+\frac{1}{2} \tag{5.54}$$

可以写成一个分子是 1 的形式而不需要倒转，这就给出了 31/13 的最终连分式表示

$$\frac{31}{13}=2+\frac{1}{2+\frac{1}{1+\frac{1}{1+\frac{1}{2}}}} \tag{5.55}$$

显然对任何有理数连分式算法有限步分开和倒转后终止，因为出现的分子是严格递减的(例子中是 31,5,3,2,1). 这个过程终止的速度有多快？事实上如果 $\varphi=s/r$ 是一个有理数，并且 s 和 r 是 L 比特的整数，则 φ 的连分式展开可以用 $O(L^3)$ 步运算计算——$O(L)$ 分开和倒转步骤，每个步骤用 $O(L^2)$ 个基本算术门.

第二种方法是如果 $r'\neq r$，则 r' 肯定是 r 的一个因子，除非事件 $s=0$ 发生，其概率为 $1/r<1/2$. 但经过几次重复，$s=0$ 的情况就可以不考虑了. 设我们用 $a'\equiv a^{r'}\pmod N$ 代替 a，则 a' 的阶是 r/r'. 重复算法，并尝试计算 a' 的阶. 如果成功，可计算 a 的阶，因为 $r=r'\times r/r'$. 如果失败，则得到 r/r' 的因子 r''，可以计算 $a''\equiv(a')^{r''}\pmod N$ 的阶. 迭代这个过程，直到确定 a 的阶，它最多需要 $\log(r)=O(L)$ 次，因为每次重复都把当前的候选对象 $a''\cdots$ 的阶降低至少一半.

第三种方法比前两种方法要好. 因它只需要常数次尝试，而不是 $O(L)$ 次重

复. 思路是把相位估计重复两次，第一次得到 r_1'，s_1'，第二次得到 r_2'，s_2'. 设 s_1' 和 s_2' 没有公因子，r 可以通过取 r_1' 和 r_2' 的最小公倍数得到. s_1' 和 s_2' 没有公因子的概率为

$$1-\sum_q p(q \mid s_1')\,p(q \mid s_2') \tag{5.56}$$

其中的和为所有素数 q 之和，$p(x \mid y)$ 表示 x 整除 y 的概率. 如果 q 整除 s_1'，则它也能整除真正的 s，第一次迭代的 s_1，故为估计 $p(q \mid s_1')$ 的上界，只要估计 $p(q \mid s_1)$ 的上界，其中 s_1 是从 0 到 $r-1$ 中按均匀分布选出. 容易看出 $p(q \mid s_1) \leqslant 1/q$，因此 $p(q \mid s_1') \leqslant 1/q$. 类似地，$p(q \mid s_2') \leqslant 1/q$，于是 s_1' 和 s_2' 没有公因子的概率是

$$1-\sum_q p(q \mid s_1')\,p(q \mid s_2') \geqslant 1-\sum_q \frac{1}{q^2} \tag{5.57}$$

右边项可以用不同的方法估计上界，在练习 5.16 中提供了一个简单的技术，给出

$$1-\sum_q p(q \mid s')\,p(q \mid s_1') \geqslant \frac{1}{4} \tag{5.58}$$

因此得到正确 r 的概率至少为 1.4.

练习 5.15　证明正整数 x 和 y 的最小公倍数是 $xy/\gcd(x,y)$，其中 $\gcd(x,y)$ 表示 x,y 的最大公因子. 因此若 x 和 y 是 L 比特数，可以在 $O(L^3)$ 步运算内算出.

练习 5.16　对所有的 $x \geqslant 2$，证明 $\int_2^{x+1} 1/y^2\,\mathrm{d}y \geqslant 2/3x^2$. 证明下式

$$\sum_q \frac{1}{q} \leqslant \frac{3}{2}\int_2 \frac{1}{y}\,\mathrm{d}y = \frac{3}{4} \tag{5.59}$$

由上式，可知式(5.58)成立.

这个算法需要消耗多少资源？Hadamard 变换需要 $O(L)$ 个门，逆 Fourier 变换需要 $O(L^2)$ 个门，量子线路的主要资源消耗在求模幂，这需要 $O(L^3)$ 个门，因此整个量子线路的门数也是 $O(L^3)$ 的. 连分式算法又增加了 $O(L^3)$ 个门，因为要用 $O(L^2)$ 个门去获得 r'. 利用第三种方法从 r' 获得 r，我们仅需要重复这个过程常数次，以得到阶 r，总共消耗 $O(L^3)$ 规模的资源. 算法总结如下.

算法　量子求阶

输入　(1)对与 L 比特数 N 互质的数 x，进行变换 $|j\rangle|k\rangle \to |j\rangle|x^j k \bmod N\rangle$ 的黑箱 $U_{x,N}$；(2)初始化为 $|0\rangle$ 的 $t=2L+1+\left\lceil \log\left(2+\frac{1}{2\epsilon}\right)\right\rceil$ 个量子比特；(3)初始化为状态 $|1\rangle$ 的 L 个量子比特.

输出　最小的，整数 $r>0$，使 $x^r=1 \pmod N$.

运行时间　$O(L^3)$ 个运算，成功的概率是 $O(1)$.

过程

(1) $|0\rangle|1\rangle$　　初始状态

$$(2) \rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1} |j\rangle |1\rangle \qquad // 产生叠加$$

$$(3) \rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1} |j\rangle |x^j \bmod N\rangle \qquad // 应用 U_{x,N}$$

$$\approx \frac{1}{\sqrt{r2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1} e^{2\pi isj/r} |j\rangle |u_s\rangle$$

$$(4) \rightarrow \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1} |\widetilde{s/r}\rangle |u_s\rangle \qquad // 应用逆 Fourier 变换到第一寄存器$$

$$(5) \rightarrow \widetilde{s/r} \qquad // 测量第一寄存器$$

$$(6) \rightarrow r \qquad // 应用连分式算法$$

5.3.2 应用：因子分解

区分素数和合数，以及将合数分解为素因子的问题，是整个算术中最重要和最有用的一个问题.……科学的尊严似乎要求，每一个有助于解决这样一个优雅和著名问题的努力要得到热情支持.

——*Carl Friedrich Gauss*，*Donald Knuth* 的引文

给定一个正合数 N，怎样的一组素数乘起来与之相等？因为求阶的快速算法可以很容易地变成因子分解的快速算法，所以这个因子问题实际上等价子我们刚讨论过的求阶问题.本节将解释把因子问题归结为求阶问题的方法，并给出这个归约的一个例子.

把因子问题归结为求阶的过程分成两个基本步骤.第一步，证明如果我们能够找到方程 $x^2 = 1 \pmod N$ 的一个不平凡解 $x \neq \pm 1 \pmod N$，则可以计算出 N 的一个因子.第二步，证明一个随机选择与 N 互质的 y 很可能具有偶数的阶 r，使得 $y^{r/2} \neq \pm 1 \pmod N$，因此 $x \equiv y^{r/2} \pmod N$ 是 $x^2 = 1 \pmod N$ 的一个不平凡解.这两步体现在如下定理中，定理的证明可以在附录 D 的 D.3 节找到.

定理 5.2 设 N 是一个 L 比特的合数，而 x 是方程 $x^2 = 1 \pmod N$ 在整数范围 $1 \leqslant x \leqslant N$ 内的一个不平凡解，即，既不满足 $x = 1 \pmod N$，也不满足 $x = N-1 = -1 \pmod N$，则用 $O(L^3)$ 步计算出的 $\gcd(x-1, N)$ 和 $\gcd(x+1, N)$ 中至少有一个是 N 的不平凡因子.

定理 5.3 设 $N = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ 是一个正奇合数的素因子分解，令 x 是在 $1 \leqslant x \leqslant N-1$ 内均匀随机选出的整数，且 x 与 N 互质，令 r 是 x 模 N 的阶，则

$$p(r \text{ 是偶数，且 } x^{r/2} \neq -1 \pmod N) \geqslant 1 - \frac{1}{2^m} \tag{5.60}$$

定理 5.2 和定理 5.3 结合起来，可以给出以很高概率返回任意合数 N 的一个不平凡因子的算法.（根据目前所知）除用到的求阶子程序外，算法所有步骤都可以在经典计算机上有效执行. 重复这个过程，可以求出 N 的完整素因子分解. 算法总结如下.

算法　因子分解到求阶的归约

输入　一个合数 N.

输出　N 的一个不平凡因子.

运行时间　$O((\log N)^3)$ 个运算，成功的概率是 $O(1)$.

过程

(1) 若 N 是偶数，返回因子 2.

(2) 确定对 $a\geqslant 1$ 和 $b\geqslant 2$ 是否有 $N=a^b$，如果是，返回因子 a（利用练习 5.17 的经典算法）.

(3) 随机地在 1 到 $N-1$ 范围内选择 x，若 $\gcd(x,N)>1$，则返回因子 $\gcd(x,N)$.

(4) 利用求阶子程序，求 x 模 N 的阶 r.

(5) 若 r 是偶数且 $x^{r/2}\neq -1 \pmod N$，则计算 $\gcd(x^{r/2}-1,N)$ 和 $\gcd(x^{r/2}+1,N)$，并且测试出这两个数中哪个是不平凡因子，如果有一个是因子则返回该数. 否则，算法失败.

算法的第 1 步和第 2 步要么返回一个因子，要么保证 N 是一个包含多于一个素因子的奇数. 这些步骤可以分别用 $O(1)$ 和 $O(L^3)$ 步运算完成. 第 3 步要么返回一个因子，要么随机从 $\{0,1,2,\cdots,N-1\}$ 中抽出 x. 第 4 步调用求阶子程序，计算 x 模 N 的阶 r. 第 5 步结束算法，因为定理 5.3 以至少 $\frac{1}{2}$ 的概率保证 r 为偶数且 $x^{r/2}\neq -1 \pmod N$，于是定理 5.2 保证要么 $\gcd(x^{r/2}-1,N)$ 要么 $\gcd(x^{r/2}+1,N)$ 是 N 的一个不平凡因子. 盒子 5.4 给出这个利用量子求阶子程序的算法的一个例子.

练习 5.17　设 N 为 L 比特长. 本练习的目的是找出一个有效的经典算法，判定 $N=a^b$ 是否对某些整数 $a\geqslant 1$ 和 $b\geqslant 2$ 成立. 这可以按如下步骤达到.

(1) 证明若这样的 b 存在，则必满足 $b\leqslant L$.

(2) 证明为计算 $\log_2 N$，对 $b\leqslant L$ 计算 $x=y/b$，以及计算两个最接近 2^x 的整数 u_1 和 u_2，至多需要 $O(L^2)$ 个运算.

(3) 证明为计算 u_1^b 和 u_2^b（反复使用平方）和检查它们是否等于 N，至多需要 $O(L^2)$ 个运算.

(4) 将前面的结果结合起来给出一个 $O(L^4)$ 算法，以判定 $N=a^b$ 是否对整数 a 和 b 成立.

盒子 5.4 以量子力学方式因子分解 15

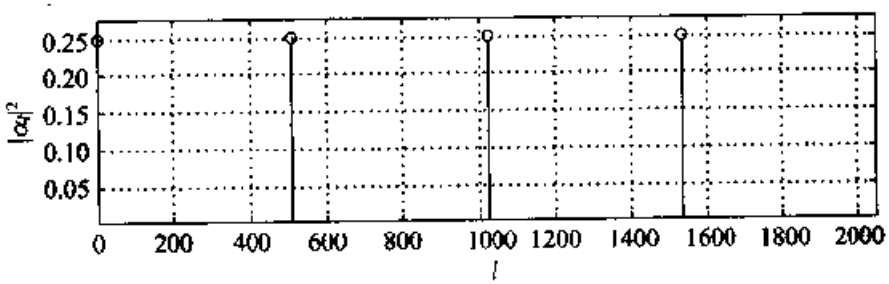
通过对 $N=15$ 分解因子，来说明利用求阶、相位估计和连分式展开的量子因子分解算法. 首先，选择与 N 没有公因子的一个随机数，假设选 $x=7$. 接下来，我们用量子求阶算法计算 x 相对 N 的阶：从状态 $|0\rangle|0\rangle$ 开始，并通过应用 $t=11$，Hadamard 变换到第一寄存器产生状态

$$\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}|k\rangle|0\rangle=\frac{1}{\sqrt{2^t}}[|0\rangle+|1\rangle+|2\rangle+\cdots+|2^t-1\rangle]|0\rangle \quad (5.61)$$

选择这样的 t，保证了误差概率 ε 至多为 1/4. 然后，计算 $f(k)=x^k \bmod N$，并把结果放在第二寄存器中

$$\begin{aligned}&\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}|k\rangle|x^k \bmod N\rangle \quad (5.62)\\ &=\frac{1}{\sqrt{2^t}}[|0\rangle|1\rangle+|1\rangle|7\rangle+|2\rangle|4\rangle+|3\rangle|13\rangle\\ &\quad+|4\rangle|1\rangle+|5\rangle|7\rangle+|6\rangle|4\rangle+\cdots]\end{aligned}$$

再应用逆 Fourier 变换 $FT^\dagger$ 到第一寄存器，并测量它. 分析所得结果分布的一个方法是，计算第一寄存器的约化概率密度函数，并对它应用 $FT^\dagger$，然后计算测量统计量. 不过，因为第二寄存器上没有进一步的运算，我们可以代之以应用隐含测量原理(4.4 节)，而假设第二寄存器也被测量，得到 1,7,4,13 的随机结果. 设我们得到 4(任何结果都可以)，这意味着输入到 $FT^\dagger$ 的状态应该是 $\sqrt{\frac{4}{2^t}}[|2\rangle+|6\rangle+|10\rangle+|14\rangle+\cdots]$. 应用 $FT^\dagger$ 后，我们对 $2^t=2048$ 绘出的概率分布如下图所示.



得到某个状态 $\sum_l \alpha_l|l\rangle$. 最终测量于是以几乎恰好每个 1/4 的概率给出 0,512，1024 或 1536 中的一个结果. 假设我们得到 $l=1536$，那么计算连分式展开就给出 $1536/2048=1/(1+(1/3))$，这样 3/4 成为展开的一个渐近值，$r=4$ 就是 $x=7$ 的阶. 碰巧的是，r 是偶数，且 $x^{r/2} \bmod N=7^2 \bmod 15=4\neq -1 \bmod 15$，于是算法奏效：计算最大公因子 $\gcd(x^2-1,15)=3$ 和 $\gcd(x^2+1,15)=5$ 给出 $15=3\times 5$.

练习 5.18(因子分解 91)　假设我们希望因子分解 $N=91$. 验证第 1 步和第 2 步会通过. 对第 3 步，设我们选择 $x=4$，它与 91 互质. 计算 x 相对 N 的阶，并证明 $x^{r/2} \bmod 91 = 64 \not\equiv -1 \pmod{91}$，因此算法会成功，并给出 $\gcd(64-1,91)=7$. 这不是读者所见到过的分解 91 的最有效方法. 的确，如果所有的计算都在经典计算机上进行，这个归约不会导致一个有效的因子分解算法，因为尚不知道在经典计算机上解决求阶问题的有效解法.

练习 5.19　证明 $N=15$ 是需要用到求阶子程序的最小数，即它是既非偶数又非某个更小整数的幂的最小的合数.

5.4　量子 Fourier 变换的一般应用

到此为止，我们在本章中描述的量子 Fourier 变换的主要应用是相位估计和求阶，这种技术可以解决哪些其他问题？本节中，定义一个称为隐含子群问题的非常一般的问题，并描述一个解决该问题的有效量子算法. 这个问题围绕着众所周知的量子 Fourier 变换的指数加速应用，在函数定义域和值域结构非常复杂情况下，可被视为求一个周期函数的未知周期的一种推广. 为以最容易理解的方式描述该问题，我们从两个更具体的应用：求(一维函数的)周期问题和离散对数问题出发，然后再回到一般的隐含子群问题. 注意本节的阐述比本章中前面的小节更简明和概念化，这意味着，希望掌握全部细节的读者必须付出更多努力.

5.4.1　求周期问题

考虑如下问题. 设 f 是一个输出为单比特的周期函数，满足对某个未知的 $0<r<2^L$，$f(x+r)=f(x)$，其中 $x,r\in\{0,1,2,\cdots\}$. 给定一个执行酉变换 $U|x\rangle|y\rangle\to|x\rangle|y\oplus f(x)\rangle$ 的量子黑箱(其中$\oplus$表示模 2 加)，为确定 r 需要用到黑箱多少次和多少其他运算？注意实际中 U 作用在一个有限域上，它的尺寸决定于对 r 期望的精度. 下面是一个利用一次黑箱计算和 $O(L^2)$ 次其他运算的算法.

算法　求周期

输入　(1)一个执行运算 $U|x\rangle|y\rangle=|x\rangle|y\oplus f(x)\rangle$ 的黑箱；(2)一个存储函数值的状态，初始化为 $|0\rangle$；(3)初始化为 $|0\rangle$ 的 $t=O(L+\log(1/\varepsilon))$ 量子比特.

输出　最小的 $r>0$ 的整数，使得 $f(x+r)=f(x)$.

运行时间　利用 U 一次，和 $O(L^2)$ 个运算，成功概率为 $O(1)$.

过程

(1) $|0\rangle|0\rangle$ // 初态

(2) $\rightarrow \frac{1}{\sqrt{2^t}}\sum_{x=0}^{2^t-1}|x\rangle|0\rangle$ // 产生叠加

(3) $\rightarrow \frac{1}{\sqrt{2^t}}\sum_{x=0}^{2^t-1}|x\rangle|f(x)\rangle$ // 应用 U

$$\approx \frac{1}{\sqrt{r2^t}}\sum_{l=0}^{r-1}\sum_{x=0}^{2^t-1}e^{2\pi ilx/r}|x\rangle|\hat{f}(l)\rangle$$

(4) $\rightarrow \frac{1}{\sqrt{r}}\sum_{l=0}^{r-1}|\widetilde{l/r}\rangle|\hat{f}(l)\rangle$ // 对第一寄存器应用逆 Fourier 变换

(5) $\rightarrow l/r$ // 测量第一寄存器

(6) $\rightarrow r$ // 应用连分式算法

掌握这个基于相位估计,并和量子求阶算法基本相同的算法的关键是第 3 步,其中我们引入了状态

$$|\hat{f}(l)\rangle \equiv \frac{1}{\sqrt{r}}\sum_{x=0}^{r-1}e^{-2\pi ilx/r}|f(x)\rangle \tag{5.63}$$

它是$|f(x)\rangle$的 Fourier 变换. 第 3 步中的等式基于

$$|f(x)\rangle = \frac{1}{\sqrt{r}}\sum_{l=0}^{r-1}e^{2\pi ilx/r}|\hat{f}(l)\rangle \tag{5.64}$$

注意 x 是 r 的整倍数时,$\sum_{l=0}^{r-1}e^{2\pi ilx/r}=r$,其他情况为 0 时,容易验证此式. 第 3 步中的等式需要近似,因为 2^t 一般不是 r 的整倍数(不必为整数倍,这是相位估计的界保证的). 由式(5.22),第 4 步应用逆 Fourier 变换到第一寄存器,给出相位 l/r 的一个估计,其中 l 是随机选取的. r 可在最后一步用连分式展开有效计算得到.

为什么这样做是对的? 理解这一点的一条途径是认识到式(5.63)是$|f(x)\rangle$在$\{0,1,\cdots,2^L-1\}$上的 Fourier 变换的一个近似(见练习 5.20),且 Fourier 变换具有盒子 5.5 描述的有趣而有用的移不变性质. 另一条途径是看到求阶算法所做的正是求函数 $f(x)=x^r \bmod N$ 的周期,因而求一般周期函数周期的能力也就不足为奇了. 另外就是意识到黑箱 U 可以自然地用特征向量,恰好是$|\hat{f}(l)\rangle$的某个酉算子来实现,如下面练习 5.21 所示,这样 5.2 节的相位估计过程就能用上了.

盒子 5.5　Fourier 变换的移不变性质

Fourier 变换，式(5.1)，有一个有趣而且非常有用的性质，称为移不变性质. 为使用描述这个性质更一般应用的记号，让我们把量子 Fourier 变换描述为

$$\sum_{h\in H} a_h \mid h\rangle \rightarrow \sum_{g\in G} \tilde{a}_g \mid g\rangle \tag{5.65}$$

其中 $\tilde{a}_g = \sum_{h\in H} a_h \exp(2\pi i g h / \mid G \mid)$，$H$ 是 G 的某个子集，G 是 Hilbert 空间标准正交基状态的指标集. 例如，对 n 量子比特系统，G 可以是从 0 到 $2^n - 1$ 的数的集合，$\mid G$ 表示 G 中元素的个数. 设我们对初态应用执行酉变换

$$U_k \mid g\rangle = \mid g + k\rangle \tag{5.66}$$

的算子 U_k，然后应用 Fourier 变换，其结果

$$U_k \sum_{h\in H} a_h \mid h\rangle = \sum_{h\in H} a_h \mid h + k\rangle \rightarrow \sum_{g\in G} e^{2\pi i g k / \mid G \mid} \tilde{a}_g \mid g\rangle \tag{5.67}$$

不管 k 是什么，$\mid g\rangle$ 幅度的大小都不变，即 $\mid \exp(2\pi i g k / \mid G \mid)\tilde{a}_g \mid = \mid \tilde{a}_g \mid$. 以群论的语言说，$G$ 是一个群，H 是 G 的一个子群，如果一个 G 上的函数 f 在 H 的陪集上是常数，那我们说 f 的 Fourier 变换在 H 的陪集上是不变的.

练习 5.20　设 $f(x+r) = f(x)$，且 $0 \leqslant x < N$，N 是 r 的一个整倍数，计算

$$\tilde{f}(l) \equiv \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i l x / N} f(x) \tag{5.68}$$

并将此结果与式(5.63)联系起来，其中用到事实

$$\sum_{k=0,r,2r,\cdots,N-r} e^{2\pi i k l / N} = \begin{cases} N/r, & l \text{ 是 } N/r \text{ 的整倍数} \\ 0, & \text{其他} \end{cases} \tag{5.69}$$

练习 5.21(求周期与相位估计)　设为上述周期函数给定一个执行变换 $U_y \mid f(x)\rangle = \mid f(x+y)\rangle$ 的酉算子 U_y.

(1) 证明 U_y 的特征向量是 $\mid \tilde{f}(l)\rangle$，并计算其特征值.

(2) 证明对某个 x_0 给定 $\mid f(x_0)\rangle$，U_y 可被用来实现和求周期问题中的 U 一样有用的黑箱.

5.4.2　离散对数问题

我们刚考虑的求周期问题是一个简单的问题，因为周期函数的定义域和值域是整数. 当函数更复杂时会怎样？考虑函数 $f(x_1, x_2) = a^{x_1 + x_2} \bmod N$，其中所有变量都是整数，$r$ 是使得 $a^r \bmod N = 1$ 的最小正整数. 这个函数是周期的，因为

$f(x_1+l,x_2-ls)=f(x_1,x_2)$，但现在周期是二元的，$(l,-ls)$，其中 l 是整数. 这个函数看起来很奇怪，但它对密码系统很有用，因为确定 s 就可以解称为离散对数的问题. 离散对数的问题是：给定 a 和 $b=a^s$，s 是多少？下面是一个解这个问题的量子算法，用执行变换 $U|x_1\rangle|x_2\rangle|y\rangle \to |x_1\rangle|x_2\rangle|y\oplus f(x)\rangle$ 的量子黑箱 U 的一次计算和 $O(\lceil \log r\rceil^2)$ 个其他运算，我们假定通过前述的求阶算法，已经知道使得 $a^r \bmod N=1$ 的最小的 $r>0$.

算法 离散对数

输入 (1)对 $f(x_1,x_2)=b^{x_1}a^{x_2}$，执行运算 $U|x_1\rangle|x_2\rangle|y\rangle=|x_1\rangle|x_2\rangle|y\oplus f(x_1,x_2)\rangle$ 的黑箱；(2)一个初始化为 $|0\rangle$ 的存储函数值的状态；(3)初始化为 $|0\rangle$ 的两个 $t=O(\lceil \log r\rceil+\log(1/\epsilon))$ 量子比特寄存器.

输出 最小正整数 s，使得 $a^s=b$.

运行时间 用到一次 U，和 $O(\lceil \log r\rceil^2)$ 个运算，成功的概率是 $O(1)$.

过程

(1) $|0\rangle|0\rangle|0\rangle$ // 初态

(2) $\to \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|0\rangle$ // 产生叠加

(3) $\to \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|f(x_1,x_2)\rangle$ // 应用 U

$$\approx \frac{1}{2^t\sqrt{r}}\sum_{l_2=0}^{r-1}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}e^{2\pi i(sl_2x_1+l_2x_2)/r}|x_1\rangle|x_2\rangle|\hat{f}(sl_2,l_2)\rangle$$

$$=\frac{1}{2^t\sqrt{r}}\sum_{l_2=0}^{r-1}\Big[\sum_{x_1=0}^{2^t-1}e^{2\pi i(sl_2x_1)/r}|x_1\rangle\Big]\Big[\sum_{x_2=0}^{2^t-1}e^{2\pi i(l_2x_2)/r}|x_2\rangle\Big]|\hat{f}(sl_2,l_2)\rangle$$

(4) $\to \frac{1}{\sqrt{r}}\sum_{l_2=0}^{r-1}|\widetilde{sl_2/r}\rangle|\widetilde{l_2/r}\rangle|\hat{f}(sl_2,l_2)\rangle$ // 应用逆 Fourier 变换到前两个寄存器

(5) $\to (\widetilde{sl_2/r},\widetilde{l_2/r})$ // 测量前两个寄存器

(6) $\to s$ // 应用推广的连分式算法

同样，理解这个算法的关键在第 3 步，在第 3 步引入状态

$$|\hat{f}(l_1,l_2)\rangle=\frac{1}{\sqrt{r}}\sum_{j=0}^{r-1}e^{-2\pi il_2j/r}|f(0,j)\rangle \tag{5.70}$$

它是 $|f(x_1,x_2)\rangle$ 的 Fourier 变换(练习 5.22). 此式中，l_1 和 l_2 的值必须满足

$$\sum_{k=0}^{r-1}e^{2\pi ik((l_1/s)-l_2)/r}=r \tag{5.71}$$

否则 $|\hat{f}(l_1,l_2)\rangle$ 的幅度将近于 0. 最后一步推广的连分式展开来，以 5.3.1 节类似

的方式确定 s，这留作一个简单练习.

练习 5.22　证明

$$|\tilde{f}(l_1,l_2)\rangle = \sum_{x_1=0}^{r-1}\sum_{x_2=0}^{r-1} e^{2\pi i(l_1x_1+l_2x_2)/r}|f(x_1,x_2)\rangle$$

$$= \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{2\pi i l_2 j/r}|f(0,j)\rangle \tag{5.72}$$

且这个表达式不为零的限制条件是，$(l_1/s)\ l_2$ 是 r 的整倍数.

练习 5.23　用式(5.70)计算

$$\frac{1}{r}\sum_{l_1=0}^{r-1}\sum_{l_2=0}^{r-1} e^{2\pi i(l_1x_1+l_2x_2)/r}|\tilde{f}(l_1,l_2)\rangle \tag{5.73}$$

且证明结果是 $f(x_1,x_2)$.

练习 5.24　建立离散对数算法第 6 步需要的，从 sl_2/r 和 l_2/r 的估计确定 s 的推广的连分式算法.

练习 5.25　为用于量子离散对数算法的黑箱 U 构造一个量子线路，该黑箱以 a 和 b 为参数，执行酉变换 $|x_1\rangle|x_2\rangle|y\rangle \rightarrow |x_1\rangle|x_2\rangle|y\oplus b^{x_1}a^{x_2}\rangle$，需要多少基本运算?

5.4.3　隐含子群问题

到现在，有一个模式清楚起来：若给定一个周期函数，即使周期的结构相当复杂，我们还是常能有效地确定周期. 然而，重要的是，并非所有周期函数的周期都能被确定. 这样问题的一般性的框架，可以简洁地用群论(参看附录 B 的简短概述)语言表达如下.

令 f 是一个从有限生成群 G 到有限集合 X 的函数，满足 f 在子群 K 的陪集上是定常，且在每个陪集上不同. 给定一个对 $g\in G, h\in X$ 和适当选取的 X 上的二元运算$\ominus$，执行酉变换 $U|g\rangle|h\rangle = |g\rangle|h\ominus f(g)\rangle$ 的量子黑箱，求 K 的一个生成集.

求阶、求周期、离散对数和许多其他问题都是这个隐含子群问题的实例，图 5.5 列出了一些有趣例子.

对一个有限的 Abel 群 G，量子计算机可以用 $\log|G|$ 多项式数目的运算和一次黑箱函数计算，以非常类似本节中其他问题的方法求解隐含子群问题(事实上，用类似的思路解有限生成的 Abel 群问题也是可以的，但这里我们关注有限例子). 我们把算法细节的描述留作练习，说明基本思路后，练习应该是容易的. 算法的许多方面本质上是一样的，因为有限 Abel 群同构于模算术中整数的加法群的积. 这意味着 G 上的量子 Fourier 变换是定义良好的(参看 B.3 节)，且仍可以有效计算. 算法的第一个重要步骤是用 Fourier 变换(推广了 Hadamard 运算)产生群元的一个叠加，在接下来的步骤中，该叠加在 f 的黑箱作用下变换为

$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle|f(g)\rangle \tag{5.74}$$

像以前一样，我们要在 Fourier 基下重写$|f(g)\rangle$. 我们从

$$|f(g)\rangle=\frac{1}{\sqrt{|G|}}\sum_{l=0}^{|G|-1}e^{2\pi ilg/|G|}|\tilde{f}(l)\rangle \tag{5.75}$$

开始，其中我们选择 $\exp[-2\pi ilg/|G|]$作为 $g\in G$ 的一个以 l 为指标(Fourier 变换把群元映射到其表示：参看练习 B.23)的表示(参看练习 B.13). 关键在于认识到这个表达式可以化简，因为 f 在 K 的不同陪集上是定常的，于是

名 称	G	X	K	函 数
Detsch	$\{0,1\},\oplus$	$\{0,1\}$	$\{0\}$ or $\{0,1\}$	$K=\{0,1\}$: $\begin{cases}f(x)=0\\f(x)=1\end{cases}$ $K=\{0\}$: $\begin{cases}f(x)=x\\f(x)=1-x\end{cases}$
Simon	$\{0,1\}^n,\oplus$	任意有限集	$\{0,s\}$ $s\in n\{0,1\}^n$	$f(x\oplus s)=f(x)$
求周期	$Z,+$	任意有限集	$\{0,r,2r,\cdots\}$ $r\in G$	$f(x+r)=f(x)$
求阶	$Z,+$	$\{a^j\},j\in Z_r$ $a^r=1$	$\{0,r,2r,\cdots\}$ $r\in G$	$f(x)=a^x$ $f(x+r)=f(x)$
离散对数	$Z_r\times Z_r$ $+(\mathrm{mod}\ r)$	$\{a^j\},j\in Z_r$ $a^r=1$	$(l,-ls)$ $l,s\in Z_r$	$f(x_1,x_2)=a^{lx_1+x_2}$ $f(x_1+l,x_2-ls)=f(x_1,x_2)$
置换的阶	$Z_{2^m}\times Z_{2^n}$ $+(\mathrm{mod}\ 2^m)$	Z_{2^n}	$\{0,r,2r,\cdots\}$ $r\in X$	$f(x,y)=\pi^x(y)$ $f(x+r,y)=f(x,y)$ $\pi=X$ 上的置换
隐含线性函数	$Z\times Z,+$	Z_N	$(l,-ls)$ $l,s\in X$	$f(x_1,x_2)=$ $\pi(sx_1+x_2\mathrm{mod}\ N)$ $\pi=X$ 上的置换
Abel 稳定子	(H,X) $H=$任意 Abel 群	任意有限集	$\{s\in H\mid$ $f(s;x)=x$ $\forall x\in X\}$	$f(gh,x)=f(g,f(h,x))$ $f(gs,x)=f(g,x)$

图 5.5 隐含子群问题. 函数 f 从群 G 映射到有限集 X，且在隐含子群 $K\subseteq G$ 的陪集上为定常，Z_N 在这表中表示集合$\{0,1,\cdots,N-1\}$，而 Z 是整数集. 问题是给定计算 f 的黑箱，求 K(或它的一个生成集).

$$|\tilde{f}(l)\rangle=\frac{1}{\sqrt{|G|}}\sum_{g\in G}e^{-2\pi ilg/|G|}|f(g)\rangle \tag{5.76}$$

对 l 的一切值都具有近于 0 的幅度，除了那些满足

$$\sum_{h\in K}e^{-2\pi ilh/|G|}=|K| \tag{5.77}$$

的 l 以外.

如果我们能确定 l，则用这个表达式给出的线性约束可使我们确定 K 的元，并且因为 K 是 Abel 的，这允许我们为隐含子群最终确定一个生成集合，从而解决该问题.

然而，问题并不总是这么简单. 求周期和离散对数算法之所以可行，是因为连分式展开可成功地从 $l/|G|$ 得到 l，在这些问题里，l 和 $|G|$ 没有公因子的概率很高. 不过一般情况下，这不一定是真的，因为 $|G|$ 完全可以是一个含有很多因子的合数，并且我们没有关于 l 的任何有用的先验知识.

幸运的是，这个问题可以得到解决：如上面提到的，任何有限 Abel 群 G 同构于素幂阶循环群的积，即，$G=Z_{p_1}\times Z_{p_2}\times\cdots\times Z_{p_M}$，其中 p_i 都是素数，而 Z_{p_i} 是整数 $\{0,1,\cdots,p_i-1\}$ 上的，以模 p_i 加为群运算的群. 我们可以把式(5.75)中的相位对 $g_i\in Z_{p_i}$ 重新表达为

$$e^{2\pi i k\cdot l/r}=\prod_{i=1}^{M}e^{2\pi i l'_i g_i/p_i} \tag{5.78}$$

现在相位估计过程就给出 l'_i，据此我们可定出 l，于是如上面所描述去尝试采样 K，从而解决隐含子群问题.

练习 5.26　因为 K 是 G 的一个子群，当我们把 G 分解为素幂阶循环群的乘积时，也分解了 K. 重新表达式(5.77)，证明为确定 l'_i，可以在对应于 K 的循环子群 K_{p_i} 中采样.

练习 5.27　当然，一般有限 Abel 群 G 到素幂阶循环子群积的分解，是一个困难的问题(例如至少和整数分解因子一样困难). 这里，可以用量子算法再次补救：说明用本章的算法，如何有效地按期望方式分解 G.

练习 5.28　详细写出对有限 Abel 群解隐含子群问题的量子算法，并补充运行时间和成功概率的估计.

练习 5.29　采用隐含子群问题的框架，给出解图 5.5 列出的 Deutsch 问题和 Simon 问题的量子算法.

5.4.4　其他量子算法

描述隐含子群问题的量子算法的框架最迷人的一个地方，就是它暗示通过考虑不同的群 G 和函数 f，来解决更困难的问题. 我们只考虑了这个问题对 Abel 群的解，对非 Abel 群怎样？这些群很有趣(参看附录 B，对非 Abel 群上一般 Fourier 变换的讨论)：例如，图同构问题是，确定两个给定的图在 n 个顶点的标号的某个置换下是否相同(3.2.3 节). 这些置换可以描述为对称群 S_n 中的变换，并且在这些群上进行快速 Fourier 变换的算法是存在的. 然而，尚不知道解图同构问题的有效算法.

即使在量子计算机上，还是无法解决隐含子群问题的更一般情形，有这样一个统一的框架仍然是有用的，因为它使我们能够提出如何跨出限制的问题，很难相信所有可能发现的快速量子算法仅仅是解隐含子群问题. 如果我们把这些问题看作基于

Fourier 变换的陪集不变性质，那么在寻找新算法时，或许要做的事情是考察具有别的不变量的其他变换. 在另外的方向上，我们可以问：如果借助于任意给定的量子状态(但要独立于问题)，可以有效解决哪些难的隐含子群问题？毕竟如第 4 章所述，构造大多数量子状态实际上是指数量级难度的. 如果真有量子算法利用它们来解难的问题，那么这样的状态将是一种有用的资源(一个真实的量子 oracle).

隐含子群问题也刻画出一类量子算法的背后的一个重要约束条件，量子算法指数式快于它们的(已知的)经典对应物，这是一个带许诺的问题，指的是它是具有形式"$F(X)$许诺具有某性质：刻画该性质."相当令人失望的是，我们将在下章末说明，在求解不具有某种许诺的问题时，量子计算机将不能对经典计算机进行指数加速，最好的加速是多项式的. 另一方面，这给我们一条量子计算机擅长解决什么类型问题的重要线索：回顾起来，隐含子群问题可以视为量子计算的一个自然的候选对象. 还有哪些自然的问题？让我们一起来思考吧.

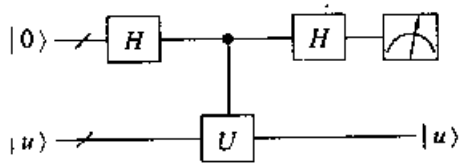
问题 5.1 构造量子 Fourier 变换

$$|j\rangle \rightarrow \frac{1}{\sqrt{p}}\sum_{k=0}^{p-1} e^{2\pi ijk/p}|k\rangle \tag{5.79}$$

的一个量子线路，p 是素数.

问题 5.2(被测量的量子 Fourier 变换) 设量子 Fourier 变换是量子计算的最后一步，接着是在计算基中的测量. 证明量子 Fourier 变换和测量的复合，等价于一个完全由单量子比特门和测量，以及经典控制组成而没有双量子比特门的量子线路. 读者也许会发现 4.4 节的讨论是有用的.

问题 5.3(Kitaev 算法) 考虑如图量子线路



其中$|u\rangle$是 U 的对应特征值 $e^{2\pi i\varphi}$的一个本征态. 证明顶上的量子比特以 $p=\cos^2(\pi\varphi)$概率测得 0. 因为状态$|u\rangle$不受线路影响，它可以重复使用，若用 U^k 代替 U，其中 k 是在控制之下的任意整数，证明通过重复这个线路和适当增加 k，可以有效地获得所期望的 p 的任意多比特，于是可以得到 φ 的任意多比特. 这是另外一种相位估计算法.

问题 5.4 我们给出的因子分解算法的界 $O(L^3)$是不严格的，证明可以达到一个更好的上界 $O(L^2\log L\log\log L)$.

*** 问题 5.5(非 Abel 隐含子群)** 令 f 是有限群 G 到任意有限值域 X 的一个函数，且 f 许诺在子群 K 的不同的左陪集上为定常且不同. 从状态

$$\frac{1}{\sqrt{|G|^m}}\sum_{g_1,\cdots,g_m}|g_1,\cdots,g_m\rangle|f(g_1),\cdots,f(g_m)\rangle \tag{5.80}$$

开始，证明选择 $m=4\log|G|+2$，可以使我们以至少 $1-1/|G|$ 的概率识别出 K，注意 G 不必是 Abel 的，也不需要在 G 上做 Fourier 变换. 这个结果表明，我们可以（仅用 $O(\log|G|)$ 次 oracle 调用）产生一个对应于可能的不同隐含子群的纯状态，输出近乎正交的最终结果. 然而，尚不知道是否存在允许从这个最终状态有效（即利用 $\mathrm{poly}(\log|G|)$ 个运算）识别隐含子群的 POVM.

问题 5.6（采用 Fourier 变换的加法）　考虑构造量子线路计算 $|x\rangle \rightarrow |x+y \bmod 2^n\rangle$ 的任务，其中 y 是一个固定的常数，且 $0\leqslant x<2^n$. 证明对 y 的值，比如 1，完成这个任务的一个有效途径，是首先进行量子 Fourier 变换，然后应用单量子比特的相位移动，再进行逆 Fourier 变换. 对什么样的 y 值用这种加法是容易的，需要多少次运算？

第 5 章的总结　量子 Fourier 变换及其应用

- 当 $N=2^n$ 时，量子 Fourier 变换

$$|j\rangle=|j_1,\cdots,j_n\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\mathrm{e}^{2\pi ijk/N}|k\rangle \tag{5.81}$$

可以写成形式

$$|j\rangle \rightarrow \frac{1}{2^{n/2}}(|0\rangle+\mathrm{e}^{2\pi i 0.j_n}|1\rangle)(|0\rangle+\mathrm{e}^{2\pi i 0.j_{n-1}j_n}|1\rangle)\cdots(|0\rangle+\mathrm{e}^{2\pi i 0.j_1 j_2\cdots j_n}|1\rangle) \tag{5.82}$$

且可用 $\Theta(n^2)$ 个门实现.

- **相位估计**：令 $|u\rangle$ 是算子 U 的对应特征值 $\mathrm{e}^{2\pi i\varphi}$ 的一个本征态. 从初态 $|0\rangle^{\otimes t}|u\rangle$ 开始，给定对整数 k 有效计算 U^{2^k} 的能力，该算法（图 5.3 所示）可用来有效地获得状态 $|\tilde{\varphi}\rangle|u\rangle$，其中 $\tilde{\varphi}$ 以至少 $1-\epsilon$ 的概率精确到 $t-\left\lceil \log\left(2+\frac{1}{2\epsilon}\right)\right\rceil$ 位，来近似 φ.

- **求阶问题**：x 模 N 的阶是使得 $x^r \bmod N=1$ 的最小正整数. 用量子相位估计算法，对 L 比特的整数 x 和 N，可以用 $O(L^3)$ 次运算计算这数.

- **因子问题**：L 比特整数 N 的素因子可以通过把此问题归结为求一个与 N 互质的随机数 x 的阶的问题，用 $O(L^3)$ 次运算确定.

- **隐含子群问题**：所有已知的快速量子算法都可以描述为解下述问题：令 f 为从一个有限生成的群 G 到一个有限集 X 的函数，使得 f 在子群 K 的陪集上是定常，且在每个陪集上不同. 给定一个对 $g\in G$ 和 $h\in X$，执行酉变换 $U|g\rangle|h\rangle=|g\rangle|h\oplus f(g)\rangle$ 的量子黑箱，求 K 的一个生成集.

历史和进一步阅读的材料

Fourier 变换的定义可以推广到本章考虑的范围以外. 在一般场合下 Fourier 变换定义在一组复数 a_g 上,其中指标 g 选自某个群 G. 本章中我们把 G 选为整数的模 2^n 加群,常记作 Z_{2^n}. Deutsch[Deu85]证明群 Z_{2^n} 上的 Fourier 变换可以在量子计算机上有效实现,这就是前些章中的 Hadamard 变换. Shor[Sho94]意识到量子计算机的可观的作用能对某些特定的 m 值,能有效实现群 Z_m 上的量子 Fourier 变换. 受这个结果启发,Coppersmith[Cop94],Deutsch(未发表)和 Cleve(未发表)给出我们在本章中用的 Z_{2^n} 上量子 Fourier 变换的简单量子线路. Cleve、Ekert、Machiavello 和 Mosca[CEMM98],以及 Griffiths 和 Niu[GN96]独立地发现张量积公式(5.4),事实上,这个结果很早以前就被 Danielson 和 Lanczos 认识到. 式(5.5)开始的简化证明是 Zhou 建议的. Griffiths 和 Niu[GN96]给出了问题 5.2 中的带测量的量子 Fourier 变换.

Kitaev[Kit95]将 Z_{2^n} 上的 Fourier 变换推广到任意有限 Abel 群,并同时给出问题 5.3 中的相位估计过程. Cleve、Ekert、Macchiavello 和 Mosca[CEMM98]将 Shor 和 Kitaev 引入的方法集成在一起,成为 5.2 节的基础. Mosca 的博士论文很好地描述了相位估计算法[Mos99].

Shor 在 1994 年的原始论文[Sho94]宣布了量子求阶算法,并注意到离散对数和因子问题可以归结为求阶问题,他最终的论文,包括广泛的讨论和丰富的文献,于 1997 年发表[Sho97]. 这篇文章还包含对乘法进行巧妙计算的讨论,甚至可进一步加速相对简单的乘法的算法. 利用这些快速乘法,一个合数 n 分解因子需要的资源的规模,如在本章引论所断言的,为 $O(n^2 \log n \log\log n)$. 1995 年 Kitaev[Kit95]宣布了一个求一般 Abel 群稳定子的算法,他证明该算法可把求离散对数和因子作为特殊情况来求解,而且,这个算法包含 Shor 算法中没有的一些内容. 求因子算法的很好综述见 Ekert 和 Jozsa[EJ96],也可以参看 DiVincenzo[DiV95a]. 连分式的讨论基于 Hardy 和 Wright[HW60]的第 10 章. 在本书写作的时候,在经典计算机上最有效的经典因子分解算法是数域筛法,这在 A. K. Lenstra 和 H. W. Lenstra, Jr. 编辑的文集[LL93]中有描述.

许多学者考虑过把量子算法推广到解隐含子群问题. 从历史上看,Simon 首先注意到,量子算法可以求满足 $f(x \oplus s) = f(x)$ 的函数的隐含周期[Sim94, Sim97]. 事实上,Shor 通过推广 Simon 的结果,并用 Z_N 上的 Fourier 变换来代替 Simon 的 Hadamard 变换(Z_2^n 上的一种 Fourier 变换),而得到自己的结果. 接着 Boneh 和

Lipton 注意到量子算法和隐含子群问题的联系，并给出一个解隐含线性函数问题的量子算法[Lip91]. Jozsa 首先给出 Deutsch-Jozsa、Simon 和 Shor 算法的在隐含子群形式下的统一描述[Joz97]. Ekert 和 Jozsa 对 Abel 和非 Abel 快速 Fourier 变换算法在量子算法加速方面的研究[EJ98]，也很富启发性. 我们在 5.4 节中对隐含子群问题的阐述是按照 Mosca 和 Ekert[EM99, Mos99]的框架. Cleve 证明求一个置换的阶的问题在一台有界误差概率经典计算机上，需要指数次计算[Cle99]. Ettinger 和 Høyer[EH99]，Roetteler 和 Beth[RB98]，Pueschel，Roetteler 和 Beth[PRB98]，Beals[Bea97]（还描述了在对称群上量子 Fourier 变换的构造），以及 Ettinger，Høyer 和 Knill[EHK99]都试图将这种方法推广到 Abel 群以外. 这些结果表明，到目前为止，对求非 Abel 群的隐含子群的问题存在仅利用 $O(\log|G|)$ 次 oracle 调用的量子算法，但这是否可以在多项式时间内实现尚不清楚（问题 5.5）.

CHAPTER 6

第 6 章 量子搜索算法

假设我们希望在一张给定的包含许多城市的地图上，确定经过所有城市的最短路径，寻找这样路径的一个简单算法是，遍历经过这些城市的所有路径，并保持具有最短长度路径的动态记录. 在一台经典计算机上，假设有 N 条可能路径，用这种方法显然可以用 $O(N)$ 次运算可以决定最短路径. 引人瞩目的是，存在量子搜索算法，有时称为 Grover 算法，可以对这种搜索算法进行实质性的加速，只需要 $O(\sqrt{N})$ 次操作. 而且，这个量子搜索算法可以加速许多(虽不是全部)启发式搜索的经典算法，这些远比刚描述的路径搜索的例子广得多，在这个意义下，它是通用的.

本章首先阐述量子搜索算法. 6.1 节描述基本算法. 6.2 节基于 4.7 节的量子仿真算法，从另一角度推导该算法. 接着介绍该算法的三个重要应用：6.3 节是量子计数，6.4 节是 NP 完全问题求解的加速，6.5 节是非结构化数据库的搜索. 人们或许会希望改进搜索算法，比二次加速做得更好，但 6.6 节证明事实上这是不可能的. 最后 6.7 节证明这个速度上的限制适用于大多数非结构化问题.

6.1 量子搜索算法

像 3.1.1 节中那样，我们首先引人基于黑箱(oracle)的搜索算法，这样就能给出搜索过程的非常一般的描述，并能用几何方式形象地表示它的步骤和执行方式.

6.1.1 oracle

假设在 N 个元素的搜索空间中进行搜索. 我们不直接搜索元素，而是把注意力放在那些元素的指标上，指标对应于从 0 到 $N-1$ 的数字. 为方便起见，假定 $N=2^n$，于是指标可以存储在 n 个比特中. 进而假设搜索问题恰好有 M 个解，

$1 \leqslant M \leqslant N$. 搜索问题的一个特例可以方便地表为一个输入 x 的函数 f，x 是从 0 到 $N-1$ 的整数，f 的定义是，若 x 是搜索问题的一个解 $f(x)=1$，而如果 x 不是搜索问题的解，则 $f(x)=0$.

设有一个量子 oracle 可以识别搜索问题的解，Oracle 的内部工作方式将在后面讨论，识别的结果通过 oracle 的一个量子比特给出. 更确切地，这个 oracle 是一个酉算子 O，根据在计算基上的作用定义

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle \tag{6.1}$$

其中 $|x\rangle$ 是一个指标寄存器，$\oplus$ 表示模 2 加法，oracle 的量子比特 $|q\rangle$ 是一个单量子比特，当 $f(x)=1$ 时翻转，否则不变. 我们可以通过制备 $|x\rangle|0\rangle$，应用 oracle，检查 oracle 量子比特是否翻转到 $|1\rangle$，来判断 x 是否为搜索问题的一个解.

在量子搜索算法中，正像 1.4.4 节中 Deutsch-Jozsa 算法中所做的，在 oracle 量子比特初始化为 $(|0\rangle-|1\rangle)/\sqrt{2}$ 时，应用 oracle 是有用的. 若 x 不是搜索算法的解，应用 oracle 到状态 $|x\rangle(|0\rangle-|1\rangle)/\sqrt{2}$，并不改变状态；另一方面，如果 x 是搜索算法的解，则 $|0\rangle$ 和 $|1\rangle$ 在 oracle 的作用下相交换，给出终了状态 $-|x\rangle(|0\rangle-|1\rangle)/\sqrt{2}$. 于是 oracle 的作用是

$$|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \xrightarrow{O} (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \tag{6.2}$$

注意 oracle 量子比特的状态没有改变. 事实上这个量子比特将在量子搜索算法过程中保持为 $(|0\rangle-|1\rangle)/\sqrt{2}$，为了简化描述，可以在下面算法的讨论中省略.

在这个约定下，oracle 的作用可以写成

$$|x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle \tag{6.3}$$

我们说 oracle 通过改变解的相位，标记了搜索问题的解. 对有 M 个解的 N 元搜索问题，实际上为得到一个解，只需要在量子计算机上应用搜索 oracle $O(\sqrt{N/M})$ 次.

这种不描述 oracle 实际上如何工作的讨论是相对抽象的，甚至或许让人迷惑. 表面上看 oracle 好像已经知道了搜索问题的解，这种基于 oracle 查询的量子搜索算法能有什么用呢？答案是，知道搜索问题的解和能识别解是有区别的，关键在于有可能在不需要知道解的情况下识别解.

因子问题是说明这一点的一个简单例子. 设有一给定的大数 m，并被告知它是两个素数 p 和 q 的乘积——同样的情形会出现在试图破解 RSA 公钥密码系统时（附录 E）. 为确定 p 和 q，经典计算机上显然的办法是搜索从 2 到 $m^{1/2}$ 的所有数，以找到两个素因子中较小的一个，即，我们连续地用在 2 到 $m^{1/2}$ 范围内的每个数去试除 m，直到找到较小的素因子，另一个素因子可以通过 m 除以较小的素因子得到.

显然，这种基于搜索的方法在经典计算机上需要大约 $m^{1/2}$ 次试除，以找到因子.

量子搜索算法可以用于加速这个过程. 由定义，oracle 在输入状态 $|x\rangle$ 上的作用是用 x 除 m，并且检查是否可以除尽，如果是，就翻转 oracle 比特. 利用这个 oracle 的量子搜索算法，可以以很大的概率给出两个素因子中较小的一个，但为使算法能够工作，我们需要构造 oracle 的一个有效线路实现. 如何做到这一点是可逆计算的一个练习. 我们根据定义，若 x 整除 m，则函数 $f(x)\equiv 1$，否则 $f(x)=0$ 开始，$f(x)$ 告诉我们试除是否成功. 利用 3.2.5 节的可逆计算技术，通过改造用于试除的通常(不可逆)的经典电路，构造一个经典可逆电路，把 (x,q)——表示初始设为 x 的输入寄存器和初始设为 q 的一个比特的输出寄存器——变为 $(x,q\oplus f(x))$. 这个可逆电路的资源消耗在试除的不可逆经典电路的两倍以内，故我们认为两个电路本质上消耗同样的资源. 进一步，经典可逆电路可立即翻译成 oracle 所要求的，把 (x,q) 变为 $(x,q\oplus f(x))$ 的量子线路. 关键的思路在于，即使不知道 m 的因子，我们也可以具体构造一个可以识别搜索问题解的 oracle. 利用这个 oracle 和量子搜索算法，可以用 $O(m^{1/4})$ 的 oracle 查询搜索 2 到 $m^{1/2}$ 的范围，也就是，我们大致需要进行 $m^{1/4}$ 次试除，而不像经典算法的 $m^{1/2}$ 次.

求因子的例子只有概念上的而非实际上的意义：存在比遍历所有可能除数快得多的经典求因子算法. 不过，它说明了应用量子搜索算法的一般模式：基于搜索技术的经典算法可以被量子搜索算法加速. 本章后半部分考察量子搜索算法确实有助于加速 NP 完全问题的求解的情形.

6.1.2 过程

搜索算法运行的框架如图 6.1 所示，算法使用一个单个的 n 量子比特寄存器. oracle 的内部工作，包括它可能需要的附加工作量子比特，对描述量子搜索算法本身并不重要. 算法的目的是用最少的 oracle 应用次数求出搜索问题的一个解.

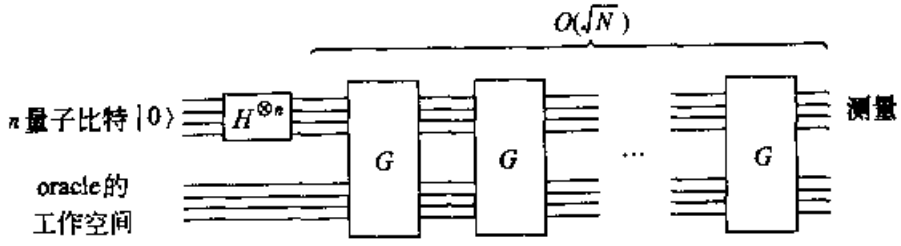


图 6.1 量子搜索算法的线路框架. 为实现 oracle 可能用到工作量子比特，但量子搜索算法的分析只涉及 n 量子比特寄存器.

算法从计算机的初态 $|0\rangle^{\otimes n}$ 开始，用 Hadamard 变换使计算机处于均衡叠加态

$$|\psi\rangle = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle \tag{6.4}$$

量子搜索算法由反复应用记作 G 的称为 Grover 迭代(Grover iteration)或 Grover 算子的量子子程序组成. Grover 迭代的量子线路如图 6.2 所示，可分成四步.

(1) 应用 oracle O;

(2) 应用 Hadamard 变换 $H^{\otimes n}$;

(3) 在计算机上执行条件相移，使$|0\rangle$以外的每个计算基态获得 -1 的相位移动

$$|x\rangle \rightarrow -(-1)^{\delta_{x0}}|x\rangle \tag{6.5}$$

(4) 应用 Hadamard 变换 $H^{\otimes n}$.

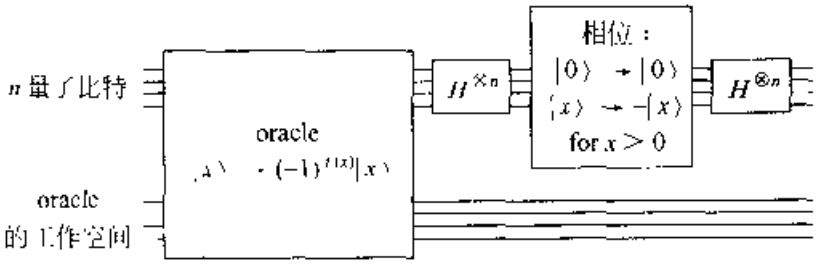


图 6.2　Grover 迭代 G 的线路.

练习 6.1　证明对应于 Grover 迭代中，相移的酉算子是 $2|0\rangle\langle 0| - I$.

Grover 迭代中的每个运算都可在量子计算机上有效实现，第 2 步和第 4 步的 Hadamard 变换各需要 $n = \log(N)$次运算. 第 3 步的条件相移可用 4.3 节的技术实现，只用 $O(n)$个门. oracle 调用的消耗依赖特定的应用，这个例子中 Grover 迭代只需要一个单 oracle 调用. 注意第 2,3,4 步结合的效果为

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I \tag{6.6}$$

其中$|\psi\rangle$是式(6.4)中的均衡叠加态. 于是 Grover 迭代 G 可以写成 $G = (2|\psi\rangle\langle\psi| - I)O$.

练习 6.2　证明应用运算$(2|\psi\rangle\langle\psi| - I)$到一般状态$\sum_k \alpha_k |k\rangle$产生

$$\sum_k [-\alpha_k + 2\langle\alpha\rangle]|k\rangle \tag{6.7}$$

其中$\langle\alpha\rangle \equiv \sum_k \alpha_k / N$是 α_k 的均值，因此，$(2|\psi\rangle\langle\psi| - I)$有时称为关于均值的反演(inversion about mean)运算.

6.1.3　几何可视化

Grover 迭代能做什么？注意到 $G = (2|\psi\rangle\langle\psi| - I)O$，事实上，我们将证明，Grover 迭代可视为在由开始向量$|\psi\rangle$和搜索问题解组成的均匀叠加态张成的二

维空间中的一个旋转. 为弄清这一点，采用 $\sum_x'$ 表示所有 x 上的搜索问题解的和，用 $\sum_x''$ 表示所有 x 上的非搜索问题解的和. 定义归一化状态

$$|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle \tag{6.8}$$

$$|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x' |x\rangle \tag{6.9}$$

简单的代数运算表明，初态 $|\psi\rangle$ 可重新表示为

$$|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle \tag{6.10}$$

故量子计算机的初态属于 $|\alpha\rangle$ 和 $|\beta\rangle$ 张成的空间.

通过认识到运算 O 对 $|\alpha\rangle$ 和 $|\beta\rangle$ 定义的平面上向量 $|\alpha\rangle$ 进行了一次反射，可以很巧妙地理解 G，即 $O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle$. 类似地，$2|\psi\rangle\langle\psi| - I$ 也执行了 $|\alpha\rangle$ 和 $|\beta\rangle$ 定义的平面上 $|\psi\rangle$ 的一次反射. 两个反射的积是一个旋转. 这告诉我们对所有 k，状态 $G^k|\psi\rangle$ 留在 $|\alpha\rangle$ 和 $|\beta\rangle$ 定义的平面上，同时它还给出转角. 令 $\cos\theta/2 = \sqrt{(N-M)/N}$，使得 $|\psi\rangle = \cos\theta/2\ |\alpha\rangle + \sin\theta/2\ |\beta\rangle$. 如图 6.3 所示，构成 G 的两个反射把 $|\psi\rangle$ 变为

$$G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle \tag{6.11}$$

于是转角实际上即为 θ. 由此连续应用 G，把状态变为

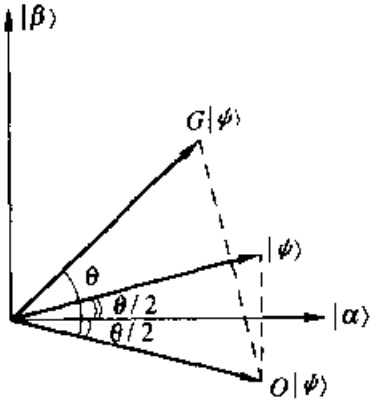


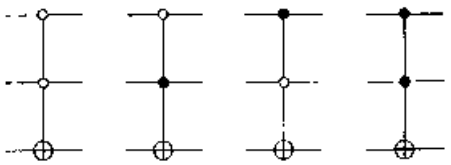
图 6.3 单次 Grover 迭代 G 的作用：状态向量朝搜索问题的所有解的叠加 $|\beta\rangle$ 转 θ 角. 开始时状态向量偏离与 $\beta\rangle$ 正交的 $|\alpha\rangle$ 状态 $\theta/2$ 角，oracle 运算 O 把状态以状态 $|\alpha\rangle$ 进行反射，接着运算 $2|\psi\rangle\langle\psi| - I$ 把它以 $|\psi\rangle$ 作反射. 图中 $|\alpha\rangle$ 和 $|\beta\rangle$ 稍加延长，以避免混乱（所有状态都应该是单位向量）. 经过反复的 Grover 迭代，状态向量接近于 $|\beta\rangle$. 在 $|\beta\rangle$ 点，在计算基中观测将以很高的概率输出搜索问题的一个解. 算法具有可观效率，是因为 θ 的作用像 $\Omega(\sqrt{M/N})$，而把状态向量转到接近 $|\beta\rangle$，只需要应用 $GO(\sqrt{N/M})$ 次.

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle - \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle \tag{6.12}$$

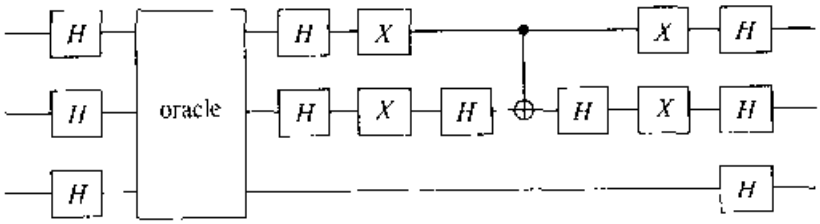
总之，G 是 $|\alpha\rangle$ 和 $|\beta\rangle$ 定义的二维空间中的一个旋转，每次应用 G，把空间旋转 θ 弧度. 反复应用 Grover 迭代，把状态向量旋转得接近 $|\beta\rangle$. 当这个时候，在计算基中的一个观测，就以很高的概率产生与 $|\beta\rangle$ 重叠的输出，即搜索问题的一个解，对 $N=4$ 的一个说明搜索算法的例子，在盒子 6.1 中给出.

盒子 6.1　量子搜索：双比特的例子

下面是说明量子搜索算法在大小为 $N=4$ 的搜索空间上，如何工作的具体例子. oracle 对除 $x=x_0$ 外的所有 x 有，$f(x)=0$，而 $f(x_0)=1$，可取为如图四种线路中的任何一种，



从左到右分别对应 $x_0=0,1,2,3$，其中顶上两个量子比特承载对 x 的查询，而底下的量子比特承载 oracle 的响应. 执行开始的 Hadamard 变换和一个单次 Grover 迭代 G 的量子线路为



起初，顶上的两个量子比特处于状态 $|0\rangle$，底下的量子比特为 $|1\rangle$. 点框中的门执行条件相移运算 $2|00\rangle\langle 00|-I$. 为得到 x_0，我们必须重复多少次 G? 从式(6.15)，利用 $M=1$，可知需要不多于一次迭代. 事实上因为在式(6.14)中 $\theta=\pi/3$，在这种特殊情况下，需要恰好一次迭代，以精确得到 x_0. 在图 6.3 的几何图像中，我们的初态 $|\psi\rangle=(|00\rangle+|01\rangle+|01\rangle+|11\rangle)/2$ 偏离 $|\alpha\rangle 30°$，并且一次的 $\theta=60°$ 旋转，把 $|\psi\rangle$ 移到 $|\beta\rangle$. 可以直接验证使用这个量子线路，应用 orcale 一次后，顶上两个量子比特的测量给出 x_0. 与之对照，经典计算机——或经典电路——为区分四种 oracle，平均需要 2.25 次 oracle 调用.

练习 6.3　证明 $|\alpha\rangle,|\beta\rangle$ 基中，可以把 Grover 迭代写成

$$G=\begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix} \tag{6.13}$$

其中 θ 是一个 0 到 2π 之间的实数(为简单起见假定 $M\leqslant N/2$,这个限制很快会取消),它满足

$$\sin\theta=\frac{2\sqrt{M(N-M)}}{N} \tag{6.14}$$

6.1.4 性能

为把$|\psi\rangle$旋转得接近$|\beta\rangle$,需要多少次 Grover 迭代?系统的初态为$|\psi\rangle=\sqrt{(N-M)/N}|\alpha\rangle+\sqrt{M/N}|\beta\rangle$,因此旋转 $\arccos\sqrt{M/N}$弧度,系统进入$|\beta\rangle$状态.令 $\mathrm{CI}(x)$记最接近实数 x 的整数,其中按习惯,我们把一半向下取整,如 $\mathrm{CI}(3.5)=3$.重复 Grover 迭代

$$\mathrm{R}=\mathrm{CI}\left(\frac{\arccos\sqrt{M/N}}{\theta}\right) \tag{6.15}$$

次,把$|\psi\rangle$旋转到离$|\beta\rangle$的 $\theta/2\leqslant\pi/4$ 的角度范围内,于是对状态在计算基中的观测,将至少以$\frac{1}{2}$的概率给出搜索问题的一个解.事实上,对 M 和 N 的特殊值可以达到高得多的成功概率.例如,当 $M\ll N$ 时,我们有 $\theta\approx\sin\theta\approx2\sqrt{M/N}$,故最终状态的角误差至多是 $\theta/2\approx\sqrt{M/N}$,给出最多为 M/N 的错误概率.注意 R 依赖于解的数目 M,但不依赖于那些解的性质,因此如果我们知道 M,就可以使用所描述的量子搜索算法.在 6.3 节中我们将说明在应用搜索算法时,如何去除知道 M 这个要求.

作为量子搜索算法调用 oracle 的精确次数的表达式,式(6.15)是有用的,但有一个概括 R 的实质行为的更简单表达式也很重要.为此,根据式(6.15)知 $R\leqslant\lceil\pi/2\theta\rceil$,因此 θ 的一个下界将给出 R 的一个上界.暂且假设 $M\leqslant N/2$,我们有

$$\frac{\theta}{2}\geqslant\sin\frac{\theta}{2}=\sqrt{\frac{M}{N}} \tag{6.16}$$

由此可导出需要的迭代次数的一个漂亮的上界

$$R\leqslant\left\lceil\frac{\pi}{4}\sqrt{\frac{N}{M}}\right\rceil \tag{6.17}$$

即必须进行 $R=O(\sqrt{N/M})$次 Grover 迭代(从而 oracle 调用),才能以高的概率得到搜索问题的一个解,这是对经典算法要求的 $O(N/M)$次 oracle 调用的二次加速.对 $M=1$ 情况的量子搜索算法总结如下.

算法 量子搜索

输入 (1)进行变换 $O|x\rangle|q\rangle=|x\rangle|q\oplus f(x)\rangle$的黑箱 oracle$O$,其中对除 x_0 外的所有 $0\leqslant x<2^n$ $f(x)=0$,而 $f(x_0)=1$;(2)处于状态$|0\rangle$的 $n+1$ 量子比特.

输出 x_0.

运行时间 $O(\sqrt{2^n})$次运算，以$O(1)$概率成功.

过程

(1) $|0\rangle^{\otimes n}|0\rangle$ // 初态

(2) $\rightarrow \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$ // 应用$H^{\otimes n}$到前n量子比特，应用HX到最后一个量子比特.

(3) $\rightarrow [(2|\psi\rangle\langle\psi|-I)O]^R\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$

$\approx |x_0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$ // 应用Grover迭代$R\approx\lceil\pi\sqrt{2^n}/4\rceil$次

(4) $\rightarrow x_0$ // 测量前n量子比特.

练习 6.4 像上面那样，对多解情况($1<M<N/2$)，给出量子搜索算法的具体步骤.

当多于1/2的元是搜索问题的解时，即$M\geqslant N/2$会怎样？从表达式$\theta=\arcsin(2\sqrt{M(N-M)}/N)$(对比式(6.14))，我们看到当$M$从$N/2$变到$N$时，$\theta$会减小. 作为结果，搜索算法所需要的迭代次数对$M\geqslant N/2$情况，会随$M$增加. 直观上一个搜索算法有这样的性质是愚蠢的：我们希望当解的数目增加时，求解应该变得容易. 至少有两种解决这个问题的办法. 如果事先知道M大于$N/2$，就随机从搜索空间中取一个元，并用oracle检查它是否为一个解. 这种方法成功的概率至少是$\frac{1}{2}$，并且只需要调用oracle一次. 它的缺点是我们可能事先不知道解的数目M.

在我们不知道是否有$M\geqslant N/2$的情形，可以用另外一种方法. 这种方法有自身的价值. 如6.3节所述，该方法对简化搜索问题解的量子计数算法的分析很有用. 其思路是通过增加N个均不为解的元到搜索空间，来使搜索空间的元的数量加倍，结果是在新的搜索空间中，少于1/2的元是解. 这可以通过增加一个单量子比特$|q\rangle$到搜索指标，把要搜索的元的数目加倍到$2N$来实现. 构造一个新的增广oracle O'，它仅标记搜索问题解且把附加位置0，练习6.5中将说明这个oracle O'如何通过对O的一次调用构造. 新的搜索问题在$2N$项中只有M个解，故运行基于新oracle O'的搜索算法，可知至多需要调用$O'R=\pi/4\sqrt{2N/M}$次，可导出进行搜索需要调用$OO(\sqrt{N/M})$次.

练习 6.5 证明用一次O调用，基本量子门和附加的量子比特$|q\rangle$可以构造增广的oracle O'.

量子搜索算法用途广泛，后面的几节要介绍其中一部分. 该算法的巨大功效来源于，我们没有对搜索问题假定任何特别的结构. 这是基于oracle的问题提法带来

的好处，只要方便，在本章剩下的部分我们就采用这种观点. 当然，在实际应用中，我们必须懂得如何实现 oracle. 在我们考虑的每个实际问题中，我们都给出 oracle 实现的具体描述.

练习 6.6 验证，除了一个不要紧的全局相位因子，盒子 6.1 第二个图中带点的框中的门完成相移运算 $2|00\rangle\langle 00|-I$.

6.2 作为量子仿真的量子搜索

量子搜索算法的正确性很容易验证，但从任何意义上说，想出这样一个算法的途径都不是显然的. 本章我们概要介绍一个能让我们“推导”出量子搜索算法的启发式方法，目的是希望为技巧性很强的量子算法设计任务提供一些直观感觉. 作为附带结果，我们将得到一个确定性量子搜索算法，因为我们的目的是得到灵感而不是原理. 为简单起见，我们假设搜索问题恰好有一个解标作 x.

方法分成两步. 首先，我们猜想解决搜索问题的一个 Hamilton 量. 更确切地，我们写出依赖于解 x 和初态 $|\psi\rangle$ 的 Hamilton 量 H，使得按照 H 演化的量子系统在给定时间内，从 $|\psi\rangle$ 跑到 $|x\rangle$. 一旦我们找到了这样的 Hamilton 量和初态，我们可以进行第二步，用量子线路来模拟 Hamilton 量的作用. 令人吃惊的是，沿着这个过程，可以很快得到量子搜索算法. 在问题 4.3 中，我们研究量子线路的通用性时，已经碰到过这两个阶段过程. 它对量子搜索的研究也可用.

算法中我们假设量子计算机开始状态处于 $|\psi\rangle$，后面我们会给出 $|\psi\rangle$ 应该是什么，但在弄清算法的动态过程之前，保持 $|\psi\rangle$ 为待定比较方便. 量子搜索的目的是把 $|\psi\rangle$ 变到 $|x\rangle$ 或其近似量，我们应当猜测怎样的 Hamilton 量才合适于引起这样的演化？简单性提示我们，应当猜测一个纯粹由项 $|\psi\rangle$ 和 $|x\rangle$ 构成的 Hamilton 量. 于是 Hamilton 量必然是 $|\psi\rangle\langle\psi|$，$|x\rangle\langle x|$，$|\psi\rangle\langle x|$ 和 $|x\rangle\langle\psi|$ 这样的项的和，沿这条思路，最简单的 Hamilton 量或许是

$$H=|x\rangle\langle x|+|\psi\rangle\langle\psi| \tag{6.18}$$

$$H=|x\rangle\langle\psi|+|\psi\rangle\langle x| \tag{6.19}$$

事实上这两个 Hamilton 量都能导致量子搜索算法，不过，我们暂且限于分析式 (6.18) 的 Hamilton 量. 回忆 2.2.2 节，经过时间 t，初态为 $|\psi\rangle$ 的按照 Hamilton 量 H 演化的一个量子系统的状态，由

$$\exp(-\mathrm{i}Ht)\,|\psi\rangle \tag{6.20}$$

给出. 直观上看起来很好：经过一小段时间 t，把 $|\psi\rangle$ 转入到 $(I-\mathrm{i}tH)\,|\psi\rangle=(1-\mathrm{i}t)|\psi\rangle-\mathrm{i}t\langle x|\psi\rangle|x\rangle$，即 $|\psi\rangle$ 在 $|x\rangle$ 的方向上略作旋转. 让我们作一下全面分析，目的是分析是否存在 t，使得 $\exp(-\mathrm{i}Ht)|\psi\rangle=|x\rangle$，显然我们可以把分析限于

由$|x\rangle$和$|\psi\rangle$张成的二维空间. 执行 Gram-Schmidt 过程，可以找到$|y\rangle$，使得$|x\rangle$和$|y\rangle$构成该空间的标准正交基，且$|\psi\rangle=\alpha|x\rangle+\beta|y\rangle$，其中$\alpha$和$\beta$满足$\alpha^2+\beta^2=1$. 为方便起见，我们还假定选择$|x\rangle$和$|y\rangle$相位，使得$\alpha$和$\beta$是非负实数. 在$|x\rangle$，$|y\rangle$基中，我们有

$$H=\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}+\begin{bmatrix}\alpha^2 & \alpha\beta\\ \alpha\beta & \beta^2\end{bmatrix}=\begin{bmatrix}1+\alpha^2 & \alpha\beta\\ \alpha\beta & 1-\alpha^2\end{bmatrix}=I+\alpha(\beta X+\alpha Z) \tag{6.21}$$

因此

$$\exp(-\mathrm{i}Ht)|\psi\rangle=\exp(-\mathrm{i}t)[\cos(\alpha t)|\psi\rangle-\mathrm{i}\sin(\alpha t)(\beta X+\alpha Z)|\psi\rangle] \tag{6.22}$$

全局相位因子$\exp(-\mathrm{i}t)$可以忽略，经过简单的代数运算，可证明$(\beta X+\alpha Z)|\psi\rangle=|x\rangle$，于是系统$t$时间后的状态为

$$\cos(\alpha t)|\psi\rangle-\mathrm{i}\sin(\alpha t)|x\rangle \tag{6.23}$$

于是在$t=\pi/2\alpha$时刻，对系统的观测以概率 1 产生结果$|x\rangle$：即我们已经找到搜索问题的一个解. 不幸的是，观测时间依赖于$|\psi\rangle$在$|x\rangle$方向的分量α，从而依赖于$|x\rangle$，而$|x\rangle$是所要确定的. 明显的解决办法是尝试使α对所有的x相同，即把$|\psi\rangle$选为均匀叠加态

$$|\psi\rangle=\frac{\sum_x|x\rangle}{\sqrt{N}} \tag{6.24}$$

作这样的选择对所有x有，$\alpha=1/\sqrt{N}$，于是观测时间$t=\pi\sqrt{N/2}$不依赖于对x值的了解. 进而，状态式(6.24)有一个明显的优点，即我们知道如何通过做 Hadamard 变换来制备这样的状态.

现在知道 Hamilton 量式(6.18)把$|\psi\rangle$转到$|x\rangle$，能够找到一个量子线路来模拟式(6.18)的 Hamilton 量，从而得到一个量子搜索算法吗？应用 4.7 节的方法，我们看到模拟H的一条自然途径是，对短时间增量Δt，交替模拟 Hamilton 量$H_1\equiv|x\rangle\langle x|$和$H_2\equiv|\psi\rangle\langle\psi|$，如图 6.4 和图 6.5 所示，这些 Hamilton 量可以用第 4 章的方法很容易模拟.

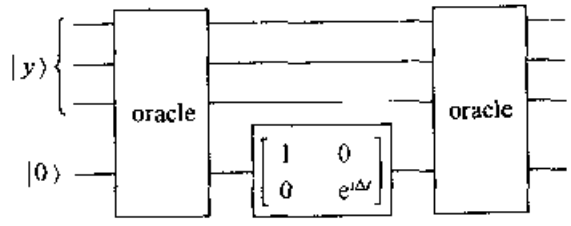


图 6.4　用两个 oracle 调用，实现运算$\exp(-\mathrm{i}|x\rangle\langle x|\Delta t)$的线路.

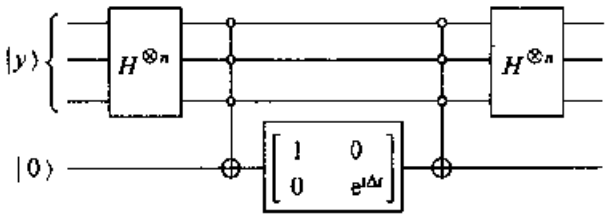


图 6.5 对式(6.24)中$|\psi\rangle$,实现运算$\exp(-i|\psi\rangle\langle\psi|\Delta t)$的线路.

练习 6.7 验证图 6.4 和图 6.5 所示线路分别实现运算$\exp(-i|x\rangle\langle x|\Delta t)$和$\exp(-i\ \psi\rangle\langle\psi|\Delta t)$,其中$|\psi\rangle$如式(6.24)所示.

量子仿真调用 oracle 的次数取决于,为得到合理精确结果要求多大的时间步长.设我们用长为 Δt 的仿真步长,可达到 $O(\Delta t^2)$ 的精度,则需要的总步数是 $t/\Delta t=\Theta(\sqrt{N}/\Delta t)$,于是累积误差是 $O(\Delta t^2\times\sqrt{N}/\Delta t)=O(\Delta t\sqrt{N})$. 为得到合理的高成功概率,需要使误差为 $O(1)$. 这意味着必须选择 $\Delta t=\Theta(1/\sqrt{N})$,这导致调用 oracle 的次数为 $O(N)$——并不比经典解法好. 如果用更精确的量子仿真算法,如精度为 $O(\Delta^3)$ 的算法会如何?这种情况下累积误差为 $O(\Delta t^3\sqrt{N})$,故为达到合理的成功概率,我们需要选择 $\Delta t=\Theta(N^{-1/4})$,导致总共 $O(N^{3/4})$ 次 oracle 调用. 这比经典算法明显有改善,尽管不如 6.1 节的量子搜索算法. 一般而言,利用更精确的量子仿真技术,会导致进行仿真需要的 oracle 调用次数的减少.

练习 6.8 设仿真步的精度可达 $O(\Delta t^r)$,证明以合理精度模拟 H 需要的 oracle 调用次数是 $O(N^{r/2(r-1)})$. 注意当 r 增大时,N 的指数接近 1/2.

我们用 4.7 节的量子仿真的一般结果分析了式(6.18)Hamilton 量的量子仿真的精度. 当然,在这个例子中处理的是特殊的 Hamilton 量,而不是一般的,因而提示我们,具体计算一个仿真步 Δt 的结果而不是基于一般化的分析,也许是有意义的. 我们可以用任何特别选择的仿真方法来做这件事——定出仿真步的结果的工作有点繁琐,不过本质上是直接了当的计算. 显然起点是具体计算最低阶仿真技术的作用,即计算$\exp(-i|x\rangle\langle x|\Delta t)\exp(-i|\psi\rangle\langle\psi|\Delta t)$或$\exp(-i|\psi\rangle\langle\psi|\Delta t)\times\exp(-i|x\rangle\langle x|\Delta t)$中的一个或两个. 两种情况的结果实质上相同,我们限于研究 $U(\Delta t)\equiv\exp(-i|\psi\rangle\langle\psi|\Delta t)\exp(-i|x\rangle\langle x|\Delta t)$. 显然 $U(\Delta t)$ 的作用只在$|x\rangle\langle x|$和$|\psi\rangle\langle\psi|$张成的空间上为不平凡,故我们限于该空间,并在基$|x\rangle,|y\rangle$中讨论,其中$|y\rangle$定义如上. 注意在这个表示中,$|x\rangle\langle x|=(I+Z)/2=(I+\hat{z}\cdot\sigma)/2$,其中 $\hat{z}\equiv(0,0,1)$是沿 z 方向的单位向量,而$|\psi\rangle\langle\psi|=(I+\boldsymbol{\phi}\cdot\sigma)/2$,其中$\boldsymbol{\phi}=(2\alpha\beta,0,(\alpha^2-\beta^2))$(回忆这是 Bloch 向量表示,参看 4.2 节). 简单计算表明除了一个不要紧的全局相位因子,

$$U(\Delta t) - \left(\cos^2\left(\frac{\Delta t}{2}\right) - \sin^2\left(\frac{\Delta t}{2}\right)\boldsymbol{\psi}\cdot\hat{z}\right)I - 2i\sin\left(\frac{\Delta t}{2}\right)\left(\cos\left(\frac{\Delta t}{2}\right)\frac{\boldsymbol{\psi}+\hat{z}}{2} + \sin\left(\frac{\Delta t}{2}\right)\frac{\boldsymbol{\psi}\times\hat{z}}{2}\right)\cdot\boldsymbol{\sigma} \tag{6.25}$$

练习 6.9　验证式(6.25)(提示：参看练习 4.15).

式(6.25)蕴含 $U(\Delta t)$ 是 Bloch 球面上绕

$$\boldsymbol{r} - \cos\left(\frac{\Delta t}{2}\right)\frac{\boldsymbol{\psi}+\hat{z}}{2} + \sin\left(\frac{\Delta t}{2}\right)\frac{\boldsymbol{\psi}\times\hat{z}}{2} \tag{6.26}$$

一个旋转，且转过的角 θ 为

$$\cos\left(\frac{\theta}{2}\right) = \cos^2\left(\frac{\Delta t}{2}\right) - \sin^2\left(\frac{\Delta t}{2}\right)\boldsymbol{\psi}\cdot\hat{z} \tag{6.27}$$

且用 $\boldsymbol{\psi}\cdot\hat{z} = a^2 - \beta^2 = (2/N - 1)$ 代入，可简化为

$$\cos\left(\frac{\theta}{2}\right) = 1 - \frac{2}{N}\sin^2\left(\frac{\Delta t}{2}\right) \tag{6.28}$$

注意到 $\boldsymbol{\psi}\cdot\boldsymbol{r} = \hat{z}\cdot\boldsymbol{r}$，故 $|\psi\rangle\langle\psi|$ 和 $|x\rangle\langle x|$ 在 Bloch 球面上绕轴 $\boldsymbol{r}$ 的同一圆上. 总之，$U(\Delta t)$ 的作用是绕轴 $\boldsymbol{r}$ 旋转 $|\psi\rangle\langle\psi|$，如图 6.6，每次转过一个角 θ. 当 $|\psi\rangle\langle\psi|$ 进行了足够多的旋转接近 $|x\rangle\langle x|$ 时，我们就停下来. 因为我们考虑的是量子仿真，所以我们假想 Δt 非常小，但式(6.28)表明为使 θ 最大化，该做的聪明选择是取 $\Delta t = \pi$. 如果这样做，就有 $\cos(\theta/2) = 1 - 2N$，对于大的 N 相应地 $\theta \approx 4/\sqrt{N}$，找到解 $|x\rangle$ 需调用 oracle 的次数为 $O(\sqrt{N})$，正像原始的量子搜索算法那样.

事实上，如果我们取 $\Delta t = \pi$，则量子仿真实际上等同于原始的量子搜索算法，

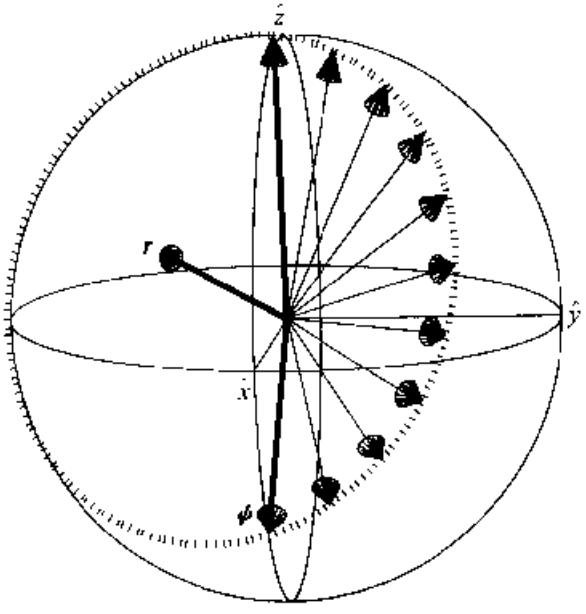


图 6.6　初态 ψ 绕 r 旋转到最终状态 $\hat{z}$ 的 Bloch 球面图.

因为在量子仿真中用的算子为 $\exp(-i\pi|\psi\rangle\langle\psi|) = I-2|\psi\rangle\langle\psi|$ 和 $\exp(-i\pi|x\rangle\langle x|) = I-2|x\rangle\langle x|$，并且除了一个不重要的全局相位因子，这些算子等同于构成 Grover 迭代的步骤. 从这个角度看，图 6.2 和图 6.3 所示的量子搜索算法线路是图 6.4 和图 6.5 的仿真线路的简化，为 $\Delta t = \pi$ 的特殊情形.

练习 6.10 证明通过适当选取 Δt，可以得到用 $O(\sqrt{N})$ 次调用的量子搜索算法，并且最终状态恰好是 $|x\rangle$，算法成功概率为 1，而不是以小概率成功.

我们从量子仿真角度重新推导了量子搜索算法. 这个方法为什么可以奏效？它可以用来寻找其他快速量子算法吗？我们不能以任何确定性的方式回答这个问题，不过下面的一些想法或许是有趣的. 所采用的基本过程包括四方面：(1)给定要解的问题，包括量子算法的输入和输出的描述；(2)猜测一个解问题的 Hamilton 量，并验证它实际上可用；(3)寻找一个模拟该 Hamilton 量的过程；(4)分析仿真消耗的资源. 这同更经典一些的方法有两点不同：我们猜测一个 Hamilton 量而不是量子线路，另外在经典方法中没有仿真步的对应物，两点不同中前者更重要. 在给出解决一个问题的量子线路上存在巨大的自由度，虽然这种自由是量子计算强大能力的部分地来源，但它使得寻找好的线路相当困难. 与之对照，定出 Hamilton 量是一个局限得多的问题，因此在解问题中自由度要小些，但这样的约束实际上使寻找解一个问题的有效量子算法容易得多. 我们已经看到量子搜索算法是这种情形，或许用这个方法可以发现其他量子算法，但我们尚不知道. 看来可以确定的是，“量子算法就是量子仿真”的观点为促进量子算法的发展，提供了有用的新视角.

练习 6.11(连续量子搜索的多重解) 猜测一个 Hamilton 量用以解有 M 个解的连续时间搜索问题.

练习 6.12(量子搜索的不同 Hamilton 量) 设

$$H = |x\rangle\langle\psi| + |\psi\rangle\langle x|, \tag{6.29}$$

(1) 给定按 Hamilton 量的 H 演化，证明从状态 $|\psi\rangle$ 到状态 $|x\rangle$ 用 $O(1)$ 次旋转.

(2) 说明如何进行 Hamilton 量 H 的量子仿真，并确定以高概率得到解该仿真技术需要的 oracle 调用次数.

6.3 量子计数

在事先未知的情况下，多快可以确定 N 元搜索问题的解数 M？显然经典计算机上需要 $\Theta(N)$ 次对 oracle 的调用，来确定 M，在量子计算机上，有可能通过把 Grover 迭代和基于量子 Fourier 变换(第 5 章)的相位估计技术结合，以比经典计

算机快得多的方式估计解的数目. 这有一些重要的应用. 首先，如果我们能很快估计解的数目，就可能很快找到一个解，即使解的数目未知，通过首先对解进行计数，再应用量子搜索算法找到一个解. 其次，量子计数使我们能根据解数是否为 0，来判定解是否存在. 这方面的应用如 NP 完全问题的解，NP 完全问题可以重新表述为搜索问题解的存在性.

练习 6.13　考虑计数问题的一个经典算法. 该算法在搜索空间中均匀独立地进行 k 次采样，令 $X_1,\cdots,X_k$ 为 orcale 调用的结果，即当第 j 个调用显示为问题的一个解时，$X_j=1$，而第 j 个调用没有显示为问题的一个解时，$X_j=0$. 这个算法给出搜索问题解的数目的估计 $S\equiv N\times\sum_j X_j/k$. 证明 S 的标准偏差为 $\Delta S=\sqrt{M(N-M)/k}$. 证明为以至少 3/4 概率，以精度 $\sqrt{M}$，对所有 M 估计 M，必须有 $k=\Omega(N)$.

练习 6.14　证明对任何至少以概率在 $c\sqrt{M}$ 精度内，对所有的 M 估计 M，必须有 $\Omega(N)$ 次 oracle 调用.

量子计数是 5.2 节相位估计过程，在估计 Grover 迭代 G 的特征值上的应用，这估计使我们能够确定搜索问题解的个数 M. 设 $|\alpha\rangle$ 和 $|b\rangle$ 是 $|\alpha\rangle$ 和 $|\beta\rangle$ 张成空间中 Grover 迭代的两个特征向量，令 θ 是 Grover 迭代所确定的旋转角，由式(6.13)可以看到相应的特征值是 $e^{i\theta}$ 和 $e^{i(2\pi-\theta)}$. 为分析方便，假设 oracle 已经如 6.1 节所述被扩充，搜索空间的规模被扩大到 $2N$，并保证 $\sin^2(\theta/2)=M/2N$.

用于量子计数的相位估计线路如图 6.7 所示，该线路的功能是以至少 $1-\varepsilon$ 的成功概率估计 θ 到 m 比特精度. 如每个相位估计算法，第一个寄存器包含 $t\equiv m+\lceil\log(2+1/2\varepsilon)\rceil$ 量子比特，第二个寄存器包含 $n+1$ 量子比特，足以实现在扩充的搜索空间中的 Grover 迭代. 第二寄存器通过 Hadamard 变换初始化，为所有可能输入的均匀叠加态 $\sum_x|x\rangle$. 如 6.1 节所看到的，该状态是本征态 $|a\rangle$ 和 $|b\rangle$ 的叠加，故由 5.2 节的结果，图 6.7 中线路在 $|\Delta\theta|\leqslant 2^{-m}$ 精度内，至少以 $1-\varepsilon$ 概率给出 θ 或 $2\pi-\theta$ 的一个估计. 进而，$2\pi-\theta$ 和 θ 在同一精度水平上的估计显然等价，故实际上相位估计算法以 $1-\varepsilon$ 概率在精度 2^{-m} 内确定 θ.

利用式 $\sin^2(\theta/2)=M/2N$ 和对 θ 的估计，我们得到解的个数的一个估计 M，这个估计的误差 ΔM 是多少？

$$\frac{|\Delta M|}{2N}=\left|\sin^2\left(\frac{\theta+\Delta\theta}{2}\right)-\sin^2\left(\frac{\theta}{2}\right)\right| \tag{6.30}$$

$$=\left(\sin\left(\frac{\theta+\Delta\theta}{2}\right)+\sin\left(\frac{\theta}{2}\right)\right)\left|\sin\left(\frac{\theta+\Delta\theta}{2}\right)-\sin\left(\frac{\theta}{2}\right)\right| \tag{6.31}$$

计算表明 $|\sin((\theta+\Delta\theta)/2-\sin(\theta/2))|\leqslant|\Delta\theta|/2$，并且三角不等式蕴含 $|\sin((\theta+\Delta\theta)/2)\leqslant\sin(\theta/2)+|\Delta\theta|/2$，故

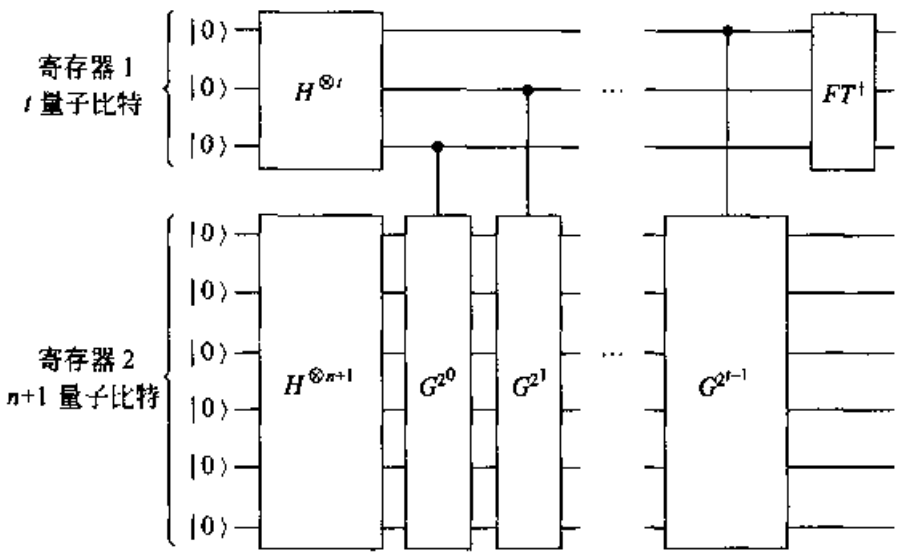


图 6.7 量子计算机上进行近似量子计数的线路.

$$\frac{|\Delta M|}{2N} < \left(2\sin\left(\frac{\theta}{2}\right)+\frac{|\Delta\theta|}{2}\right)\frac{|\Delta\theta|}{2} \tag{6.32}$$

以 $\sin^2(\theta/2) = M/2N$ 和 $|\Delta\theta| \leqslant 2^{-m}$ 代入，给出关于 M 误差的最终估计

$$|\Delta M| < \left(\sqrt{2MN}+\frac{N}{2^{m+1}}\right)2^{-m} \tag{6.33}$$

作为一个例子，设取 $m=\lceil n/2\rceil+1$，且 $\varepsilon = 1/6$，则有 $t=\lceil n/2\rceil+3$，于是算法要求 $\Theta(\sqrt{N})$ 次Grover 迭代，$\Theta(\sqrt{N})$ 次 oracle 调用. 由式(6.33)，求得精度为 $|\Delta M| < \sqrt{M/2}+1/4 = O(\sqrt{M})$. 将这与练习 6.14 相比，按练习 6.14，在经典计算机上要求 $O(N)$ 次 oracle 调用，才能达到类似的精度.

事实上，刚才的例子还起到决定搜索问题的解是否存在的作用，即判断 $M=0$ 还是 $M\neq 0$. 若 $M=0$，则有 $|\Delta M| < 1/4$，于是算法必以至少 5/6 的概率给出估计 0. 反之，若 $M\neq 0$，则容易验证将 M 估计为非 0 的概率至少是 5/6.

量子计数的另一个应用是当解的数目 M 未知时，找出搜索问题的一个解. 6.1 节描述的量子搜索算法应用上的一个困难是，重复 Grover 迭代(式(6.15))的次数，依赖于知道解的数目 M. 首先用基于相位估计的量子计数算法以高概率估计 θ 和 M，然后应用 6.1 节中的量子搜索算法，重复 Grover 迭代到把 θ 和 M 代入式(6.15)决定的次数 R，这个问题可以得到一定程度的解决. 这种情况的角误差最多为 $\pi/4\,(1+|\Delta\theta|/\theta)$，于是像以前那样取 $m=\lceil n/2\rceil+1$，给出不超过 $\pi/4\times 3/2 = 3\pi/8$ 的角误差，相应的搜索算法成功概率至少为 $\cos^2(3\pi/8)=1/2-1/2\sqrt{2}\approx 0.15$. 如果以这样的精度，得到 θ 估计的概率是 5/6，像前面的例子那样，则得到搜索问题的一个解的概率是 $5/6\times\cos^2(3\pi/8)\approx 0.12$. 这个概率经过

计数 搜索的组合过程几次重复，会很快增大到接近 1.

6.4 NP 完全问题解的加速

量子搜索可以用于加速 NP 复杂性类(3.2.2 节)中的问题求解. 我们已经在 6.1.1 节看到，求因子如何可以被加速，下面，我们说明量子搜索如何用于帮助求解 Hamilton 圈问题. 一个图的 Hamilton 圈是遍历该图的每一个顶点的简单回路，HC 问题即为确定给定的图是否具有一个 Hamilton 圈. 这个问题属于 NP 完全问题类，一般认为(尚未证明)在经典计算机上不可解.

解 HC 问题的一个简单算法是，遍历顶点的所有可能排序：(1)生成图顶点的每个可能排序$(v_1,\cdots,v_n)$，允许重复，因为这样可以在不影响结果的实质情况下使分析容易；(2)对每个排序，检查它是否是图的一个 Hamilton 圈，若不是，则继续检查其他排序.

因为有 $n^n = 2^{n\log n}$ 个可能的顶点排序需要搜索，在最坏情况下该算法需要 $2^{n\log n}$ 次对 Hamilton 性质的检查. 事实上，NP 类中的任何问题都可以以类似的方式来解：规模 n 的问题如果有 $w(n)$ 比特给定的证据，其中 $w(n)$ 是 n 的某个多项式，则如果解存在遍历 $2^{w(n)}$ 个可能的证据将给出问题的一个解.

量子搜索可以用来通过增加搜索的速度来加速这样的算法. 特别地，我们用 6.3 节描述的算法来确定搜索问题是否有解. 令 $m = \lceil \log n \rceil$，算法的搜索空间将由 mn 量子比特的串表示，每个 m 量子比特块用来存储一个单个顶点的索引. 于是我们可以把计算基状态写成$|v_1,\cdots,v_n\rangle$，其中每个$|v_i\rangle$用相应的 m 量子比特串表示，总共有 mn 量子比特. 搜索算法的 oracle 必须完成变换

$$O'|v_1,\cdots,v_n\rangle = \begin{cases} |v_1,\cdots,v_n\rangle, v_1,\cdots,v_n \text{不是 Hamilton 圈} \\ -|v_1,\cdots,v_n\rangle, v_1,\cdots,v_n \text{ 是 Hamilton 圈} \end{cases} \tag{6.34}$$

当我们有图的描述时，这样的 oracle 是容易设计和实现的. 可以取一个能识别图中 Hamilton 圈的多项式规模的经典电路，并把它转化为可逆电路，它仍有多项式规模，计算变换$(v_1,\cdots,v_n,q) \to (v_1,\cdots,v_n,q \oplus f(v_1,\cdots,v_n))$，其中若 $v_1,\cdots,v_n$ 是一个 Hamilton 圈，$f(v_1,\cdots,v_n) = 1$，否则为 0. 在量子计算机上实现相应的电路，并让最后一个量子比特从状态$(|0\rangle - |1\rangle)/\sqrt{2}$开始，就得到期望的变换. 这里我们不打算给出具体的细节，而只指出关键：利用 Hamilton 圈识别的经典方式实现的直接推论，oracle 需要的门的个数是 n 的多项式. 利用搜索算法确定解是否存在的变形(6.3 节)可以看到：需要调用 oracle $O(2^{mn/2}) = O(2^{n\lceil \log n\rceil/2})$ 次，来确定 Hamilton 圈是否存在. 当 Hamilton 圈存在时，反复应用计数-搜索算法的组合，容易得到这样的一个圈，并可作为该问题的一个证据.

总结如下.

• 经典算法需要 $O(p(n)2^{n\lceil\log n\rceil})$次运算以确定 Hamilton 圈是否存在,其中多项式因子 $p(n)$是为实现 oracle,即检查一条候选路径是否为 Hamilton 的一组门,需要附加的消耗.决定所需资源的因素是 $2^{n\lceil\log n\rceil}$中的幂.经典算法是确定性的,成功概率为 1.

• 量子算法要求 $O(p(n)\ 2^{n\lceil\log n\rceil/2})$次运算来决定是否存在 Hamilton 路径,多项式因子 $p(n)$是为实现 oracle 附加的消耗,决定所需资源的因素是 $2^{n\lceil\log n\rceil/2}$中的幂.对该算法有一个固定的误差概率(如 1/6),可以通过重复算法 r 次降到 $1/6^r$.

• 量子算法渐近地需要经典算法平方根的运算次数.

6.5 非结构化数据库的量子搜索

假设某人给你一个包含一千种花名字的清单,问你"Perth Rose"出现在清单的什么地方.如果这花名在清单中恰好出现一次,而清单没有以任何显然的形式排序,那么你在找到"Perth Rose"之前平均需要检查 500 个名字.用量子搜索算法可以加速这种数据库搜索吗?事实上,量子搜索算法有时称为一种数据库搜索算法,但它在那方而的使用是有限的,且基于某些假设.本节我们来看一下在概念上非常类似于经典计算机的场合下,量子搜索算法如何用于搜索非结构化数据库.我们描绘的框架将明确量子计算机搜索经典数据库所需要的资源.

设我们有一个包含 $N\equiv 2^n$ 个元的数据库,每个元的长度为 l 比特,这些元标记为 $d_1,\cdots,d_N$.我们希望确定一个特定的 l 比特串 s 是否在数据库中.解这一问题的经典计算机通常分成两部分,如图 6.8 所示.一部分是中央处理单元,或称 CPU,负责利用少量的暂存进行数据处理.第二部分是大的内存.它存储由 2^n 个 l 比特单元块组成的数据库.假设内存是被动的,这意味着它不具备单独处理数据的能力,只能把数据从内存装载(LOAD)到 CPU 中,把来自 CPU 的数据存储(STORE)到内存,以及对暂存在 CPU 中的数据进行处理.当然,经典计算机可以按不同的思路设计,但这种 CPU-内存的划分是流行和普遍的结构.

为在非结构化数据库中找出给定串 s 的位置,最有效的经典算法如下.首先,在 CPU 中设置一个指向数据库元素的 n 比特索引,我们假设 CPU 大得足以存储 $n\equiv\lceil\log N\rceil$比特的索引.索引从 0 开始,随算法迭代 1 次就加 1.每次迭代中,对应于索引的数据库的项被装入 CPU,并与要找的串比较.如果它们相同,算法输出索引值并终止.如果不相同,算法增加索引并继续.显然,这个算法在最坏情况需要装入内存项 2^n 次,并且这是在这个计算模型上,解此问题的可能的最有效算法.

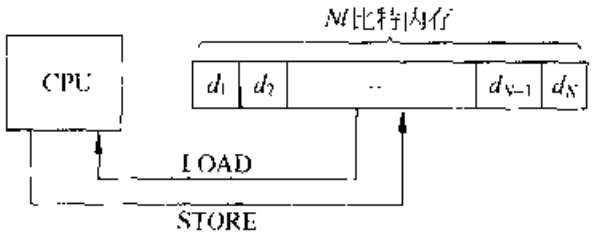


图 6.8　由独立的中央处理单元(CPU)和内存组成的计算机上的经典数据库搜索. 在内存上只能直接进行两种操作——一个内存元素可以被 LOAD 到 CPU 中,或来自 CPU 的一项可以被 STORE 到内存中.

对应的算法在量子计算机上实现的效率如何? 并且即使量子加速是可能的,这类算法有多大用处呢? 我们首先阐明加速是可能的,然后转到这样一个算法用途的问题. 设我们的量子计算机由 CPU 和内存这两个单元组成,如经典计算机. 假定 CPU 有四个寄存器: (1)一个初始化为 $|0\rangle$ 的 n 量子比特索引寄存器; (2)一个初始化为 $|s\rangle$,并在整个计算中保持该状态的 l 量子比特寄存器; (3)一个初始化为 $|0\rangle$ 的 l 量子比特数据寄存器; (4)一个初始化为 $(|0\rangle-|1\rangle)/\sqrt{2}$ 的 1 量子比特寄存器.

内存单元可以用两种方式之一实现. 最简单的方式是一个包含 $N=2^n$ 个单元的量子内存,每个单元由 l 量子比特组成,它包含数据库的记录 $|d_x\rangle$. 第二种是把内存实现为具有 $N=2^n$ 个单元的经典内存,每个单元有 l 比特,包含着数据库记录 d_x. 然而与经典内存不同,它可以由一个索引 x 寻址,而 x 可以处于多重值的叠加. 这个索引允许从内存 LOAD 单元值的一个叠加. 内存访问的工作方式如下. 若 CPU 的索引寄存器处于状态 $|x\rangle$,且数据寄存器处在状态 $|d\rangle$,则第 x 个内存单元的内容 d_x 被加到数据寄存器: $|d\rangle \to |d \oplus d_x\rangle$,其中加是按位模 2 的. 首先,让我们来看这种能力如何用于执行量子搜索,然后讨论怎样从物理上构造这样的内存.

实现量子搜索算法的关键在 oracle 的实现,它必须翻转在内存中定位 s 索引的相位. 设 CPU 处于状态

$$|x\rangle\,|s\rangle\,|0\rangle\,\frac{|0\rangle-|1\rangle}{\sqrt{2}} \tag{6.35}$$

应用 LOAD 操作,把计算机状态置于状态

$$|x\rangle\,|s\rangle\,|d_x\rangle\,\frac{|0\rangle-|1\rangle}{\sqrt{2}} \tag{6.36}$$

这时第二和第三寄存器进行比较,如果相同,则应用比特翻转到寄存器 4; 否则保持不变. 这个操作的效果是

$$|x\rangle|s\rangle|d_x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}\rightarrow\begin{cases}-|x\rangle|s\rangle|d_x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}, d_x=s\\ |x\rangle|s\rangle|d_x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}, d_x\neq s\end{cases}\tag{6.37}$$

接着通过再次执行 LOAD 操作，把数据寄存器恢复到状态$|0\rangle$. oracle 的总体作用保持寄存器 2,3,4 不受影响，并与寄存器 1 不纠缠. 于是总的效果是，如果 $d_x=s$，则寄存器 1 的状态从$|x\rangle$变到$-|x\rangle$，否则保持寄存器不变. 利用这样实现的 oracle，我们可以用量子搜索算法来确定 s 在数据库中的位置. 这用到 $O(\sqrt{N})$次 LOAD 操作，而与之对照的经典方式需要 N 次 LOAD 操作.

为使 oracle 在叠加情形正常工作，内存起先看来似乎应该是量子力学机制的. 但事实上，如前面注意到的，在一些条件下可以用经典方式实现内存，这样使它可以有强得多的抗噪声能力. 但仍然需要量子寻址方案，图 6.9 显示如何做到这一点的示意图. 操作的原理是一种把量子索引的二进制编码的状态(其中 0 到 2^n-1 由 n 量子比特表示)翻译成寻址经典数据库的一元编码(其中 0 到 2^n-1 由在 2^n 个可能位置的单个探头的位置表示)的方法，数据库的改变是在探头与其位置不相关的自由度上作出，接着逆转二进制到一元编码，在数据寄存器中给出希望的内容.

有量子搜索算法用于搜索经典数据库的实际例子吗？需要说明两个不同的方面. 首先，数据库通常不是非结构化的. 简单的数据库，如本节引论中讨论的包含花名称的数据库，可以维持字母序，使得对一个 N 元数据库可以用二进制搜索在 $O(\log(N))$时间内定位一个元. 然而，某些数据库可能需要复杂得多的结构，尽管存在复杂的技术来优化经典的搜索过程，对于复杂到一定程度或意料之外的查询，事先确定的结构可能帮不上太大的忙，这时查询问题实质上可视为我们讨论的非结构化数据库搜索问题.

其次，对于可以搜索经典数据库的量子计算机而言，要求有一个量子寻址方案. 我们给出的方案需要 $O(N\log N)$个量子开关，这基本上相当于存储数据库需要的相同规模的硬件. 我们假设了这些开关将来会像经典内存单元一样简单和便宜，但如果事实并非如此，那么建造量子计算机来进行量子搜索，与使用分布在内存单元中经典计算硬件相比，可能就不够经济了.

基于以上考虑，看来量子搜索算法的主要用途将不是搜索经典数据库，而是可能会用于搜索困难问题的解，如上节讨论的 Hamilton 圈，旅行商和可满足性问题的解.

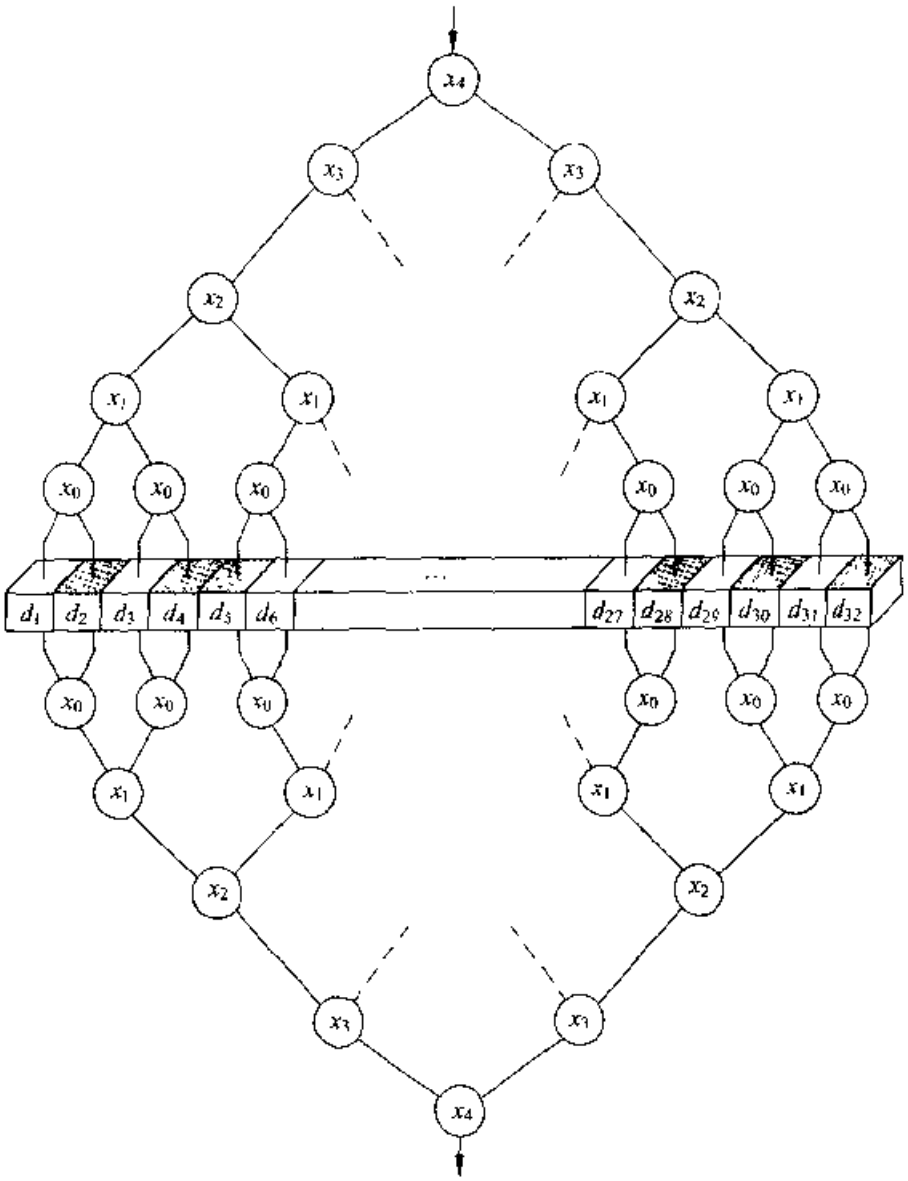


图 6.9　一个带有五个量子比特量子寻址机制的 32 单元经典内存的示意图. 每个圈代表一个开关，由圈在其中的量子比特寻址. 例如，当 $|x_4\rangle=|0\rangle$ 时，相应的开关把输入量子比特接通到左边；当 $|x_4\rangle=|1\rangle$ 时，输入量子比特接到右边. 如果 $|x_4\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$，则取两条路径的均衡叠加. 数据寄存器量子比特从树的顶端进入，并且按路由向下到达数据库，并按内存的内容改变它的状态. 量子比特接着回到一个确定的位置，并携带获取的信息. 物理上来说，这可以通过例如单光子作数据寄存器量子比特实现，它们可以用非线性干涉计控制(第 7 章). 经典数据库可以仅是一片“0”(以白色方块表示)无变换地让光透过而“1”(带阴影的方块)把光的极性改变 90°的塑料.

6.6 搜索算法的最优性

我们证明了量子计算机通过仅仅调用 oracle $O(\sqrt{N})$次，就能够搜索 N 项数据集. 现在要证明没有量子算法能够以少于 $\Omega(\sqrt{N})$次 oracle 调用，完成此项任务，因此所给出的算法是最优的.

假设算法从状态$|\psi\rangle$出发. 为简单起见，对搜索问题有惟一解的情况，我们证明 x 下界. 为确定 x，我们被允许使用一个对解 x 产生 -1 相移，而保持其他状态不变的 oracle O_x，$O_x = I-2|x\rangle\langle x|$. 我们假设算法从$|\psi\rangle$开始，且恰好应用 oracle O_x k 次，并在 oracle 运算之间穿插酉运算 $U_1, U_2, \cdots, U_k$. 定义

$$|\psi_k^x\rangle \equiv U_k O_x U_{k-1} O_x \cdots U_1 O_x |\psi\rangle \tag{6.38}$$

$$|\psi_k\rangle \equiv U_k U_{k-1} \cdots U_1 |\psi\rangle \tag{6.39}$$

即，$|\psi_k\rangle$是当在没有 oracle 运算条件下，执行系列酉运算 $U_1, \cdots, U_k$ 导致的状态，令$|\psi_0\rangle = |\psi\rangle$. 我们的目的是估计量

$$D_k \equiv \sum_x \| \psi_k^x - \psi_k \|^2 \tag{6.40}$$

其中为简化记号，用 ψ 代替$|\psi\rangle$. 直观上，D_k 是对经 oracle 作用 k 步以后，偏差的一个度量. 如果这个量很小，则所有$|\psi_k^x\rangle$大致相同，并且不可能以高的概率正确识别 x. 证明的技巧在于说明两件事：(1) D_k 的一个估界表明它的增长不可能快于 $O(k^2)$；(2)证明为能够区分 N 个不同项，D_k 必须是 $\Omega(N)$的. 把这两个结果结合起来就得到期望的下界估计.

首先，给出 $D_k \leqslant 4k^2$ 的归纳证明. 显然这对 $k=0$ 成立，其中 $D_k=0$. 注意到

$$D_{k+1} = \sum_x \| O_x \psi_k^x - \psi_k \|^2 \tag{6.41}$$

$$= \sum_x \| O_x(\psi_k^x - \psi_k) + (O_x - I)\psi_k \|^2 \tag{6.42}$$

应用 $\| b+c \|^2 \leqslant \| b \|^2 + 2\| b \| \| c \| + \| c \|^2$，其中 $b \equiv O_x(\psi_k^x - \psi_k)$且 $c \equiv (O_x - I)\psi_k = -2\langle x|\psi_k\rangle|x\rangle$，给出

$$D_{k+1} \leqslant \sum_x \left(\| \psi_k^x - \psi_k \|^2 + 4\| \psi_k^x - \psi_k \| \, |\langle x|\psi_k\rangle| + 4|\langle \psi_k|x\rangle|^2 \right) \tag{6.43}$$

对右边第二项运用 Cauchy-Schwarz 不等式，并且 $\sum_x |\langle x|\psi_k\rangle|^2 = 1$，得到

$$D_{k+1} \leqslant D_k + 4\left(\sum_x \| \psi_k^x - \psi_k \|^2 \right)^{\frac{1}{2}} \left(\sum_{x'} |\langle \psi_k|x'\rangle|^2 \right)^{\frac{1}{2}} + 4 \tag{6.44}$$

$$\leqslant D_k + 4\sqrt{D_k} + 4 \tag{6.45}$$

根据归纳假设 $D_k \leqslant 4k^2$，可得

$$D_{k+1} \leqslant 4k^2 + 8k + 4 - 4(k+1)^2 \tag{6.46}$$

归纳完成.

为完成证明，需要证明只有当 D_k 是 $\Omega(N)$ 时，成功的概率才是高的. 我们假设对所有 x 有 $|\langle x|\psi_k^x\rangle|^2 \geqslant 1/2$，于是一次观测得到解的概率至少是 $\frac{1}{2}$. 用 $e^{i\theta}|x\rangle$ 代替 $|x\rangle$，不改变成功的概率，所以不失一般性假定 $\langle x|\psi_k^x\rangle = |\langle x|\psi_k^x\rangle|$，可得

$$\| \psi_k^x - x \|^2 = 2 - 2|\langle x|\psi_k^x\rangle| \leqslant 2 - \sqrt{2} \tag{6.47}$$

定义 $E_k \equiv \sum_x \| \psi_k^x - x \|^2$，可以看到 $E_k \leqslant (2-\sqrt{2})N$. 现在来证明 D_k 是 $\Omega(N)$ 的. 定义 $F_k \equiv \sum_x \| x - \psi_k \|^2$，有

$$D_k = \sum_x \| (\psi_k^x - x) + (x - \psi_k) \|^2 \tag{6.48}$$

$$\geqslant \sum_x \| \psi_k^x - x \|^2 - 2\sum_x \| \psi_k^x - x \| \, \| x - \psi_k \| + \sum_x \| x - \psi_k \|^2 \tag{6.49}$$

$$= E_k + F_k - 2\sum_x \| \psi_k^x - x \| \, \| x - \psi_k \| \tag{6.50}$$

应用 Cauchy-Schwarz 不等式，得到 $\sum_x \| \psi_k^x - x \| \, \| x - \psi_k \| \leqslant \sqrt{E_k F_k}$，于是有

$$D_k \geqslant E_k + F_k - 2\sqrt{E_k F_k} = (\sqrt{F_k} - \sqrt{E_k})^2 \tag{6.51}$$

在练习 6.15 中，将证明 $F_k \geqslant 2N - 2\sqrt{N}$. 这个结果与 $E_k \leqslant (2-\sqrt{2})N$ 结合，对充分大的 N，给出 $D_k \geqslant cN$，其中 c 是任何小于 $(\sqrt{2} - \sqrt{2-\sqrt{2}})^2 \approx 0.42$ 的常数. 因为 $D_k \leqslant 4k^2$，这便意味着

$$k \geqslant \sqrt{cN/4} \tag{6.52}$$

总之，为以至少 $\frac{1}{2}$ 的概率找到搜索问题的一个解，我们必须调用 oracle 至少 $\Omega(\sqrt{N})$ 次.

练习 6.15 利用 Cauchy-Schwarz 不等式，证明对任何归一化状态向量 $|\psi\rangle$ 和一组有 N 个向量的标准正交基向量 $|x\rangle$，有

$$\sum_x \| \psi - x \|^2 \geqslant 2N - 2\sqrt{N} \tag{6.53}$$

练习 6.16 设对所有可能值 x 的均匀平均而不是对 x 的所有值，要求差错的概率小于 1/2，证明 $O(\sqrt{N})$ 次 oracle 调用对解搜索问题仍是必需的.

这个结果，即量子搜索算法实际上是最优的，是喜忧参半. 可喜的是它告诉我

们，对这个问题至少我们完全发挥了量子力学的极限，不会有进一步的提高了. 可悲的是，我们或许希望能比量子搜索算法二次加速做得好得多. 我们或许推想能用 $O(\log N)$ 次 oracle 调用，来搜索 N 元空间. 假设这样的算法存在，就能够在量子计算机上有效求解 NP 完全问题，因为它可以用大致 $w(n)$ 次 oracle 调用，搜索全部的 $2^{w(n)}$ 项可能证据，这里多项式 $w(n)$ 是证据的按比特计算的长度. 不幸的是，这样的算法不可能存在. 这对未来的算法设计者是个有用的信息，因为它表明基于简单搜索，解决 NP 完全问题的方法肯定是要失败的.

我们在这里冒昧地发表一点看法. 许多研究者相信 NP 完全问题困难的根本原因是，它们的搜索空间本质上是无结构的，并且解决这类问题的(精确到一个多项式因子)最好的可能方法是采用搜索的办法. 如果有人持这样的观点，那么这对量子计算将是一个坏消息，因为这表明量子计算机可有效求解的问题类，BQP，不包含 NP 完全问题. 当然，这只是一种看法，NP 完全问题仍可能具有某些未知的结构，使它们可以在量子计算机，或甚至是在经典计算机上被有效求解. 说明这一点的一个很好问题是，被普遍视为属于难度介于 P 和 NP 完全类之间的 NPI 类的因子问题，量子力学有效求解因子问题的关键是，利用了该问题的一个隐含结构——可归约为求阶问题. 即便是揭示了这个惊人的结构，人们还是没能利用该结构开发出因子分解的有效经典算法，尽管量子力学结构能够给出一个有效的因子分解算法或许其他被怀疑属于 NPI 类的问题，像图同构问题，或许甚至是 NP 完全问题自身，也潜藏着类似的结构.

练习 6.17(对多重解的最优性) 假设搜索问题有 M 个解，证明为找到一个解需要 $O(\sqrt{N/M})$ 次 oracle 调用.

6.7 黑箱算法的极限

本章以量子搜索算法的推广作结束，此算法可以估计量子计算能力. 本章开头，我们把搜索问题描述为求一个 n 比特整数 x，使得函数 $f:\{0,1\}^n \to \{0,1\}$ 的值等于 $f(x)=1$. 与此相关的判定问题是，是否存在 x 使得 $f(x)=1$. 解这个判定问题具有同样难度，并可表为计算 Boolean 函数 $F(X)=X_0 \vee \cdots \vee X_{N-1}$，其中 $\vee$ 表示二元或运算(OR)，$X_k = f(k)$，而 X 表示集合 $\{X_0, X_1, \cdots, X_{N-1}\}$. 更一般地，我们或许希望计算除或以外的其他函数. 例如，$F(X)$ 可以是与(AND)，奇偶校验(PARITY，模 2 和)，或多数函数(MAJORITY)(当且仅当 $X_k=1$ 的个数大于 1，$F(X)=1$). 一般而言，我们可以把 F 看成任意 Boolean 函数. 给定计算 f 的黑箱，一台不管是经典的还是量子的计算机，能够多快地计算这些函数?

或许看起来要回答这样的问题，在没有关于 f 的任何知识的情况下是很难

的.但事实上即使在这个黑箱模型中,可以确定的东西还是有很多,其中我们认为 oracle 完成任务方式是不成问题的,复杂性以调用 orcale 次数衡量.前面几节对搜索算法的分析说明了处理这样问题的一种方式,但得到查询复杂性的一个更有力的方法是,我们现在要简要介绍的多项式方法.

让我们从一些有用的定义开始.确定性查询复杂性 $D(F)$,是经典计算机完成 F 的确定性计算,需要调用 oracle 的最少次数.相应的量子对应物 $Q_E(F)$,是一台量子计算机为确定性地计算 F 需要的最少 oracle 调用次数.因为量子计算机的概率输出特性,一个更有意义的量是有界误差复杂性 $Q_2(F)$,即量子计算机以至少 2/3 概率输出 F,需要的最少 oracle 调用次数(2/3 是任意取的——这个概率只要有限地大于 1/2,就能通过重复增加接近到 1).相关的度量是零误差复杂性 $Q_0(F)$,指要么肯定性地输出 F,要么以小于 1/2 概率给出一个没有定论的结果,量子计算机需要的最小 oracle 调用次数.所有这些界都必须对任意 oracle 函数 f 成立(或换句话说,任何到 F 的输入 X).注意 $Q_2(F)\leqslant Q_0(F)\leqslant Q_E(F)\leqslant D(F)\leqslant N$.

多项式方法基于表示 Boolean 函数的最小阶(实)多线性多项式的性质.下面要考虑的所有多项式是 $X_k\in\{0,1\}$ 的函数,且因为 $X_k^2=X_k$,所以是多线性的.我们说一个多项式 $p:R^N\to R$ 表示 F,如果 $p(X)=F(X)$ 对所有 $X\in\{0,1\}^N$ 成立(这里 R 表示实数集).这样的多项式总是存在的,因为可以具体构造出一个合适的候选多项式

$$p(X)=\sum_{Y\in\{0,1\}^N}F(Y)\prod_{k=0}^{N-1}[1-(Y_k-X_k)^2] \tag{6.54}$$

p 的最小阶是惟一的,这留作练习 6.18.F 的这样一个表示的最小阶,记作 $\deg(F)$,是 F 复杂性的一个有用的度量.例如,已知 $\deg(\mathrm{OR})$,$\deg(\mathrm{AND})$ 和 $\deg(\mathrm{PARITY})$ 都等于 N,事实上,已经知道大多数函数的阶是 N.而且,业已证明

$$D(F)\leqslant 2\deg(F)^4 \tag{6.55}$$

这个结果为确定性经典方式计算大多数 Boolean 函数设定了一个上界.把这个概念加以扩展,如对所有 $X\in\{0,1\}^N$ 一个多项式满足 $|p(X)-F(X)|\leqslant 1/3$,则我们说 p 近似 F,以 $\widetilde{\deg}(F)$ 表示这种近似多项式的最小阶.这种度量对于随机化经典计算很重要,且如将看到的,在量子情形也很重要.已经知道 $\widetilde{\deg}(\mathrm{PARITY})=N$,

$$\widetilde{\deg}(\mathrm{OR})\in\Theta(\sqrt{N})\qquad\text{并且}\qquad\widetilde{\deg}(\mathrm{AND})\in\Theta(\sqrt{N}) \tag{6.56}$$

又

$$D(F)\leqslant 216\,\widetilde{\deg}(F)^6 \tag{6.57}$$

式(6.55)和式(6.57)中给出的界,只是写作本书时的最好已知结果,它们的证明超出本书的范围,但读者可以在"历史和进一步阅读的材料"中找到进一步的相关信

息.人们相信得到严格的估界是有可能的,但对我们的目的而言,这些界就够了.

练习 6.18 证明 Boolean 函数 $F(X)$的最小阶多项式表示是惟一的.

练习 6.19 证明 $P(X)=1-(1-X_0)(1-X_1)\cdots(1-X_{N-1})$表示或.

多项式在量子算法结果的描述中自然产生.让我们把执行 T 次 oracle 调用 O 的量子算法 Q 的输出写成

$$\sum_{k=0}^{2^n-1} c_k \mid k\rangle \tag{6.58}$$

我们将证明幅度 c_k 是变量 $X_0,X_1,\cdots,X_{N-1}$的阶最多为 T 的多项式.任何 Q 都可以按如图 6.10 所示的量子线路实现.第一次 oracle 调用之前,状态$|\psi_0\rangle$可以写成

$$\mid \psi_0\rangle = \sum_{ij}(a_{i0j} \mid i\rangle \mid 0\rangle + a_{i1j} \mid i\rangle \mid 1\rangle) \mid j\rangle. \tag{6.59}$$

其中第一个标号对应 n 量子比特的 oracle 调用,接着的标号对应子 oracle 存放结果的单量子比特,最后的标号对应 Q 所使用的 $m-n-1$ 个工作量子比特.经过 oracle 调用,得到状态

$$\mid \psi_1\rangle = \sum_{ij}(a_{i0j} \mid i\rangle \mid X_i\rangle + a_{i1j} \mid i\rangle \mid X_i \oplus 1\rangle) \mid j\rangle \tag{6.60}$$

但由于 X_i 非 0 即 1,可以重写为

$$\mid \psi_1\rangle = \sum_{ij}[((1-X_i)a_{i0j} + X_i a_{i1j}) \mid i0\rangle + ((1-X_i)a_{i1j} + X_i a_{i0j}) \mid i1\rangle] \mid j\rangle \tag{6.61}$$

注意在$|\psi_0\rangle$中,计算基态的幅度对 X 的阶为 0,而在 $\psi_1\rangle$中阶为 1(对 X 为线性).一个重要的事实是,Q 在调用 oracle 前后进行的任何酉运算,都不改变这些多项式的阶,而每次 oracle 调用,可以使阶至多增加 1.因此,经过 T 次调用,幅度多项式的阶最多为 T.而且,在计算基下测量输出式(6.58)以 $P_k(X)=|c_k|^2$ 概率给出结果 k,这个概率是 X 的最多 $2T$ 阶实多项式.

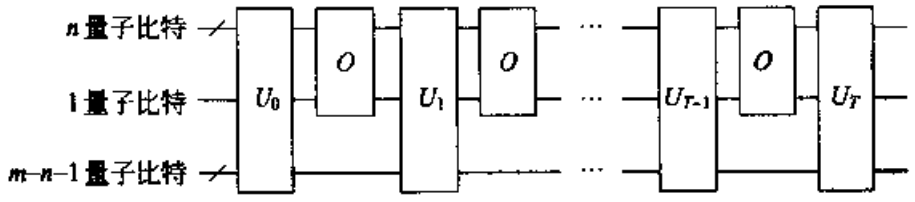


图 6.10 进行 T 次 oracle 调用的量子算法的一般量子线路.$U_0,U_1,\cdots,U_T$ 是 m 量子比特上的任意酉变换,而 oracle 作用在 $n+1$ 量子比特上.

得到一个结果 1 的概率 $P(X)$的阶最多也是 $2T$,因为由算法知,它是多项式族 $P_k(X)$的一个子集的和.在 Q 肯定产生正确答案的情形下,$P(X)=F(X)$,子是

$\deg(F)\leqslant 2T$，由此导出

$$Q_E(F)\geqslant\frac{\deg(F)}{2} \tag{6.62}$$

在 Q 以有界的差错概率给出答案的情形下，可知 $P(X)$ 近似 $F(X)$，因此有 $\widetilde{\deg}(F)\leqslant 2T$，并可导出

$$Q_2(F)\geqslant\frac{\widetilde{\deg}(F)}{2} \tag{6.63}$$

结合式(6.55)和式(6.62)，我们得到

$$Q_E(F)\geqslant\left[\frac{D(F)}{32}\right]^{1/4} \tag{6.64}$$

类似地，结合式(6.57)和式(6.63)，有

$$Q_2(F)\geqslant\left[\frac{D(F)}{13824}\right]^{1/6} \tag{6.65}$$

这意味着用黑箱计算布尔函数，量子算法最多只能提供对经典算法的多项式加速　通常甚至连这样也做不到(因为 $\deg(F)$ 对大多数函数是 $\Omega(N)$ 的)．另一方面，已经知道对 $F=\mathrm{OR}$，$D(F)=N$，而随机化的经典查询复杂性为 $R(F)\in\Theta(N)$，同时结合式(6.63)、式(6.56)，和量子搜索算法已知的性能，可见 $Q_2(F)\in\Theta(\sqrt{N})$．这个二次加速正是量子搜索算法能达到的，并且多项式方法提示这个算法也许可以推广到更广的一类问题，但没有关于黑箱 oracle 函数 f 的进一步结构信息，将不可能对经典算法进行指数加速．

练习 6.20　通过构造多项式表示一个量子线路的输出 OR 函数，来证明 $Q_0(\mathrm{OR})\geqslant N$，其中线路计算 OR 的误差为 0．

问题 6.1(求最小)　设 $x_1,\cdots,x_N$ 是如 6.5 节中的内存中的数的一个数据库，证明为以至少 $\frac{1}{2}$ 概率找到清单中最小数，量子计算机仅需要访问内存 $O(\log(N)\sqrt{N})$ 次．

问题 6.2(推广的量子搜索)　令 $|\psi\rangle$ 是一个量子状态，且定义 $U_{|\psi\rangle}\equiv I-2|\psi\rangle\langle\psi|$．即 U_{ψ} 对状态 $|\psi\rangle$ 给出 -1 相位，而保持正交于 $|\psi\rangle$ 的状态不变．

(1) 设我们有实现酉算子 U 的量子线路，使得 $U|0\rangle^{\otimes n}=|\psi\rangle$，说明如何实现 U_{ψ}．

(2) 令 $|\psi_1\rangle=|1\rangle$，$|\psi_2\rangle=(|0\rangle-|1\rangle)/\sqrt{2}$，$|\psi_3\rangle=(|0\rangle-\mathrm{i}|1\rangle)/\sqrt{2}$．设从集合 $U_{|\psi_1\rangle},U_{|\psi_2\rangle},U_{|\psi_3\rangle}$ 中选择一个未知的 oracle O．给出一个量子算法，通过 oracle 的一次使用，就将其识别出来(提示：考虑超密编码)．

(3) 研究：更一般地，给定 k 个状态 $|\psi_1\rangle,\cdots,|\psi_k\rangle$，和一个从 $U_{|\psi_1\rangle},\cdots,U_{|\psi_k\rangle}$ 中选出的 oracle O，为以高概率识别该 oracle，需要应用 oracle 多少次？

问题 6.3(数据获取) 给定一个量子 oracle,它对 n 量子比特输入(及一个工作量子比特)$|k,y\rangle$,返回 $|k,y\oplus X_k\rangle$. 证明仅用 $N/2+\sqrt{N}$ 次调用,就可以高的概率获得 X 的全部 $N=2^n$ 个比特,这意味着对任意 F 有一般的上界 $Q_2(F)\leqslant N/2+\sqrt{N}$.

问题 6.4(量子搜索与密码系统) 量子搜索具有加速搜索密码系统密钥的潜在用途. 思路是为解密,遍历可能密钥的整个空间,依次尝试密钥,并检查被解密的信息是否有意义. 说明为什么这个想法不能用于 Vernma 密码(12.6 节),当什么时候它可用于像 DES 那样的密码系统(为了解 DES,参看如文献[MvOV96]或文献[Sch96a])?

第 6 章的总结 量子搜索算法

- **量子搜索算法**:对 $N=2^n$ 种可能中有 M 个解的搜索问题,先制备状态 $\sum_x|x\rangle$,然后重复 $G\equiv H^{\otimes n}UH^{\otimes n}O$ 总共 $O(\sqrt{N/M})$ 次,其中 O 是一个搜索 oracle. 如果 x 是解,则 $|x\rangle\rightarrow-|x\rangle$,否则不变;同时 U 变 $|0\rangle\rightarrow-|0\rangle$ 且保持其他所有的计算基. 测量以高的概率得到搜索问题的一个解.
- **量子计数算法**:设一个搜索问题解的数目未知. G 具有特征值 $\exp(\pm i\theta)$,其中 $\sin^2(\theta/2)=M/N$. 基于相位估计的 Fourier 变换使我们能用 $O(\sqrt{N})$ 次 oracle 调用,以高精度估计 M. 即使解的数目事先是未知的,量子计数反过来使我们可以确定一个给定的搜索问题是否有解,并且如果有解,可以找出一个解.
- **多项式界**:对于描述为求全函数 F(与部分函数,或许诺问题相反)的问题,量子算法对经典算法至多有多项式加速,具体为 $Q_2(F)\geqslant[D(F)/13824]^{1/6}$. 而且,量子搜索是最优的:它是 $\Theta(\sqrt{N})$ 的.

历史和进一步阅读的材料

量子搜索算法和它许多的进一步发展和完善属于 Grover[Gro95,Gro97]. Boyer、Brassard、Høyer 和 Tapp[BBHT98]发表了一篇有影响的论文,在其中提出了对解的数目 M 大于 1 的量子搜索算法,并给出了量子计数算法的框架. 量子计数算法后来被 Brassard、Høyer 和 Tapp[BHT98]细化. Mosca[Mos98]从相位估计的角度研究了该算法. Grover 迭代可以看作两个反射的积,由 Aharonov[Aha99b]首先在一篇综述中指出. 连续时间 Hamilton 量式(6.18)是 Farhi 和 Gutmann[FG98]从与 6.2 节我们的观点相当不同的角度首先研究的. Grover 算法是基于 oracle 的最好算法,是

Bennett、Bernstein、Brassard 和 Vazirani[BBBV97] 证明的. 我们给出的证明是基于 Boyer、Brassard、Høyer 和 Tapp[BBHT98] 的证明. Zalka[Zal98] 对证明进行了提炼，指出量子算法渐近地和精确地为最优.

估计量子算法的能力的多项式方法是 Beals、Buhrman、Cleve、Mosca 和 de Wolf[BBC+98] 引入到量子计算中来的. Mosca 的博士论文[Mos99] 也有一个精彩的讨论，6.7 节的讨论的许多内容就基于此. 那节中的许多结果没有证明就直接被引用，下面就是这些引用：式(6.56)属于[BBC+98] 中的 Nisan 和 Smolensky，其他来源尚未发表，式(6.56)从 Paturi[Pat92] 的一个定理推导出来，而式(6.57)的推导在[BBC+98] 中. 比式(6.65)所给出的更好的界在文献[BBC+98]中给出，但要用到像块灵敏度这样的超出本书范围的概念. Ambainis[Amb00] 给出一个利用基于纠缠现象，来估计量子黑箱算法的完全不同方法.

问题 6.1 属于 Durr 和 Høyer[DH96]，问题 6.3 属于 van Dam[van98a].

CHAPTER 7
第 7 章
量子计算机：物理实现

未来的计算机的重量可能不超过 1.5 吨.

——*Popular Mechanics*，*对科学的不断发展的预测*，*1949*

我认为世界市场大概需要 5 台计算机.

——*Thomas Watson*，*IBM 董事长*，*1943*

量子计算与量子信息之所以有意义，是因为我们相信量子信息处理机器可以在现实中实现，否则，该领域就只是引起数学上的好奇心而已. 然而，量子线路，算法和通信系统的实验实现被证明是极富挑战性. 本章探讨量子信息处理装置和系统的物理实现的一些指导性原则和原型系统.

7.1 节综述量子计算机物理实现上需要考虑的各种折衷因素，这个讨论是 7.2 节量子计算实验实现的一组充分条件的细节前瞻，这些条件在 7.3 节到 7.7 节中，通过考虑 5 种不同的原型物理系统的一系列例子研究，加以说明. 这 5 种原型是：简单谐振子、光子和非线性光介质、腔量子电动力学装置、离子阱和分子核磁共振. 对每类系统，我们简单描述其物理装置、决定它动态的 Hamilton 量、控制系统完成量子计算的方法，以及主要缺点. 我们并不深入描述这些系统的物理学特性，因为每类系统自身都构成一个完整的领域，内容将超出本书的范围. 我们只总结与量子计算和量子信息相关的概念，以便使读者能够同时了解实验上的挑战和理论上的潜力. 另一方面，从量子信息的角度分析这些系统，也提供了一个全新的视角. 我们希望对读者能有启发和帮助，因为它能出人意料地简化某些重要物理学推导. 7.8节以讨论某些其他物理系统——量子点、超导门和半导体中的自旋——结束. 这些方面对本领域也是有意义的. 仅想抓住每种实现要点的读者，每节末都提供一个摘要.

7.1 指导性原则

建造一台量子计算机有哪些实验要求？理论的基本单元是量子比特——双能级量子系统，我们在1.5节简要考察了人们相信量子比特在自然界存在的原因，以及它们可能的存在形式. 为实现量子计算机，我们不只是要赋予量子比特某种鲁棒的物理表示(在其中它们能保持其量子性质)，还要选择量子比特在其中按期望方式演化的一个系统. 而且，我们必须能够把量子比特制备到某个特定的初态集合，并测量系统的输出状态.

实验实现的挑战在于，这些基本要求常常只能部分得到满足. 一枚硬币有两个状态，是一个好的比特，但不是一个好的量子比特，因为它不能长久处于(正面和反面的)叠加态. 一个单核自旋可以成为一个非常好的量子比特，因为与外磁场相同或相反的叠加，可以持续很长时间，甚至是数天. 但用核自旋建造量子计算机非常困难，因为单个核子与外界的耦合如此之弱，以致测量它们的定向非常困难. 这些限制相互矛盾是普遍现象：必须很好地隔离量子计算机，以便保持它的量子性质，但同时它的量子比特又必须是可访问的，以便量子比特被用于完成计算任务，并被处理以读出计算结果. 一个现实的实现必须取得这些限制之间的微妙平衡. 于是相关的问题不是如何建造量子计算机，而是量子计算机可以造得多好？

系统	T_Q/s	T_{op}/s	$n_{op}=\lambda^{-1}$
核自旋	$10^{3}\sim10^{8}$	$10^{-1}\sim10^{-6}$	$10^{5}\sim10^{14}$
电子自旋	10^{-1}	10^{-7}	10^{6}
离子阱(In^{+})	10^{-1}	10^{-14}	10^{13}
电子-Au	10^{-6}	10^{-14}	10^{8}
电子-GaAs	10^{-10}	10^{-13}	10^{3}
量子点	10^{-6}	10^{-9}	10^{3}
光学腔	10^{-5}	10^{-14}	10^{9}
微波共振腔	10^{0}	10^{-4}	10^{4}

图7.1 相互作用的量子比特系统的不同候选物理实现相干时间 T_Q(秒)，运算时间 T_{op}(秒)，和最大运算数 $n_{op}=\lambda^{-1}=T_Q/T_{op}$ 的粗略估计. 尽管这张表中项很多，但只给出了三种本质不同的量子比特表示：自旋、电荷和光子. 离子阱利用的是被束缚在阱中对应于电子或核自旋反转的原子精细或超精细跃迁(见7.6节). 对金和GaAs以及量子点中电子的估计以电荷形式给出，用电极或某个受限区域是否包含电子表示. 在光学和微波共振腔中，共振腔中聚焦成不同模的光子(频率从吉赫兹到几百太拉赫兹)代表量子比特. 把这些估计看作一粒盐；它们只给出了无数可能性的某些方面.

什么样的物理系统有潜力成为好的候选量子信息处理系统？了解特定量子计算机实现优点的关键是量子噪声(有时称为退相干(decoherence))．因为量子计算可能的最大长度大致由，系统维持在量子力学相干状态的时间 T_Q 和完成基本酉变换(至少涉及两个量子比特)的时间 T_{op} 之比给出．在许多系统中，这两个时间实际上是有关系的，因为它们都由系统和外界的耦合强度决定．不过 $\lambda = T_{op}/T_Q$ 变化的范围可以大得惊人，如图 7.1 所示．

这些估计，有助于洞察量子信息处理机器可能的不同物理实现的优点．但实际实现中，还有许多其他的噪声来源和不完美因素．例如，通过光照引起能级间的跃迁，来操作由原子的双电子能级表示的量子比特，也可能以一定概率引起到其他电子能级的跃迁．这些也被视为噪声过程，因为它们把系统带出了定义量子比特的双态．一般而言，任何引起信息损失的过程都是噪声过程．

7.2 量子计算的条件

让我们回到详细讨论前节提到的量子计算的四个基本要求．这些要求是能够：

(1) 鲁棒地表示量子信息；

(2) 完成酉变换的通用性族；

(3) 制备基准初态；

(4) 测量输出结果．

7.2.1 量子信息的表示

量子计算基于量子状态的变换．量子比特是双能级量子系统，且作为量子计算机最简单的基本构成模块，它们提供了对状态对及其物理实现的方便标记．于是比如说自旋 3/2 粒子，可用四个状态 $|m=+3/2\rangle$，$|m=+1/2\rangle$，$|m=-1/2\rangle$，$|m=-3/2\rangle$ 来表示双量子比特．

要能计算，关键是要认识到可访问的状态是有限的．把一个粒子在一维线上的位置 x 取为状态集合，对计算来说一般不是很好，即便粒子可以处在量子态 $|x\rangle$，或甚至是某个叠加态 $\sum_x c_x |x\rangle$．因为 x 具有连续范围的可能性，而 Hilbert 空间是无穷维的，因而当没有噪声时，信息的容量是无限的．例如，在理想世界中，Shakespear 的全部著作都可以存储在(读取自)二进制小数 $x = 0.010111011001\cdots$ 的无穷位数字中，这显然是不现实的．实际情况是，噪声的出现把可以分辨的状态减少到有限数目．

事实上，一般希望通过某种对称性，来规定有限的状态空间，以使退相干最小化．例如一个自旋 1/2 粒子处在由状态 $|\uparrow\rangle$ 和 $|\downarrow\rangle$ 张成的 Hilbert 空间中，自旋状态不可能跑出二维空间，因此很好地隔离时，它是一个近乎理想的量子比特．

如果表示选得不好，则会产生退相干. 例如，如盒子 7.1 所描述的，一个处在有限方势阱中的粒子，在足够深处就可以包含两个束缚态，仅构成一个质量不高的量子比特. 因为可能有从束缚态到非束缚态的跃迁. 它们会导致退相干，因为这些跃迁会破坏叠加态. 对于单量子比特，任意叠加态最短寿命是一个重要的数字. 如 $(|0\rangle-|1\rangle)/\sqrt{2}$ 状态的(横向)弛豫时间 T_2，是自旋状态和原子系统对这个数字的一个好的测度. 注意高能状态 $|1\rangle$ 的(纵向)弛豫时间 T_1 只是传统的状态寿命，通常比 T_2 要大.

盒子 7.1　方势阱与量子比特

方势阱是量子系统的一个原型，一个粒子处在一个一维的盒子中，其行为服从 Schrödinger 方程(2.86). 该系统的 Hamilton 量是 $H=p^2/2m+V(x)$，其中若 $0<x<L$，$V(x)=0$，否则 $V(x)=\infty$. 表示为位置基下的波函数的本征能态是

$$|\psi_n\rangle=\sqrt{\frac{2}{L}}\sin\left(\frac{n\pi}{L}x\right) \tag{7.1}$$

其中 n 是整数，而 $|\psi_n(t)\rangle=e^{-iE_nt/\hbar}|\psi_n\rangle$，$E_n=n^2\pi^2/2mL^2$. 这些状态具有离散谱. 特别地，假设在实验中只需要考虑两个最低的能级，则定义感兴趣的波函数为 $|\psi\rangle=a|\psi_1\rangle+b|\psi_2\rangle$. 因为

$$|\psi(t)\rangle=e^{-i(E_1-E_0)/2t}\left[ae^{-i\omega t}|\psi_1\rangle+be^{i\omega t}|\psi_2\rangle\right] \tag{7.2}$$

其中 $\omega=(E_1-E_0)/2$，我们可以忽略除 a 和 b 以外的所有量，把状态抽象地写成二维向量 $|\psi\rangle=\begin{bmatrix}a\\b\end{bmatrix}$. 这个双能级系统表示一个量子比特. 我们的双能级系统的变换像量子比特吗？它随时间的演化是在 Hamilton 量 $H=\hbar\omega Z$ 作用下，而这个作用在旋转框架下是可以忽略的. 为在此量子比特上执行运算，对 H 进行摄动，考虑在 $V(x)$ 上增加项

$$\delta V(x)=-V_0(t)\frac{9\pi^2}{16L}\left(\frac{x}{L}-\frac{1}{2}\right) \tag{7.3}$$

在我们的双能级系统的基中，这可以通过取矩阵元素 $V_{nm}=\langle\psi_n|\delta V(x)|\psi_m\rangle$ 重写，其中 $V_{11}=V_{22}=0$，且 $V_{12}=V_{21}=V_0$，使得相对 V_0 的最低阶，H 的摄动为 $H_1=V_0(t)X$. 这产生绕 $\hat{x}$ 轴的旋转. 类似的改变势函数的技术可用于进行其他单量子比特运算.

这里给出了在方势阱中的两个最低能级如何表示一个单量子比特，以及位势的简单摄动怎样达到此量子比特上的计算操作的效果. 然而，摄动还带来高阶影响，并且真实物理系统的盒子也不是无限深的，其他能级开始出现，我们的双能级近似就失败了. 同时，在现实中，负责控制的系统也是一个量子系统，它与用于量子计算的系统相耦合. 这些问题引起退相干.

7.2.2 酉变换的性能

封闭的量子系统按照 Hamilton 量作酉演化，但为执行量子计算，我们必须能够控制 Hamilton 量，以完成从酉变换的通用性族（如 4.5 节所述）中任意选出的酉变换. 例如，一个单自旋可能按 Hamilton 量 $H=P_x(t)X+P_y(t)Y$ 演化，其中 $P_{\{x,y\}}$ 是用经典方式控制的参数. 从练习 4.10，我们知道适当选择 P_x 和 P_y，可以执行任意的单自旋旋转.

按照 4.5 节的定理，任意酉变换可由单自旋运算和受控非门运算组成. 因此，这两种量子逻辑门的实现是实验量子计算研究自然的目标，然而，一个隐含的要求是能够寻址单个量子比特，和应用这些门去选择量子比特或量子比特对. 这在许多物理系统中并不容易做到. 例如，在一个离子阱中，我们可以用一束激光在许多单个的离子中作选择性的激发，但只有当离子在空间上分开至少一个波长时才可行.

未记录到的不完整酉变换可能导致退相干. 在第 8 章中，我们将看到随机振动（单个自旋绕 $\hat{z}$ 轴的微小转动）的平均效应如何导致，量子状态相对相位表示的量子信息的丢失. 类似地，当逆转系统误差需要的信息丢失时，系统误差的积累效应就是退相干. 而且，Hamilton 量中的控制参数只是经典控制的近似：现实中，控制系统只是另外一个量子系统，真正的 Hamilton 量应该包括，控制系统在量子计算机上作用的反作用. 例如，代替上例中 $P_x(t)$ 的实际上是一个 Jaynes-Cummings 类型的原子-光子相互作用的 Hamilton 量（7.5.2 节），$P_x(t)=\sum_k \omega_k(t)(a_k+a_k^\dagger)$ 或类似共振腔光子场的某个量. 经过与量子比特相互作用，一个光子可以带走量子比特的状态信息，因此这是一个退相干过程.

对酉变换而言，两个重要数字是，可以达到的最小保真度 F（第 9 章），和完成诸如单自旋旋转或受控非门的基本运算的最大时间 t_{op}.

7.2.3 基准初态的制备

即使是经典计算，进行有用计算的一个最重要的要求就是，能够制备期望的输入. 如果我们有一个可以进行完美计算的盒子，但若不能输入数据，那又有什么用呢？对于经典机器，建立给定的输入几乎没有困难——我们只需要把某些定义输入状态的开关设置为理想配置. 然而，对量子系统，视所采用的量子比特实现，这件事可能非常困难.

注意到只需要能够（可重复地）以高保真度产生出一个特定的量子状态，因为酉变换可以把它带到其他期望输入状态. 例如，能把 n 自旋置于 $|00\cdots0\rangle$ 就足够了. 由于热效应，它们也许不能长时间停留该状态，这也和表示的选取有关.

输入状态的制备，对大多数物理系统是一个重要的问题. 例如，通过从物理上

把离子冷却到基态(7.6 节)，可以很好地制备离子的初态，但这是有挑战性的. 而且，对涉及离子计算机的物理系统，还需要考虑更多因素. 在核磁共振(7.7 节)中，每个分子可以视为一个单独的量子计算机，为达到可测量的信号强度，需要大量的分子. 尽管离子比特可以在任意叠加态停留相对长的时间，把所有分子中的所有量子比特置于相同状态也是困难的，因为$|0\rangle$和$|1\rangle$之间的能量差 $\hbar\omega$ 远小于 $k_B T$. 另一方面，简单地让系统达到平衡，将建立一个众所周知的状态，即热平衡态，密度矩阵是 $\rho \approx e^{H/k_B T}/Z$，其中 Z 是维持 $\mathrm{tr}(\rho)=1$ 的归一化因子.

有关输入状态制备的两个重要数字是：初态制备为给定状态 ρ_{in} 的最小保真度和 ρ_{in} 的熵. 这个熵的重要性在于，比如说很容易以高保真度状态制备 $\rho_{in}=I/2^n$，但这是一个没有用的状态，因为它在酉变换下是不变的. 理想的输入状态是一个纯态，熵为零. 一般地，具有非零熵的输入状态，会降低从输出结果得到答案的可行性.

7.2.4　输出结果的测量

量子计算需要什么样的测量能力？我们暂且把测量视为，将一个以上量子比特和经典系统耦合起来，使得经过一段时间，量子比特的状态被经典系统的状态所指示的过程. 例如，由一个双能级原子的基态和激发态表示的量子比特状态 $a|0\rangle+b|1\rangle$，可能通过抽运激发态并观察荧光来测量. 如果一个静电计指示在光电倍增管中检测到荧光，那么量子比特会坍缩到$|1\rangle$状态，发生这种情况的概率是 $|b|^2$. 否则，静电计检测不到电荷，量子比特会坍缩到$|0\rangle$状态.

量子计算的测量过程的一个重要特征是，当进行一个投影测量时，描述所发生情况的波函数发生坍缩(参考 2.2.5 节). 一个好的量子算法的输出是在测量时，有高概率得到有用答案的叠加态. 例如，Shor 因子分解算法其中一步是，从测量结果中找一个接近 qc/r 的整数 r，其中 q 是 Hilbert 空间的维数. 输出状态实际上非常接近所有可能 c 值的均匀叠加，但测量使之坍缩到一个单独的随机整数，从而使我们能够以高概率确定 r(如第 5 章所描述的连分式展开).

可以想到测量有许多困难，例如，低效的光子计数器和放大器热噪声，都可能减少上述方案中被测量子状态的信息. 而且，投影测量(有时称为强测量)常常难以实现，它们要求量子和经典系统的耦合要强，且可切换. 在不希望的时候测量不能发生，否则它们可能引起退相干.

不过令人吃惊的是，强测量不是必需的，量子计算可采用持续工作从不关掉的弱测量. 在相对测量耦合为短的时间内完成计算，和使用大量的量子计算机系综，使这一点成为可能. 这些系综合起来给出一个组合信号，它宏观上是可观察的，并指示着量子状态. 采用系综会带来别的问题. 例如，在因子分解算法中，若测量输出

结果是 $q\langle c\rangle/r$，算法会失败，因为 c 的平均值 $\langle c\rangle$ 不必是整数（因此连分式展开就不可能）. 幸运的是，修改量子算法可以使之能够采用系综平均的结果，这将在 7.7 节进一步讨论.

反映测量能力的一个重要数字是信噪比（SNR），它决定测量的有效性和测量设备到量子系统的耦合能给出的内在的信号强度.

7.3 谐振子量子计算机

在继续描述可实现的量子计算机的完整物理模型之前，让我们暂且考虑一个非常基本的系统——简单谐振子——并讨论为什么它不能用作一台好的量子计算机. 此例用的形式也将作为研究其他物理系统的基础.

7.3.1 物理装置

在抛物势阱 $V(x)=m\omega^2x^2/2$ 中的粒子是简单谐振子的一个例子. 在经典世界中，这可以是随能量在弹簧势能和质量动能之间转换，而在弹簧上来回振荡的一块质量；它也可以是能量在电感和电容之间来回振荡的共振电路. 这些系统中，系统的总能量是一个连续参数.

在量子领域中，即与外界耦合非常小的领域，系统的总能量只能取一些离散值. 一个高 Q 值共振腔中束缚的单模电磁辐射就是一个例子，总能量（除去一个固定偏移量）只能是，由基本常数 $\hbar$ 和被束缚的辐射的频率 ω 决定的 $\hbar\omega$ 的整倍数.

简单谐振子的本征能态可以标记为 $|n\rangle$，$n=0,1,\cdots,\infty$，和量子计算的关系是，取这些状态的有限子集来表示量子比特. 这些量子比特的寿命由如共振腔质量因子 Q 这样的参数决定. 可以通过增加共振腔壁的反射性，来把 Q 提到很高，而且，只要让系统随时间演化，就可以应用酉变换. 不过这种方案存在问题，下面会加以说明. 我们从研究系统的 Hamilton 量开始，然后讨论如何实现如受控非门那样的简单逻辑门.

7.3.2 Hamilton 量

在一维抛物势中的粒子的 Hamilton 量是

$$H=\frac{p^2}{2m}+\frac{1}{2}m\omega^2x^2 \tag{7.4}$$

其中 p 是粒子的动量算子，m 是质量，x 是位置算子，而 ω 与位势深度有关. x 和 p 在此式中是算子（见盒子 7.2），可以重写作

$$H=\hbar\omega\left(a^\dagger a+\frac{1}{2}\right) \tag{7.5}$$

其中 $a^\dagger$ 和 a 是产生和湮没算子，定义为

$$a = \frac{1}{\sqrt{2m\hbar\omega}}(m\omega x + \mathrm{i}p) \tag{7.6}$$

$$a^\dagger = \frac{1}{\sqrt{2m\hbar\omega}}(m\omega x - \mathrm{i}p) \tag{7.7}$$

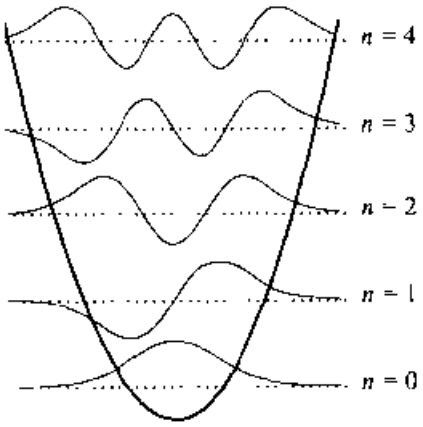
零点能 $\hbar\omega/2$ 引起观测不到的全局相位因子相移，我们可以忽略此项.

盒子 7.2　量子谐振子

谐振子是物理世界量子描述中极重要和有用的概念，并且确定它的 Hamilton 量(式(7.4))的本征能态是掌握它性质的好办法. 一个办法就是对 $\psi_n(x)$ 和本征能量 E，在 $x=\pm\infty$，$\psi(x)\to 0$ 和 $\int |\psi(x)|^2 = 1$ 下解 Schrödinger 方程

$$\frac{\hbar^2}{2m}\frac{\mathrm{d}^2\psi_n(x)}{\mathrm{d}x^2} + \frac{1}{2}m\omega^2 x^2\psi_n(x) = E\psi_n(x) \tag{7.8}$$

头五个解的示意图为：



这些波函数描绘出谐振子粒子在势阱中不同位置的概率幅.

尽管这些图，可以给出物理系统关于坐标空间的某些直观印象，我们一般地对状态空间的抽象代数性质更感兴趣. 特别地，设 $|\psi\rangle$ 和能量 E 满足式(7.8)，则按式(7.6)和式(7.7)，定义算子 a 和 $a^\dagger$ 可以由 $[H,a^\dagger]=\hbar\omega a^\dagger$ 得到

$$Ha^\dagger|\psi\rangle = ([H,a^\dagger] + a^\dagger H)|\psi\rangle = (\hbar\omega + E)a^\dagger|\psi\rangle \tag{7.9}$$

即 $a^\dagger|\psi\rangle$ 是 H 的一个具有能量 $E+\hbar\omega$ 的本征态. 类似地，$a|\psi\rangle$ 是一个具有能量 $E-\hbar\omega$ 的本征态. 出于这个原因，$a^\dagger$ 和 a 分别称为提升和递降算子. 对任意的整数 n，可知 $a^{\dagger n}|\psi\rangle$ 是本征态，其能量为 $E+n\hbar\omega$. 于是存在无穷数目的本征能态，能量有 $\hbar\omega$ 的均匀间隔. 而且 H 是半正定的，必存在某个 $|\psi_0\rangle$ 使得 $a|\psi_0\rangle=0$，这就是基态 H 具有最低能量的本征态. 这些结果有效地刻画了量子谐振子的本质，并使我们可以用紧凑的符号 $|n\rangle$ 表示本征态，其中 n 是整数，且 $H|n\rangle = \hbar\omega(n+1/2)|n\rangle$. 我们在本章常会用到 $|n\rangle$，a 和 $a^\dagger$，因为谐振子会出现在许多物理系统中.

H 的本征态 $|n\rangle$，其中 $n=0,1,\cdots$，具有性质

$$a^\dagger a\,|\,n\rangle = n\,|\,n\rangle \tag{7.10}$$

$$a^\dagger\,|\,n\rangle = \sqrt{n+1}\,|\,n+1\rangle \tag{7.11}$$

$$a\,|\,n\rangle = \sqrt{n}\,|\,n-1\rangle \tag{7.12}$$

后面我们将得知，引入涉及 a 和 $a^\dagger$ 的附加项，如 $a_1^\dagger a_2 + a_1 a_2^\dagger$，对表达与简单谐振子的相互作用或振荡器间相互作用是方便的. 不过我们暂且限于讨论单个振荡器.

练习 7.1 根据 x 和 p 不对易的事实，并且实际上 $[x,p]=i\hbar$，具体说明 $a^\dagger a = H/\hbar\omega - 1/2$.

练习 7.2 给定 $[x,p]=i\hbar$，计算 $[a,a^\dagger]$.

练习 7.3 计算 $[H,a]$，并用这个结果证明，若 $|\psi\rangle$ 是 H 的本征态，具有能量 $E \geqslant n\hbar\omega$，则 $a^n|\psi\rangle$ 是具有能量 $E\quad n\hbar\omega$ 的一个本征态.

练习 7.4 证明 $|n\rangle = \dfrac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle$.

练习 7.5 验证式(7.11)和式(7.12)与式(7.10)以及归一化条件 $\langle n|n\rangle = 1$ 相容.

本征态的时间演化由解 Schrödinger 方程(2.86)给出，从中我们可以知道 状态 $|\,\psi(0)\rangle = \sum_n c_n(0)\,|\,n\rangle$ 随时间演化变为

$$|\,\psi(t)\rangle = \mathrm{e}^{-iHt/\hbar}\,|\,\psi(0)\rangle = \sum_n c_n \mathrm{e}^{-in\omega t}\,|\,n\rangle \tag{7.13}$$

我们为了讨论，假定可以精确制备任意状态，且系统状态可以被投影测量(2.2.3节)，此外系统与外界没有相互作用，是完全封闭的.

7.3.3 量子计算

假设我们希望用上面描述的单个简单谐振子执行量子计算，怎样做呢？ 量自然的选择是把量子比特表示成本征能态 $|n\rangle$，这种选择使我们能按如下方式完成受控非门运算. 回忆这个变换，在双量子比特状态上执行映射

$$\begin{aligned} |\,00\rangle_L &\to |\,00\rangle_L \\ |\,01\rangle_L &\to |\,01\rangle_L \\ |\,10\rangle_L &\to |\,11\rangle_L \\ |\,11\rangle_L &\to |\,10\rangle_L \end{aligned} \tag{7.14}$$

(这里，下标 L 用于把逻辑状态和谐振子基态区分开). 用映射

$$\begin{aligned} |\,00\rangle_L &= |\,0\rangle \\ |\,01\rangle_L &= |\,2\rangle \\ |\,10\rangle_L &= (|\,4\rangle + |\,1\rangle)/\sqrt{2} \\ |\,11\rangle_L &= (|\,4\rangle - |\,1\rangle)/\sqrt{2} \end{aligned} \tag{7.15}$$

对这两个量子比特进行编码. 设在 $t=0$ 时刻，系统开始于这些基态张成的某个状态，且我们简单地让系统向前演化到时间 $t=\pi/\hbar\omega$. 这引起本征能态经历变换 $|n\rangle \to \exp(-i\pi a^{\dagger}a)|n\rangle = (-1)^n|n\rangle$，使得 $|0\rangle$，$|2\rangle$ 和 $|4\rangle$ 都保持不变，但 $|1\rangle \to -|1\rangle$. 我们得到了期望的受控非门变换.

一般地，物理系统能够执行酉变换 U 的充要条件就是，由 Hamilton 量 H 定义的系统的时间演化算子 $T=\exp(-iHt)$ 和 U 具有几乎一样的特征值谱. 在上面的例子中，受控非门能够容易实现，是因为它的特征值只有 $+1$ 和 -1，可以直接安排编码，使谐振子的时间演化算子具有同样的特征值. 振荡器的 Hamilton 量可以被摄动，以实现几乎任何特征值谱，并且任意数量的量子比特都可以通过把它们映射到系统无穷的本征态中来表示. 这提示我们或许整个量子计算机可以在一个简单谐振子中实现.

7.3.4　不足

当然，上述方案存在许多问题. 显然，即便知道如何由基本门构造该算子，对某个量子计算的酉算子，我们也不总是知道它的特征值谱. 事实上，对量子算法处理的大部分问题，特征值谱的知识等同于解的知识.

另一显然的问题是，上面用到的技术不允许计算的串联，因为一般来说，两个酉变换的串联给出一个特征值不相关的新变换.

最后，用单个谐振子进行量子计算的想法是有缺陷的，因为它忽略了信息数字化表示的原则. 一个 2^n 维 Hilbert 空间映射到单个谐振子的状态空间，将不得不允许具有能量 $2^n\hbar\omega$ 的状态. 与之对照，同样的 Hilbert 空间可以由 n 个双能级量子系统得到，却最多具有 $n\hbar\omega$ 的能量. 在具有 2^n 个刻度的经典转盘和 n 经典比特的寄存器之间也可作类似对比. 量子计算立足于数字化计算，而不是模拟计算.

谐振子量子计算机的主要特点概括如下（类似地，我们考虑的每个系统都要在相应的小节末进行总结）. 我们就从单个振荡器的研究，转向下面的由光子和原子构成的谐振子系统.

- 量子比特的表示：单个量子振荡器的能级 $|0\rangle$，$|1\rangle$，…，$|2^n\rangle$ 给出 n 量子比特.
- 酉演化：任意酉变换 U，可以通过把它的特征值谱与 Hamilton 量 $H=a^{\dagger}a$ 的特征值谱匹配实现.
- 初态制备：未考虑.
- 读出：未考虑.
- 不足：不是数字化表示，而且用匹配特征值对通常具有未知特征值的任意 U 实现变换不可行.

7.4 光子量子计算机

一种能表示量子比特的实际物理系统是光子. 光子是中性粒子,没有强的相互作用,与大多数物质也没有强的相互作用. 它们在光纤中可以长距离低损耗地传输,可用移相器进行有效的延迟,并且很容易用分束器组合. 光子展示出特征性量子现象,如双缝实验中产生的干涉. 原则上,以非线性光学介质为媒介,可以形成光子的相互作用. 这种理想的情况存在问题,不过,从对元件、体系结构和光子量子信息处理器的不足的研究可以学到很多东西,正如在本节将看到的.

7.4.1 物理装置

让我们从什么是单个光子,它们怎样表示量子状态,以及对操作光子有用的实验器件开始,主要描述移相器、分束器和非线性光学 Kerr 介质的经典行为.

光子可用以下方式表示量子比特. 如我们在简单谐振子的讨论中看到的,电磁共振腔中的能量以 $\hbar\omega$ 为单位量子化,每个这样的量子称为一个光子. 一个共振腔可能包含 0 个或 1 个光子的叠加态,该状态可表为一个量子比特 $c_0|0\rangle+c_1|1\rangle$,但我们采取不同做法. 考虑两个总能量是 $\hbar\omega$ 的共振腔,并把量子比特的两个状态取为光子在共振腔($|01\rangle$)还是在另一个($|10\rangle$). 叠加的物理状态子是将写作 $c_0|01\rangle+c_1|10\rangle$,我们称这个为双轨(dual-rail)表示. 注意我们将集中在,作为波包穿过自由空间而不是共振腔中的单个光子,我们可以假想有一个沿着波包移动的共振腔. 量子比特中的每个共振腔将对应于一个不同的空间模.

实验室中产生单光子的一个方案是减弱激光的输出. 激光输出一个称为相干态的状态$|\alpha\rangle$,定义为

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle \tag{7.16}$$

其中$|n\rangle$是一个 n 光子的本征能态. 这个状态曾是量子光学深入研究的主题,具有许多我们在这里不能描述的漂亮性质,只要明白被抽运到高于激光阈值的激光相干态,是从驱动的振荡器中自然辐射出来的就可以了. 注意平均能量是$\langle\alpha|n|\alpha\rangle=|\alpha|^2$. 当衰减时,相干态变为更弱的相干态,而弱相干态可以导致以高概率仅含一个光子.

练习 7.6(光子湮没的本征态) 证明相干态是光子湮没算子的一个本征态,即证明对某个常数 λ,$a|\alpha\rangle=\lambda|\alpha\rangle$.

例如,对 $\alpha=\sqrt{0.1}$,我们得到状态 $\sqrt{0.90}|0\rangle+\sqrt{0.09}|1\rangle+\sqrt{0.002}|2\rangle+\cdots$. 于是如果光成功通过了衰减器,那么我们以高于 95% 的概率知道它是单个光子,

则失败的概率是 5%，注意 90%的时间根本没有光子通过，于是这个源的速率是每单位时间 0.1 个光子．最后，这个源并不指示（以某种经典输出的手段）光子是否被输出，两个这样的源无法同步．

可以用参数化降频转换（down conversion）获得更好的同步性，这涉及将频率为 ω 的光子送到非线性光学介质如 KH_2PO_4，以产生频率为 $\omega_1+\omega_2=\omega_0$ 的光子对．动量也被转换，使得 $k_1+k_2=k_3$．以致当（破坏性地）检测到一个单 ω_2 光子时，知道存在一个 ω_1 光子（图 7.2）．通过将它与门耦合起来，使门仅在检测到一个（而不是两个以上）单光子时打开，以及适当延迟多个降频转换源的输出．我们原则上可以得到，在探测器和门的时间分辨率之内的，多个在时间上同步传播的单光子．

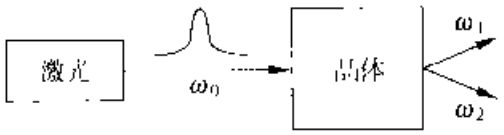


图 7.2　产生单个光子的参数化降频转换方案．

用不同的技术可以有效地探测相对宽范围波长的单个光子．对我们来说，探测器最重要的特性是，以高概率确定在一个特定空间模中，是否存在光子的探测能力．对于双轨表示，这意味着在计算基中的投影测量．实践中，不完整性降低了探测到单光子的概率．光电探测器的量子效率（quantum efficiency）$\eta(0\leqslant\eta\leqslant1)$ 是单个到达探测器的光子产生的光生载流子对（photocarrier pair），对探测器电流有贡献的概率．探测器的其他重要特征包括它的带宽（时间响应率），噪声和没有光子到达却产生的载流子形成的暗计数（dark count）．

实验中操作光子状态的最方便的设备是：镜子、移相器（phase shifter）和分束器（beam splitter）．高反射率的镜子反射光子，且改变其在空间中传播的方向，0.01%损失率的镜子并不少见．移相器不过是折射率 n 不同于自由空间 n_0 的透明介质的平板．例如普通的硅酸硼玻璃对光波长具有 $n\approx1.5n_0$．在这样的介质中传播距离 L，光子的相位改变为 e^{ikL}，其中 $k=n\omega/c_0$，而 c_0 是真空中的光速．因此光子穿过移相器，与光子穿过自由空间中的同样距离相比的相移是 $e^{i(n-n_0)L\omega/c_0}$．

另一个有用的器件，分束器，不过是部分镀银的玻璃，它反射了入射光的 R 部分，以及透射了入射光的 $1-R$ 部分．实验室中，分束器常用两个棱镜组成，并在夹层放置一个薄的金属膜，如图 7.3 所示．把分束器的角 θ 定义为 $\cos\theta=R$，注意该角使反射部分的比例参数化，不一定和分束器的物理定向有关系．该设备的两个输入和两个输出由

$$a_{out}=a_{in}\cos\theta+b_{in}\sin\theta \tag{7.17}$$

$$b_{out}=-a_{in}\sin\theta+b_{in}\cos\theta \tag{7.18}$$

联系起来，其中我们把 a 和 b 经典地视为两个端口辐射的电磁场．注意在这个定义

中，为了方便我们选择的相位约定是非标准的. 在 50/50 的特殊情况中，$\theta=45°$.

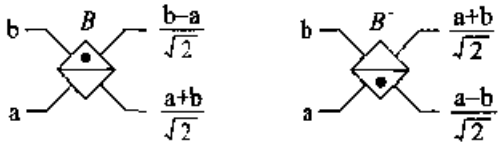


图 7.3 光学分束器的一个方案，有两个输入端口和两个输出端口，且对 50/50 分束器符合相位约定($\theta=\pi/4$). 右边的分束器是左边的逆(两者以内部画出的点相区别). 对($\theta=\pi/4$)给出了模运算的输入输出关系.

非线性光学提供了最后一个有用的器件：折射率 n 正比于穿过它的光的总强度 I 的材料，即

$$n(I) = n + n_2 I \tag{7.19}$$

这称为光学 Kerr 效应，它可以(非常微弱)出现在常见的材料，如玻璃和糖水中. 在杂掺玻璃中，n_2 为 $10^{-18}\,m^2/W \sim 10^{-11}\,m^2/W$，而在半导体中，为 $10^{-14}\,m^2/W \sim 10^{-2}\,m^2/W$. 实验中，当两束等强度的光几乎同传地穿过 Kerr 介质时，每束光会比单束情形具有多出 $e^{in_2\Pi\omega/c_0}$ 的相移. 当 L 可以具有任意长度时，这就很理想，但不幸的是，因为大多数 Kerr 介质还是高度吸收的，或把光散射到期望空间模以外. 这是单光子量子计算机不实际的主要原因，这不可能成功，我们将在 7.4.3 节要讨论这一点.

下面我们转到这些光学器件的描述.

7.4.2 量子计算

采用单光子的 $c_0|01\rangle+c_1|10\rangle$ 双轨表示来编码，利用移相器、分束器和非线性光学 Kerr 介质，任意酉变换都可用于量子信息. 通过给出描述每个设备的量子力学 Hamilton 量，可按如下方式理解这个工作过程.

如在 7.3.2 节看到的，电磁辐射共振腔模的时间演化的量子力学模型是一个谐振子. $|0\rangle$ 是真空态，$|1\rangle=a^\dagger|0\rangle$ 是单光子态，而一般地，$|n\rangle=\frac{a^{\dagger n}}{\sqrt{n!}}|0\rangle$ 是 n 光子态，其中 $a^\dagger$ 是该模的产生算子. 自由空间中的演化由 Hamilton 量

$$H = \hbar\omega a^\dagger a \tag{7.20}$$

描述，且应用式(7.13)，可知状态 $|\psi\rangle=c_0|0\rangle+c_1|1\rangle$ 在时间上的演化为 $|\psi(t)\rangle=c_0|0\rangle+c_1e^{-i\omega t}|1\rangle$. 注意双轨表示是方便的，因为自由演化只对 $|\varphi\rangle=c_0|0\rangle+c_1|1\rangle$ 改变一个探测不到的全局相位. 因此对状态流形，演化 Hamilton 量为 0.

1. 移相器

移相器 P 的作用就像正常的时间演化，但速率不同，且作用只局限于通过它的模. 这是因为光在大折射率的介质中会变慢，特别地，在折射率为 n 的介质中，经过距离 L，必在真空中多花 $\Delta\equiv(n-n_0)L/c_0$ 时间. 例如，作用 P 在真空态上没有作用：$P|0\rangle=|0\rangle$，但在单光子态，我们有 $P|1\rangle=e^{i\Delta}|1\rangle$.

P 在双轨状态上执行一项有用的逻辑运算. 把移相器放到一个模中，相对于另一穿过同样距离却不经过移相器的模，就延迟了它的相位演化. 对双轨态，除了一个没有关系的全局相位，就把 $c_0|01\rangle+c_1|10\rangle$ 变换到 $c_0e^{-i\Delta/2}|01\rangle+c_1e^{i\Delta/2}|10\rangle$. 回忆 4.2 节这个运算不过是一个旋转，

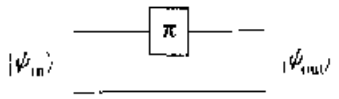
$$R_z(\Delta)=e^{i\Delta Z/2} \tag{7.21}$$

其中我们取 $|0_L\rangle=|01\rangle$ 为逻辑 0，而 $|1_L\rangle=|10\rangle$ 为逻辑 1，且 Z 是通常的 Pauli 算子；我们于是可以认为 P 是 Hamilton 量

$$H=(n_0-n)Z \tag{7.22}$$

演化的结果，这里 $P=\exp(-iHL/c_0)$.

练习 7.7 如图，如果我们用顶上的连线表示 $|01\rangle$ 模，底下的连线表示 $|10\rangle$ 模，且盒子 π 表示一个 π 的相移.



证明如下线路用

$$|\psi_{out}\rangle=\begin{bmatrix}e^{i\pi} & 0\\ 0 & 1\end{bmatrix}|\psi_{in}\rangle \tag{7.23}$$

变换双轨态. 注意在这个光学线路中，空间上的传播，由如上的框图具体表出. 在双轨表示中，按照式(7.20)的演化只把逻辑状态改变一个观测不到的全局相位，因此我们完全可以忽略它而只保持相对相移.

练习 7.8 证明 $P|\alpha\rangle=|\alpha e^{i\Delta}\rangle$，其中 $|\alpha\rangle$ 是一个相干态(注意，一般地，α 是一个复数).

2. 分束器

分束器有类似的 Hamilton 量描述，但我们不从唯象的角度出发，而是直接从 Hamilton 量开始，并证明如何导出期望的经典相位式(7.17)和式(7.18). 回忆分束器作用在两个模上，我们分别用产生(湮没)算子 $a(a^\dagger)$ 和 $b(b^\dagger)$ 表示. Hamilton 量是

$$H_{bs}=i\theta(ab^\dagger-a^\dagger b) \tag{7.24}$$

且分束器执行酉运算

$$B=\exp[\theta(a^\dagger b-ab^\dagger)] \tag{7.25}$$

可以得出，后面也会用到的 B 在 a 和 b 上的变换

$$BaB^\dagger = a\cos\theta + b\sin\theta, BbB^\dagger = -a\sin\theta + b\cos\theta \tag{7.26}$$

我们用 Baker-Campbell-Hausdorf 公式(见练习 4.49)

$$e^{\lambda G}Ae^{-\lambda G} = \sum_{n=0}^{\infty}\frac{\lambda^n}{n!}C_n \tag{7.27}$$

验证这些关系，其中 λ 是一个复数，A，G 和 C_n 是算子，且 C_n 递归地定义为对易式(commutator)的序列 $C_0 = A, C_1 = [G, C_0], C_2 = [G, C_1], C_3 = [G, C_2], \cdots, C_n = [G, C_{n-1}]$. 由于从 $[a, a^\dagger]=1$ 和 $[b, b^\dagger]=1$ 可知，对 $G \equiv ab^\dagger - a^\dagger b$，有 $[G, a] = -b$ 且 $[G, b] = a$，我们对 $BaB^\dagger$ 的展开式系数得到 $C_0 = a, C_1 = [G, a] = b, C_2 = [G, C_1] = -a, C_3 = [G, C_2] = -[G, C_0] = -b$，一般地，

$$C_{n\text{偶数}} = i^n a \tag{7.28}$$

$$C_{n\text{奇数}} = -i^{n+1} b \tag{7.29}$$

由此，可直接得到期望的结果：

$$BaB^\dagger = e^{\theta G}ae^{-\theta G} \tag{7.30}$$

$$= \sum_{n=0}^{\infty}\frac{\theta^n}{n!}C_n \tag{7.31}$$

$$= \sum_{n\text{偶数}}\frac{(i\theta)^n}{n!}a - i\sum_{n\text{奇数}}\frac{(i\theta)^n}{n!}b \tag{7.32}$$

$$= a\cos\theta + b\sin\theta \tag{7.33}$$

变换 $BbB^\dagger$，可以通过在上面的解中简单地交换 a 和 b 得到. 注意如盒子 7.3 说明的，分束器算子是从分束器和 SU(2)代数的深刻关系产生的.

从量子逻辑门角度看，B 执行一项有用的运算. 首先注意 $B|00\rangle = |00\rangle$，即两个输入模都没有光子时，输出模也都没有光子. 当模 a 有一个光子时，回忆 $|1\rangle = a^\dagger|0\rangle$，我们得到

$$\begin{aligned} B|01\rangle &= Ba^\dagger|00\rangle = Ba^\dagger B^\dagger B|00\rangle = (a^\dagger\cos\theta + b^\dagger\sin\theta)|00\rangle \\ &= \cos\theta|01\rangle + \sin\theta|10\rangle \end{aligned} \tag{7.34}$$

类似地，$B|10\rangle = \cos\theta|10\rangle - \sin\theta|01\rangle$. 因此，在 $|0_L\rangle$ 和 $|1_L\rangle$ 的状态流形上，可把 B 写作

$$B = \begin{bmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{bmatrix} = e^{i\theta Y} \tag{7.35}$$

移相器和分束器一起使用，使我们能在光学量子比特上执行任意的单量子比特运算，这是定理 4.1 的结论. 该定理断言所有的单量子比特运算都可由绕 $\hat{z}$ 轴旋转 $R_z(\alpha) = \exp(-i\alpha Z/2)$，和绕 $\hat{y}$ 轴旋转 $R_y(\alpha) = \exp(-i\alpha Y/2)$ 生成. 移相器完成的是 R_z 旋转，而分束器完成的是 R_y 旋转.

盒子 7.3　SU(2)对称与量子分束器

在 Lie 群 SU(2)与两个耦合的谐振子的代数之间有有趣的联系，有助于理解量子分束器变换. 建立对应

$$a^\dagger a - b^\dagger b \to Z \tag{7.36}$$

$$a^\dagger b \to \sigma_+ \tag{7.37}$$

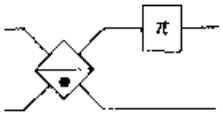
$$ab^\dagger \to \sigma_- \tag{7.38}$$

其中 Z 是 Pauli 算子，且 $\sigma_\pm = (X \mp iY)/2$ 是 Pauli 算子 X 和 Y 定义的提升和递降算子. 从 $a, a^\dagger, b,$ 和 $b^\dagger$ 的对易关系容易验证，这些定义满足 Pauli 算子的普通对易关系，见式(2.40). 而且注意总数算子 $a^\dagger a + b^\dagger b$ 与 σ_z, σ_+ 和 σ_- 如所料是可对易的，它是在 SU(2)空间中旋转下的一个不变量. 当 $\hat{n}$ 取为 $-\hat{y}$ 轴时，把 $X = a^\dagger a + bb^\dagger$ 和 $Y = -i(a^\dagger b - ab^\dagger)$ 用到 SU(2)中传统的旋转算子

$$R(\hat{n}, \theta) = e^{i\theta \hat{n}\cdot\vec{J}} \tag{7.39}$$

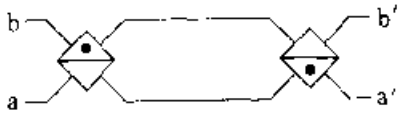
给出期望的分束器算子.

练习 7.9(光学 Hadamard 门)　证明如下线路，在双轨单光子态上的作用是一个 Hadamard 门，即，除了一个全局相位有 $|01\rangle \to (|01\rangle + |10\rangle)/\sqrt{2}$ 且 $|10\rangle \to (|01\rangle - |10\rangle)/\sqrt{2}$. 见图

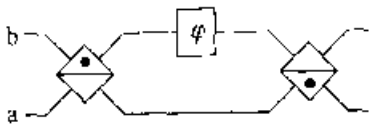


练习 7.10(Mach-Zehnder 干涉仪)　干涉仪是测量小的相移的光学工具，由两个分束器构成. 它的基本操作原理可通过这里的简单练习了解.

(1) 注意到如下线路完成恒等运算：



(2) 计算这个线路作为相移 φ 的函数(在双轨态上)执行的旋转运算：



练习 7.11　对 $\theta = \pi/4$，求 $B|0,2\rangle$.

练习 7.12(具有经典输入的量子分束器)　$|\alpha\rangle$ 和 $|\beta\rangle$ 是式(7.16)中的两个相干态. 求 $B|\alpha\rangle|\beta\rangle$ $\left(\text{提示：}|n\rangle = \dfrac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle\right)$.

3. 非线性 Kerr 介质

Kerr 介质最重要的效应是，它提供了光的两个模之间的交叉相位调制. 这在经典世界中描述为式(7.19)中的 n_2 项，实际上是在 Kerr 介质中原子的调制下光子的相互作用. 从量子力学角度看，这个效应由 Hamilton 量

$$H_{\text{xpm}} = -\chi a^{\dagger} a b^{\dagger} b \tag{7.40}$$

描述，其中 a 和 b 描述穿过介质的两个模，且对一个长为 L 的晶体，我们得到酉变换

$$K = \mathrm{e}^{\mathrm{i}\chi L a^{\dagger} a b^{\dagger} b} \tag{7.41}$$

χ 是与 n_2 有关的系数，而三阶非线性灵敏度系数通常记作 $\chi^{(3)}$. 由这个 Hamilton 量导出的经典期望行为留作练习 7.14.

将 Kerr 介质和分束器结合，可按如下方式构造一个受控非门. 对单光子状态，我们得到

$$K \mid 00\rangle = \mid 00\rangle \tag{7.42}$$

$$K \mid 01\rangle = \mid 01\rangle \tag{7.43}$$

$$K \mid 10\rangle = \mid 10\rangle \tag{7.44}$$

$$K \mid 11\rangle = \mathrm{e}^{\mathrm{i}\chi L} \mid 11\rangle \tag{7.45}$$

且取 $\chi L = \pi$，使得 $K|11\rangle = -|11\rangle$. 现在考虑两个双轨态，即光的四个模，这些态处于一个由四个基态 $|e_{00}\rangle = |1001\rangle$，$|e_{01}\rangle = |1010\rangle$，$|e_{10} = |0101\rangle$，$|e_{11} = |0110\rangle$ 张成的空间中. 注意为了方便(物理上，用镜子很容易对换两个模)，我们把第一个对的两个模的通常顺序翻转了. 现在，若 Kerr 介质作用到中间两个模上，则除了 $K|e_{11}\rangle = -|e_{11}\rangle$，对所有 i 得到 $K|e_i\rangle = |e_i\rangle$. 这是有用的，因为受控非门运算可以分解成

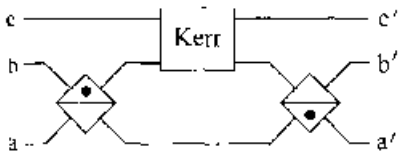
$$\underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}}_{U_{CN}} = \underbrace{\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{I \otimes H} \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}}_{K} \underbrace{\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{I \otimes H} \tag{7.46}$$

其中 H 是单量子比特 Hadamdard 变换(用分束器和移相器已实现)，而 K 是我们刚刚考虑过的 Kerr 相互作用，其中 $\chi L = \pi$. 这样的设备，如盒子 7.4 描述，可用来构造可逆光学逻辑门.

总之，受控非门 CNOT 可以从 Kerr 介质构造，且任意单量子比特运算可以用分束器和移相器实现. 单光子可以由衰减的激光产生，而用光探测器检测. 因此，理论上说，量子计算机可以用这些光学器件实现.

盒子 7.4　量子光学 Fredkin 门

用两个分束器和一个非线性 Kerr 介质可以如这个框图建造一个光学 Fredkin 门.



这个线路执行酉变换 $U=B^{\dagger}KB$，其中 B 是 50/50 分束器，K 是 Kerr 交叉相位调制算子 $K=e^{i\xi b^{\dagger}b c^{\dagger}c}$，而 $\xi=\chi L$ 是耦合常数与相互作用距离的乘积. 这给出

$$U=\exp\left[i\xi c^{\dagger}c\left(\frac{b^{\dagger}-a^{\dagger}}{2}\right)\left(\frac{b-a}{2}\right)\right] \tag{7.47}$$

$$=e^{i\frac{\xi}{2}b^{\dagger}b}e^{\frac{\xi}{2}c^{\dagger}c(a^{\dagger}b-b^{\dagger}a)}e^{-i\frac{\xi}{2}a^{\dagger}a}e^{-i\frac{\xi}{2}b^{\dagger}b}e^{i\frac{\xi}{2}a^{\dagger}a c^{\dagger}c}e^{i\frac{\xi}{2}b^{\dagger}b c^{\dagger}c} \tag{7.48}$$

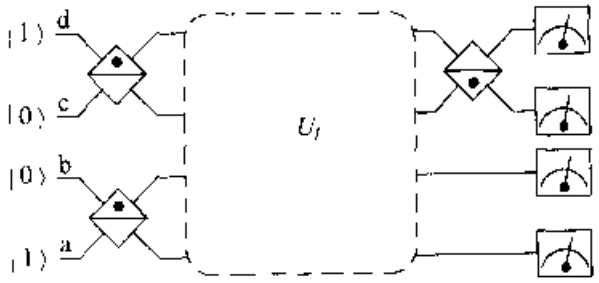
第一和第三个指数是固定相移，而最后两个相移来自交叉相位调制. 所有这些效应都是非本质的，可以被补偿. 有意义的项是第二个指数，它定义了量子 Fredkin 算子

$$F(\xi)=\exp\left[\frac{\xi}{2}c^{\dagger}c(a^{\dagger}b-b^{\dagger}a)\right] \tag{7.49}$$

对 $\xi=\pi$ 就得到普通(经典)Fredkin 门运算. 在这种情形下若没有光子输入到 c，则 $a'=a,b'=b$. 但若一个单光子输入到 c，则 $a'=b$ 且 $b'=a$. 通过认识到 $F(\chi)$ 像一个转角为 $\xi c^{\dagger}c$ 的受控分束器算子，就可以理解这一点. 注意这个描述没有用到双轨表示，在那个表示中，这个 Fredkin 门对应于一个受控非门.

练习 7.13（光学 Deutsch-Jozsa 量子线路）　在 1.4.4 节中，我们描述了用来解一个比特 Deutsch-Josza 问题的量子线路. 这里是该线路对单光子态采用分束器、移相器和非线性 Kerr 介质的版本：

(1) 用 Fredkin 门和分束器为四种可能的经典函数 U_f 构造如图线路.



(2) 在此结构中为什么不需要移相器?

(3) 对每个 U_f，具体说明怎样用干涉解释量子算法如何工作.

(4) 若用相干态代替单光子,这个实现还成立吗?

练习 7.14(经典交叉相位调制) 为考察从 K 的定义,式(7.41),导出的 Kerr 介质的期望经典行为,把它应用到两个模,一个模处子相干态而另一个处于状态 $|n\rangle$. 即,证明

$$K\,|\,\alpha\rangle\,|\,n\rangle = |\,\alpha e^{i\chi t n}\rangle\,|\,n\rangle \tag{7.50}$$

利用此式计算

$$\rho_a = \mathrm{tr}_b[K\,|\,\alpha\rangle\,|\,\beta\rangle\langle\beta\,|\,\langle\alpha\,|\,K^\dagger] \tag{7.51}$$

$$= e^{-|\beta|^2}\sum_m \frac{|\beta|^{2m}}{m!}\,|\,\alpha\, e^{i\chi t m}\rangle\langle\alpha e^{i\chi t m}\,| \tag{7.52}$$

并证明和的主要贡献来自 $m=|\beta|^2$ 项.

7.4.3 不足

量子比特的单光子表示非常吸引人. 单光子的产生和测量相对简单,并且在双轨表示中,单量子比特的任意运算都是可能的. 不幸的是,和光子发生作用是困难的——最好的非线性 Kerr 介质的能力也很弱,不能提供单光子态之间的 π 交叉相位调制. 事实上,因为非线性折射率常通过用接近光学共振的介质获得,伴随非线性总有某种吸收,可从理论上估计最好情况下为一个光子得到 π 交叉相位调制,必须有近 50 个光子被吸收. 这意味着用传统非线性光学器件建造量子计算机的前景并不乐观.

然而,通过对这样的光学量子计算机的研究,我们对量子计算机的体系结构的性质和系统的设计获得许多有价值的了解. 我们现在可以看到实验室中一台实际量子计算机可能的样子(只要有足够好的器件来构造它),一个显著特点是它几乎完全用光学干涉仪构成. 在这套装置中,信息用光子的数目和光子的相位编码,而干涉仪用来在两种表示之间转换. 虽然构造稳定的光学干涉仪是可行的,但如果另外选择了量子比特的大数字表示,那么建造稳定干涉仪会很快因缺少典型 de Broglie波长而变得困难. 即使是采用光学表示,在实验室稳定实现大规模量子算法所需要的多重互锁干涉仪也是具有挑战性的.

历史上,光学经典计算机曾被认为有希望代替电子机器,但由于没有发现足够非线性的光学材料,和它们在速度与并行上的优势,没能充分弥补它们在校准和能耗上的不足,它们最终没有达到预期效果. 另一方面,光通信是一个活跃而重要的研究领域,一个原因是对于超过 1cm 的距离上,用光子在光纤上传送一个比特需要的能量,比对同样长度的典型 50Ω 电线充电需要的能量要小. 类似地,光学量子比特也可能在如量子密码系统的量子信息通信领域,而不是在计算中,得到自然的应用.

尽管光学量子计算机的实现面临这些不足,描述其理论体系对本章剩余部分将研究的所有其他实现,绝对是有根本性意义的. 事实上,读者可以把我们下面要

考虑的实现视为不过是其他类型的光学计算机，只是具有不同(更好的!)类型的非线性介质而已.

光子量子计算机的一些基本特征如下.

• 量子比特的表示：单光子在两个模|01⟩和|10⟩之间的位置、或极化度(polarization).

• 酉演化：由移相器(R_z旋转)、分束器(R_x旋转)和非线性 Kerr 介质构造任意变换. 非线性 Kerr 介质允许两个单光子进行交叉相位调制，作用是 $\exp[i\chi L_z|11\rangle\langle 11|]$.

• 初态制备：产生单光子态(例如通过衰减激光).

• 输出：探测单光子(例如用光电倍增管).

• 不足：交叉相位调制强度比吸收损失大的非线性 Kerr 介质难以实现.

7.5 光学共振腔量子电动力学

腔量子电动力学(cavity quantum electrodynamics，C QED) 是涉及单个原子和少量光学模之间耦合的一个重要研究领域. 把单个原子置于具有很高 Q 值的光学共振腔中，使这方面的研究在实验上成为可能，因为在共振腔中只有一个或两个电磁模，并且每个模都具有很高的电场强度，原子和该场的偶极耦合强度很高. 由于高 Q 值，共振腔中的光子有机会在逃逸之前与原子进行多次相互作用. 理论上，这项技术为控制和研究单量子系统提供了独特的机会，为量子混沌、量子反馈控制和量子计算带来许多机会.

实践中，单原子 C QED 方法为上节描述的光学量子计算机的困境提供了潜在的解决办法. 单光子虽然是量子信息很好的载体，但它们需要某些其他介质才能相互作用. 传统非线性光学 Kerr 介质因为是块材料(bulk material)，而无法满足这项要求. 然而，被隔离得很好的单原子可以不必遇到同样的退相干效应的问题，而且，它们也能提供光子间的交叉相位调制. 如果相互作用能够得到控制，那么单光子的状态能在单原子之间有效传递会带来什么？这个可能的构思就是本节的主题.

7.5.1 物理装置

C QED 的两个主要实验器件是电磁共振腔和原子. 我们从描述共振模的基本物理性质开始，然后总结原子结构以及原子和光相互作用的基本内容.

1. Fabry-Perot 共振腔

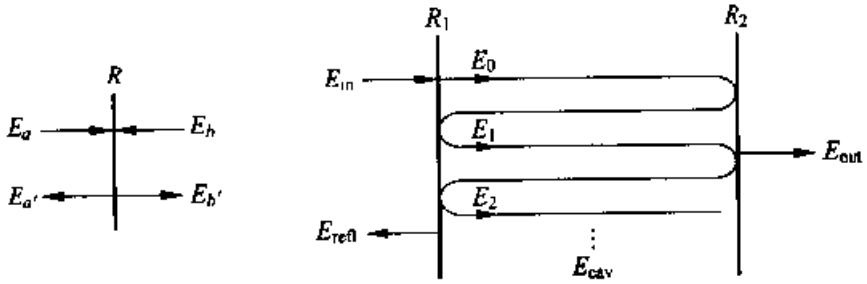
C QED 涉及的主要相互作用是，电偶极矩 $\boldsymbol{d}$ 和电场 $\boldsymbol{E}$ 之间的偶极相互作用 $\boldsymbol{d}\cdot\boldsymbol{E}$. 这个相互作用能有多强？实践中改变 $\boldsymbol{d}$ 的大小不容易，不过，实验上容易控

盒子 7.5 Fabry-Perot 共振腔

Fabry-Perot 共振腔的一个基本元件是部分镀银的镜子，入射光 E_a 和 E_b 部分反射和部分透过，产生输出场 $E_{a'}$ 和 $E_{b'}$. 它们由酉变换

$$\begin{bmatrix} E_{a'} \\ E_{b'} \end{bmatrix} = \begin{bmatrix} \sqrt{R} & \sqrt{1-R} \\ \sqrt{-R} & -\sqrt{R} \end{bmatrix} \begin{bmatrix} E_a \\ E_b \end{bmatrix} \tag{7.53}$$

联系起来，其中 R 是镜子的反射率，而“—”号的位置为了方便按习惯定出. 见图



如图所示，Fabry-Perot 共振腔由反射率为 R_1 和 R_2 的两面平行的镜子组成. 光 E_{in} 由外界入射，在共振腔内，光在两面镜子之间来回振荡，每个来回场都增加相移 $e^{i\varphi}$，φ 是路径长度和光的频率的函数. 因此，利用式(7.53)，我们求出振荡器内部场强为

$$E_{cav} = \sum_k E_k = \frac{\sqrt{1-R_1}E_{in}}{1+e^{i\varphi}\sqrt{R_1R_2}} \tag{7.54}$$

其中 $E_0 = \sqrt{1-R_1}E_{in}$，且 $E_k = -e^{i\varphi}\sqrt{R_1R_2}E_{k-1}$. 类似地，我们求出 $E_{out} = e^{i\varphi/2}\sqrt{1-R_2}$，且 $E_{refl} = \sqrt{R_1}E_{in} + \sqrt{1-R_1}\sqrt{R_2}e^{i\varphi}E_{cav}$.

对我们而言，Fabry-Perot 共振腔最重要的一个特征量是，作为输入功率和场频率函数的共振腔内部场的功率，即

$$\frac{P_{cav}}{P_{in}} = \left|\frac{E_{cav}}{E_{in}}\right|^2 = \frac{1-R_1}{|1+e^{i\varphi}\sqrt{R_1R_2}|^2} \tag{7.55}$$

有两方面值得注意. 首先，频率的选择性由 $\varphi=\omega d/c$ 的事实决定，其中 d 是镜子之间的距离，c 是光速，而 ω 是场的频率. 物理上，它来源于共振腔场和表明反射光之间的建设性和破坏性干涉. 其次，在共振情形下，共振腔场达到最大值，接近入射场的 $1/(1-R)$ 倍，这条性质对 C-QED 极有价值.

制 $|E|$，而在一个窄的频带和体积小的空间中，实现很强的电场的最重要的工具是 Fabry-Perot 共振腔.

近似假定电场是单色的，且占据单个空间模，可以给出它的一个非常简单的量子力学描述

$$E(r) = i\varepsilon E_0[ae^{ikr} \quad a^+e^{-ikr}] \tag{7.56}$$

如盒子 7.5 中描述的，这些近似对 Fabry-Perot 共振腔中的场是适用的. 这里 $k=\omega/c$ 是光的空间频率，E_0 是场强，ε 是极化率，而 r 是场的期望位置. a 和 a^+ 是在此模中光子的产生和湮没算子，其行为如 7.4.2 节所述. 注意共振腔中决定场的演化的 Hamilton 量就是

$$H_{\text{field}} = \hbar\omega a^+ a \tag{7.57}$$

且这与能量是 $|E|^2$ 共振腔中体积积分的半经典概念一致.

练习 7.15　对 $R_1=R_2=0.9$ 绘出场失谐量 φ 的函数式(7.55)的图像.

2. 双能级原子

直到本章的本节，我们都在讨论光子，或光子间通过半经典介质的交叉相位调制实现的相互作用. 现在，我们把注意力转向原子，它们的电子结构和它们与光子的相互作用. 这当然是一个已经研究得非常深入和成熟的领域，我们只描述量子计算涉及的一小部分.

原子的电子本征能态可能是非常复杂的(见盒子 7.6)，但把原子建模为仅包含两个状态，对我们来说已是极好的近似. 这个双能级原子近似是有效的，因为我们考虑的是和单色光的相互作用，在这种情形下，惟一相关的能级满足两个条件：它们的能量差与入射光子的能量匹配，而且对称性(选择规则)不禁止这个跃迁. 这些条件来源于基本的能量、角动量和宇称守恒定律. 能量守恒无非是

$$\hbar\omega = E_2 - E_1 \tag{7.58}$$

其中 E_2 和 E_1 是原子的两个本征能. 角动量和宇称守恒的要求，可以通过考虑两个轨道波函数之间 $\hat{r}$ 的矩阵元素 $\langle l_1, m_1|\hat{r}|l_2, m_2\rangle$ 来说明. 不失一般性，我们可以取 $\hat{r}$ 位于 $\hat{x}-\hat{y}$ 平面，使得它可被表为球谐函数(盒子 7.6)形式

$$\hat{r} = \sqrt{\frac{3}{8\pi}}[(-r_x + ir_y)Y_{1,-1} + (r_x + ir_y)Y_{1,1}] \tag{7.59}$$

在这个基中，$\langle l, m_1|\hat{r}|l, m_2\rangle$ 的相应元是

$$\int Y^*_{l_1 m_1} Y_{1m} Y_{l_2 m_2} \mathrm{d}\Omega \tag{7.60}$$

回忆 $m=\pm 1$，这个积分只有当 $m_2-m_1=\pm 1$ 且 $\Delta l=\pm 1$ 时为非 0. 与 $\langle l, m_1|\hat{r}|l, m_2\rangle$ 相关的偶极近似下，前一个条件是角动量守恒，第二个条件是宇称守恒. 这些条件是原子双能级近似中重要的选择定则.

练习 7.16(电偶极子选择定则)　证明式(7.60)，只有当 $m_2-m_1=\pm 1$ 且 $\Delta l=\pm 1$ 时为非 0.

在现实中，光永远不是完全单色的，从如激光器的源中产生后，纵模、抽运噪声和其他因素引起有限的线宽. 而且与外界耦合的原子永远不可能处在完全确定的

盒子 7.6 原子的能级

原子中的电子的行为像是三维盒子中的一个粒子，其 Hamilton 量为

$$H_{\mathrm{A}}=\sum_{k}\frac{|\boldsymbol{p}_k|^2}{2m}-\frac{Ze^2}{r_k}+H_{\mathrm{rel}}+H_{\mathrm{ee}}+H_{\mathrm{so}}+H_{\mathrm{hf}} \tag{7.61}$$

其中前两项描述电子的动能，电子负电荷与核子的正电荷之间的 Coulomb 引力之间的平衡；H_{rel}是相对论修正项；H_{ee}描述电子-电子耦合及电子 Fermi 子性质的贡献；H_{so}是自旋轨道相互作用，可以解释为电子的自旋与电子绕原子运动产生磁场之间的相互作用；H_{hf}是超精细相互作用，即电子自旋与核子产生的磁场之间的相互作用. H_{A} 的本征能态可按照三个整数或半整数(量子数)很好地分类：n，主量子数；l，轨道角动量；和 m，l 的 $\hat{z}$ 分量. 另外，总电子自旋 S，和核自旋 I 常常也是重要的. H 的特征值由 n 大概确定到 α^2 阶，由 H_{ee}确定到较小阶，由 H_{rel}和 H_{so}确定到 α^4 阶，且由 H_{hf}确定到约为 $10^{-3}\alpha^4$阶，其中 $\alpha=1/137$是无量纲的精细结构常数.

n 可以从盒子中一个量子的一维 Schrödinger 方程的解很容易推导，因为 Coulomb 约束位势只依赖于径向距离. 不过，轨道角动量需要一些说明，它是一个三维量. 电子的本质特征在子 H_{A} 的坐标表示对角度的依赖. 其中 $\boldsymbol{p}$ 成为 Laplace算子∇^2，给出 Schrödinger 方程

$$\frac{\Phi(\varphi)}{\sin\theta}\frac{\mathrm{d}}{\mathrm{d}\theta}\left(\sin\theta\frac{\mathrm{d}\Theta}{\mathrm{d}\theta}\right)+\frac{\Theta(\theta)}{\sin^2\theta}\frac{\mathrm{d}^2\Phi(\varphi)}{\mathrm{d}\varphi^2}+l(l+1)\Theta(\theta)\Phi(\varphi)=0 \tag{7.62}$$

其中 θ 和 φ 是通常的球坐标，而 Φ 和 Θ 是特征函数. 解 $\mathrm{Y}_{lm}(\theta,\varphi)=\Theta_{lm}(\theta)\Phi_m(\varphi)$是球谐函数(spherical harmonics)

$$\mathrm{Y}_{lm}(\theta,\varphi)\equiv(-1)^m\sqrt{\frac{2l+1}{4\pi}\frac{(l-m)!}{(l+m)!}}\mathrm{P}_{lm}(\cos\theta)\mathrm{e}^{\mathrm{i}m\varphi} \tag{7.63}$$

其中 P_{lm}是常用的 Legendre 函数

$$\mathrm{P}_{lm}(x)=\frac{(1-x^2)^{m/2}}{2^l l!}\frac{\mathrm{d}^{m+l}}{\mathrm{d}x^{m+l}}(x^2-1)^l \tag{7.64}$$

这些式中，$-l\leqslant m\leqslant l$，且可以证明 m 和 l 必须是整数或半整数. l 是轨道角动量，m 是它沿 $\hat{z}$ 轴的分量. 类似地，电子自旋 S 和核自旋 I 具有分量 m_s 和 m_i. 如上所述，原子的能态描述可能非常复杂！总之，对我们而言，可以认为原子的本征能由七个数决定：n,l,m,S,m_s,I,m_i.

本征能态，附加振荡电位势，或者甚至与真空的相互作用，都可以引起能级的不确定而使之变成具有有限宽度的一个分布.

不过，仔细选择原子和激发能，并利用选择定则，有可能使原子的双能级近似很好地成立. 整个过程的关键点是在这个近似中，若$|\psi_1\rangle$和$|\psi_2\rangle$是两个被选择的能级，则$\hat{r}$的矩阵元素为

$$r_{ij} = \langle \psi_i | \hat{r} | \psi_j \rangle \approx r_0 Y \tag{7.65}$$

其中r_0是某个常数，而Y是Pauli算子(2.1.3节，这里得到Y而不是X，只是为方便后面的讨论)，这与原子和入射电场的相互作用有关系. 原子的Hamilton量在双能级子空间就是

$$H_{\text{atom}} = \frac{\hbar\omega_0}{2} Z \tag{7.66}$$

其中$\hbar\omega_0$是两个能级之间的差，因为两个状态都是本征能态.

7.5.2 Hamilton量

在原子的双能级近似中，可以用简单得多的模型来近似原子和限制在共振腔中的电场之间的相互作用$\boldsymbol{d}\cdot\boldsymbol{E}$. 我们利用共振腔场的量子化和电子尺寸相对场的波长很小的事实，根据$\boldsymbol{d}\propto\hat{r}$的事实(电偶极子的大小是电荷乘距离)，结合式(7.56)和式(7.65)，可得到相互作用的形式

$$H_I = -\mathrm{i}gY(a - a^\dagger) \tag{7.67}$$

其中我们取$r=0$作为原子的位置(因此也是计算$\boldsymbol{E}$的点)，且把原子定向为使得$\hat{r}$与电场方向一致，g是某个描述相互作用强度的常数(这里我们不需要关心它的具体值，只需要关心这种形式). i的出现只是为了保证g是实数，因为H_I必须是Hermite的. 注意到H_I包含一般的小项，它可以被进一步简化，为此，定义Pauli提升和递降算子

$$\sigma_\pm = \frac{X \pm \mathrm{i}Y}{2} \tag{7.68}$$

使我们可以将H_I重新表达为

$$H_I = g(\sigma_+ - \sigma_-)(a - a^\dagger) \tag{7.69}$$

包含$\sigma_+ a^\dagger$和$\sigma_- a$的项在频率ω和ω_0的两倍处振荡，忽略它们是一个很好的近似(旋波近似(rotating wave approximation))，可导出总Hamilton量$H = H_{\text{atom}} + H_{\text{field}} + H_I$

$$H = \frac{\hbar\omega_0}{2} Z + \hbar\omega a^\dagger a + g(a^\dagger\sigma_- + a\sigma_+) \tag{7.70}$$

其中有必要重申一下：Pauli算子作用在双能级原子上，$a^\dagger$、a是单模场上的提升(产生)和递降(湮灭)算子，ω是场的频率，ω_0是原子的频率，而g是原子和场之间相互作用的耦合常数. 该量是研究C-QED的基本理论工具，称为Jaynes-Cummings Hamilton量，它描述了双能级原子和电磁场的相互作用.

注意到 $N=a^{\dagger}a+Z/2$ 是关于运动的常量，即 $[H,N]=0$，故这个 Hamilton 量可以写成另一种方便的形式

$$H=\hbar\omega N+\delta Z+g(a^{\dagger}\sigma+a\sigma_{+}) \tag{7.71}$$

其中 $\delta=(\omega_0-\omega)/2$ 是失谐量(detuning)——即场和原子共振之间的频率差. 这个 Jaynes-Cummings Hamilton 量非常重要，我们将利用本章剩余的近乎全部篇幅来研究它的性质和在不同物理系统中的表现形式.

练习 7.17(Jaynes-Cummings Hamilton 量的本征态) 证明

$$|\chi_n\rangle=\frac{1}{\sqrt{2}}[|n,1\rangle+|n+1,0\rangle] \tag{7.72}$$

$$|\bar{\chi}_n\rangle=\frac{1}{\sqrt{2}}[|n,1\rangle-|n+1,0\rangle] \tag{7.73}$$

是 Jaynes-Cummings Hamilton 量，式(7.71)对 $\omega=\delta=0$ 的本征态，其特征值为

$$H|\chi_n\rangle=g\sqrt{n+1}\,|\chi_n\rangle \tag{7.74}$$

$$H|\bar{\chi}_n\rangle=-g\sqrt{n+1}\,|\bar{\chi}_n\rangle \tag{7.75}$$

其中右矢的标号为|场，原子⟩.

7.5.3 单光子单原子吸收与折射

对我们来说，C-QED 中最有趣的内容是与单原子的相互作用的单光子. 这是个非同寻常的问题，这里经典电磁学理论的传统观念(如折射率和电容率)会失效. 特别地，我们希望利用单原子得到光子间的非线性相互作用.

让我们从展示 Rabi 振荡的原子-场系统的惊人而普遍的特性开始. 不失一般性，因为它只是贡献一个固定相位，所以可以忽略 N. 回忆系统的时间演化由 $U=e^{-iHt}$(这里和下面，省略 $\hbar$ 是方便的，我们在必要时总是这样做)给出，并且注意场模中最多有一个单个激发的情形，其中

$$H=-\begin{bmatrix}\delta & 0 & 0\\ 0 & \delta & g\\ 0 & g & -\delta\end{bmatrix} \tag{7.76}$$

(从左到右，从上到下，基态是|00⟩，|01⟩，|10⟩，其中左边的标号对应场，右边的标号对应原子)，可得到

$$\begin{aligned}U=&e^{-i\delta t}\,|00\rangle\langle 00|\\&+\left(\cos\Omega t+i\frac{\delta}{\Omega}\sin\Omega t\right)|01\rangle\langle 01|\\&+\left(\cos\Omega t-i\frac{\delta}{\Omega}\sin\Omega t\right)|10\rangle\langle 10|\\&-i\frac{g}{\Omega}\sin\Omega t(|01\rangle\langle 10|+|10\rangle\langle 01|)\end{aligned} \tag{7.77}$$

我们关心的是此式的最后一行，它显示原子和场来回以 Rabi 频率 $\Omega=\sqrt{g^2+\delta^2}$ 振荡，来交换一个量子的能量.

练习 7.18(Rabi 振荡) 通过式

$$e^{i\hat{n}\cdot\sigma\theta}=\cos|n|+i\hat{n}\cdot\sigma\sin|n| \tag{7.78}$$

来对 H 求幂以证明式(7.77). 这是 Rabi 振荡和 Rabi 频率的特别简单的一个推导：通常，我们要解耦合的微分方程来计算 Ω，但这里我们通过仅仅注意单原子和单光子子空间，就得到 Rabi 振荡的本质动态.

与一个单原子相互作用的光子的变化，可以由跟踪原子状态(2.4.3 节)得到. 初始状态为$|1\rangle$的光子，被原子(假设开始时处于基态$|0\rangle$)吸收的概率是

$$\chi_1=\sum_k|\langle 0k|U|10\rangle|^2=\frac{g^2}{g^2+\delta^2}\sin^2\Omega t \tag{7.79}$$

它具有通常预期的，作为相对共振失谐量 δ 函数的 Lorentz 吸收分布.

(单光子的)折射率由 U 在原子处于基态的矩阵元给出，光子的相移是场的$|1\rangle$和$|0\rangle$状态经过原子时，经历的旋转角的差，可以给出其为

$$\chi_2=\arg\left[e^{i\delta t}\left(\cos\Omega t-i\frac{\delta}{\Omega}\sin\Omega t\right)\right] \tag{7.80}$$

对于固定的非 0 的 δ，随耦合 g 减弱，吸收概率 χ_1 按 g^2 减小，但相移 χ_2 几乎保持为定常. 这是材料能够进行相移而不散射太多光的根本原因.

练习 7.19(Lorentz 吸收分布) 对 $t=1$ 和 $g=1.2$，画出式(7.79)作为失谐量 δ 的函数的图像和相应的经典结果(如果读者知道). 并说明振荡的原因是什么?

练习 7.20(单光子相移) 从 U 推导式(7.80)，且对 $t=1$ 和 $g=1.2$ 画出它作为失谐量 δ 函数的图像，并与 δ/Ω^2 比较.

原子-光子相互作用的一个自然应用是研究两个不同的光子模(每个模最多包含一个光子)与同一原子相互作用，这可以导致两个模之间的非线性相互作用. 回忆 7.4.2 节中，非线性 Kerr 介质表象上，可以描述为引起具有形如 $H=\chi a^\dagger a b^\dagger b$ 的 Hamilton 量的一个交叉相位调制的介质. 在那里，我们没有考察这种效应如何从基本相互作用产生. 在现在的框架下，可以用一个简单模型来解释 Kerr 效应. 其中两束偏振光与一个三能级原子相互作用，如图 7.4 所示. 这可用修改的 Jaynes-Cummings Hamilton 量描述

$$\begin{aligned}H=&\delta\begin{bmatrix}-1&0&0\\0&1&0\\0&0&1\end{bmatrix}+g_a\left(a\begin{bmatrix}0&0&0\\1&0&0\\0&0&0\end{bmatrix}+a^\dagger\begin{bmatrix}0&1&0\\0&0&0\\0&0&0\end{bmatrix}\right)\\&+g_b\left(b\begin{bmatrix}0&0&0\\0&0&0\\1&0&0\end{bmatrix}+b^\dagger\begin{bmatrix}0&0&1\\0&0&0\\0&0&0\end{bmatrix}\right)\end{aligned} \tag{7.81}$$

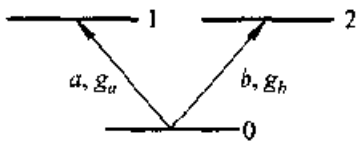


图 7.4 与算子 a 和 b 描述的两束正交偏振光相互作用的三能级原子(能级为 0,1,2). 原子-光子耦合分别为 g_a 和 g_b. 假定 0 和 1,以及 0 和 2 之间的能量差为几乎相等.

其中对应 3×3 原子算子的基底元素是$|0\rangle, |1\rangle, |2\rangle$. 在矩阵表示中,$H$ 中的有关项是块对角矩阵

$$H = \begin{bmatrix} H_0 & 0 & 0 \\ 0 & H_1 & 0 \\ 0 & 0 & H_2 \end{bmatrix} \tag{7.82}$$

其中在对 H_0 的$|a,b,$原子$\rangle = |000\rangle$,对 H_1 的$|100\rangle, |001\rangle, '010\rangle$,$|002\rangle$,对 H_2 的$|110\rangle, |011\rangle, |102\rangle$的基底下,将列从左到右排,有

$$H_0 = -\delta \tag{7.83}$$

$$H_1 = \begin{bmatrix} -\delta & g_a & 0 & 0 \\ g_a & \delta & 0 & 0 \\ 0 & 0 & -\delta & g_b \\ 0 & 0 & g_b & \delta \end{bmatrix} \tag{7.84}$$

$$H_2 = \begin{bmatrix} -\delta & g_a & g_b \\ g_a & \delta & 0 \\ g_b & 0 & \delta \end{bmatrix} \tag{7.85}$$

求幂 $U = \exp(iHt)$,可得单光子相移 $\varphi_a = \arg(\langle 100|U|100\rangle) - \arg(\langle 000|U|000\rangle)$ 和 $\varphi_b = \arg(\langle 010|U|010\rangle) - \arg(\langle 000|U|000\rangle)$,以及双光子相移 $\varphi_{ab} = \arg(\langle 110|U|110\rangle) - \arg(\langle 000|U|000\rangle)$. 对应线性介质,可以预料 $\varphi_{ab} = \varphi_a + \varphi_b$,即双光子态具有单光子态两倍的相移,因为 $\exp[-i\omega(a^\dagger a + b^\dagger b)]|11\rangle = \exp(-2i\omega)|11\rangle$. 然而,这个系统的行为是非线性的,如图 7.5 所示的 $\chi_3 \equiv \varphi_{ab} - \varphi_a - \varphi_b$. 在这个物理系统中,Kerr 效应源于,原子在两个光学模之间交换量子的微小幅度.

练习 7.21 对式(7.82)求幂,证明

$$\varphi_{ab} = \arg\left[e^{i\delta t}\left(\cos\Omega' t - i\frac{\delta}{\Omega'}\sin\Omega' t\right)\right] \tag{7.86}$$

其中 $\Omega' = \sqrt{\delta^2 + g_a^2 + g_b^2}$,以此计算非线性 Kerr 相移 χ_3. 这是对 Kerr 相互作用建模和理解的一条非常简单的途径,它绕过了通常经典非线性光学许多复杂的步骤.

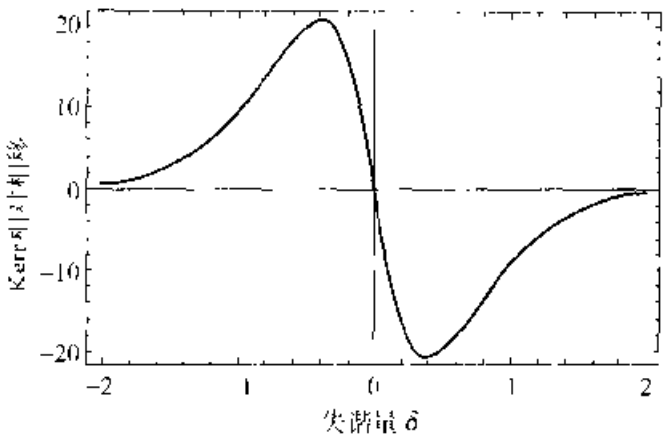


图 7.5　对 $t=0.98$、$g_a=g_b=1$ 的 Kerr 相移度数 χ_3，由对单光子和一个三能级原子计算式(7.82)得到，按失谐量 δ 的函数绘制.

练习 7.22　交叉相位调制带来一定的损失，可由原子吸收光子的概率给出. 计算这个概率，$1-\langle 110|U|110\rangle$，其中对 H，$U=\exp(-iHt)$ 如式(7.82)给出，并与作为 δ、g_a、g_b 和 t 函数的 $1-\langle 100|U|100\rangle$ 相比较.

7.5.4　量子计算

广而言之，C-QED 技术可用来以若干不同方式完成量子计算. 其中两种如下：量子信息可由光子状态表示，含有原子的共振腔提供光子间相互作用；或者用原子表示量子信息，用光子在原子间进行通信. 下面以第一种方法用于实现量子逻辑门的实验，来作为这个主题的结束.

如 7.4.2 节所述，量子计算机可由单光子态、移相器、分束器和非线性 Kerr 介质构造. 但受控非门要求的 π 交叉相位调制，用标准的块非线性光学技术几乎不可能实现. C-QED 可用于实现 7.5.3 节所述的 Kerr 相互作用；但它不像块介质，由于 Fabry-Perot 类型的共振腔提供的强场，即使在单光子水平上，它也具有很强的效应.

图 7.6 是一个 C-QED 实验的说明. 它说明用单光子实现具有酉变换

$$\begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\varphi_a} & 0 & 0 \\ 0 & 0 & e^{i\varphi_b} & 0 \\ 0 & 0 & 0 & e^{i(\varphi_a+\varphi_b-\Delta)} \end{vmatrix} \tag{7.87}$$

的逻辑门的可能性(见本章末的“历史和进一步阅读的材料”)，其中 $\Delta=16°$. 在该实验中，制备具有弱相干态的光的两个模(相差一个很小的频率)，一个是线性偏振

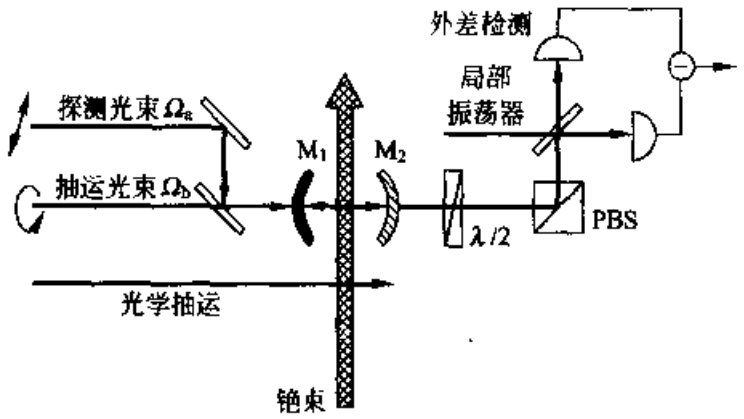


图 7.6 用于演示，以单原子提供单光子间交叉相位调制可能性的，基本量子逻辑门的实验装置框图. 弱的线偏振探测光束 Ω_a 和强一些的圆偏振抽运光束 Ω_b 被制备出来，并射入具有高反射率镜子 M_1 和 M_2 的光学共振腔. 铯原子被以光学抽运（图中显示原子的方向相反）制备成电子态 $6S_{1/2}, F=4, m=4$，使得共振腔中的平均原子数大约是 1. 光穿过共振腔，与原子相互作用；σ_+ 偏振光引起向 $6P_{3/2}, F'=5, m'=5$ 状态的强跃迁，而正交的 σ_- 偏振光引起向 $6P_{3/2}, F'=5, m'=3$ 状态的弱跃迁. 输出光的偏振用一种极化分束器（PBS）半波片和一种灵敏的平衡外差检测器（可以选择性地探测特定的由局部振荡器决定的频率的光）测量（本图得到 Q. Turchette 的允许）.

的（探测），而另一个是圆偏振的（抽运），作为共振腔的输入. 这个状态可用表为

$$|\psi_{in}\rangle = |\beta^+\rangle\left[\frac{|\alpha^+\rangle + |\alpha^-\rangle}{\sqrt{2}}\right] \tag{7.88}$$

这里需要回想线偏振光是两个可能的圆偏振状态“+”和“−”的均匀叠加. 把弱相干态近似为 $|\alpha\rangle \approx |0\rangle + \alpha|1\rangle$，对 $|\beta\rangle$ 也有类似结果（暂不考虑归一化），可得出

$$|\psi_{in}\rangle \approx [|0^+\rangle + \beta|1^+\rangle]\,[|0^+\rangle + \alpha|1^+\rangle + |0^-\rangle + \alpha|1^-\rangle] \tag{7.89}$$

这些光子穿过光学共振腔且与原子相互作用. 对于每种偏振态（独立于光子所在的模）中光子的总数，原子可引起状态的不同相移. 特别地，我们假设处于 $|1^+\rangle$ 的光子在探测光束中有 $e^{i\varphi_a}$ 的相移，在抽运光束中时有 $e^{i\varphi_b}$ 的相移. 除了这个单光子相移，状态 $|1^+1^+\rangle$ 还有一个附加的 Kerr 相移 Δ，于是变成 $e^{i(\varphi_a+\varphi_b+\Delta)}|1^+1^+\rangle$，其他状态（特别是其他偏振）没有变化. 引起这种行为的物理机制类似于 7.5.3 节的描述，而最终的效果是相同的：抽运和探测光之间的一个交叉相位调制. 于是从共振腔的输出是

$$\begin{aligned}|\psi_{out}\rangle \approx{}& |0^+\rangle[|0^+\rangle + \alpha e^{i\varphi_a}|1^+\rangle + |0^-\rangle + \alpha|1^-\rangle] \\ &+ e^{i\varphi_b}\beta|1^+\rangle[|0^+\rangle + \alpha e^{i(\varphi_a+\Delta)}|1^+\rangle + |0^-\rangle + \alpha|1^-\rangle] \qquad (7.90)\\ \approx{}& |0^+\rangle|\alpha, \varphi_a/2\rangle + e^{i\varphi_b}\beta|1^+\rangle|\alpha, (\varphi_a+\Delta)/2\rangle \qquad (7.91)\end{aligned}$$

其中$|\alpha,\varphi_a/2\rangle$表示一个线偏振探测场绕垂直方向旋转$\varphi_a/2$.场的偏振由探测器测量，给出$\varphi_a\approx 17.5°$，$\varphi_b\approx 12.5°$，且$\Delta\approx 16°$.因为$\Delta$的值是不平凡的，该结果提示，用单光子和共振腔中作为光子间相互作用的非线性光学 Kerr 介质的单个原子，有可能实现具有通用性的双量子比特门(练习 7.23).

解释实验结果时有几个重要的提醒.当入射光子穿过共振腔和原子时，不能忽略被吸收概率，故完成的真正运算是非酉的，这个问题在多重门串联时更严重，在实现受控非门时(要求$\Delta=\pi$)需要门的多重串联.事实上，本实验中共振腔的反射损失将严重影响串联的效果；为弄清如何克服这个问题，必须建立和研究适当的依赖时间的模型.同时，尽管交叉相位调制模型与测量数据一致，所用的光子—原子相互作用模型只是一个拟设，实验并未排除可用的其他模型.事实上，实验中原则上可以采用单光子状态(而不是被衰减的相干态)，在$|\varphi_{out}\rangle$中测量两个模的纠缠可能会是一个好的尝试.在这个实验当初进行的时候，还不知道全面刻画量子运算的一般方法和它对量子逻辑门的适用性.不过，现在已经非常清楚(第 8 章)这样做的一个很好的办法，即过程层析术.并且值得注意的是，这种方法甚至可以充分刻画耗散和其他非酉行为.进行这样的实验，无疑将精确地确定这里描述的实验，在多大程度上真正反映了一个量子计算过程.

尽管有上述不足，这个实验的确说明了量子信息处理需要的基本概念.它证实，像 Kerr 相互作用这样的非线性光学行为，确实发生在单光子水平上，因此验证了 Jaynes-Cummings 模型的本质.并且，这个实验在所谓的共振腔不良范围内进行，其中原子对共振模的相干耦合率g^2/k超过自由空间的非相干发射率γ，但这个耦合弱于输入光子进入和离开共振腔的比k.$g>k>\gamma$的强耦合区，提供了可能得到更大的条件相移Δ的选择.

或许最重要的是，C-QED 打开了对量子信息处理有价值的其他相互作用的大门.我们也已经看到量子信息的观点——注意单光子和单原子——如何让我们能够利用 Jaynes-Cummings Hamilton 量这一基本 C-QED 相互作用，并由它建立电磁波与物质相互作用的某些最根本的物理学理论.我们现在要结束 C-QED 的主题，但当我们接下来研究离子阱和随后研究磁共振时，我们仍会使用光子-原子相互作用，单原子和光子，以及 Jaynes-Cummings Hamilton 量这些概念.

练习 7.23　证明对φ_a，φ_b以及$\Delta=\pi$，当加上任意的单量子比特运算时，式(7.87)的双量子比特门可用于实现受控非门.事实上，对几乎所有Δ值，该门加上单量子比特酉运算都是通用的.

光学共振腔量子电动力学的总结如下：

- 量子比特的表示：两个模$|01\rangle$和$|10\rangle$之间单光子的位置或偏振.
- 酉演化：任意变换用移相器(R_z旋转)，分束器(R_y旋转)和一个 C-QED 系

统来构造. C-QED 系统由一个包含一些和光学场耦合的原子的 Fabry-Perot 共振腔构成.

- 初态的制备：产生单光子态(例如通过衰减激光).
- 输出：探测单光子(例如用光电倍增管).
- 不足：两个光子的耦合由一个原子调制，因此希望增加原子-场耦合. 然而，进入和离开共振腔的光子耦合就变得困难，并限制了串联.

7.6 离子阱(ion trap)

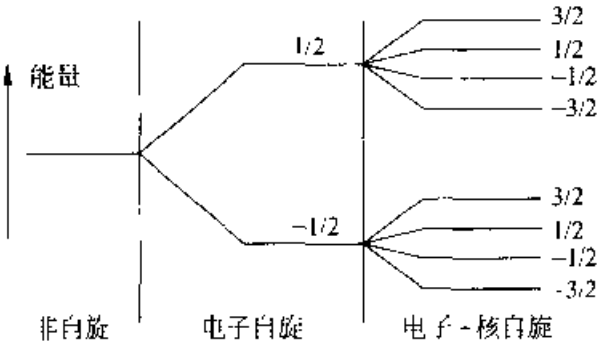
本章到此为止，我们主要集中在用光子表示量子比特的方法，现在转向用原子和核态来表示. 具体地，如 7.1 节所示，电子和核自旋都可能很好地表示量子比特. 自旋是个奇特(但非常真实)的概念(盒子 7.7)，但由于不同自旋状态的能量差与其他能量尺度(例如室温下典型原子的动能)相比通常非常小，原子的自旋状态通常难以观察，而且更难以控制. 不过在精心设计的环境下，精细的控制还是有可能的，在电磁阱中隔离和束缚少量带电原子，并将原于冷却到动能大大低于自旋能的贡献，可制造出这种环境. 进而，可以调节入射的单色光，以选择性地引发改变自旋状态的跃迁，这个改变与其他自旋状态有关. 这正是本节将描述的，被束缚离子如何进行量子计算的实质. 我们从概述实验装置和主要器件开始，然后给出描述系统模型的 Hamilton 量. 我们会描述用 ^9Be 离子实现受控非门的实验，然后以对此方法的潜力和不足的简短评述作结束.

盒子 7.7 自 旋

自旋是一个奇特的概念. 当一个粒子具有自旋时，它有磁矩，就好像它是一个带有沿回路运动的电流的复合粒子. 电子是基本粒子，但组成核子的夸克尚不知道能否由轨道运动产生自旋. 而且，迄今所知的粒子自旋都是整数或半整数.

不过自旋却是非常真实的，并是当今物理学的相当重要的部分. 整数自旋的粒子，称为 Bose 子，包括光子. 光子有些特殊，它没有质量，具有 ± 1 的自旋(没有 0 自旋)分量；这些自旋分量对应熟悉的两个正交偏振态. 便宜的塑料起偏器做成的太阳镜，在开车时可以起作用，是因为阳光从路面等表面反射后，变成了反向的部分偏振光(不管入射角如何，相对于表面具有横向电场的偏振光总发生部分反射，这与当入射光处于 Brewster 角时，横向磁极化不发生反射形成对照). 半整数自旋的粒子称为 Fermi 子，包括电子、质子和中子. 存在自旋 1/2 的粒子，它们的分量要么是 $+1/2$(自旋“上”)要么是 $-1/2$(自旋“下”). 当我们提到自旋时，常指自旋 1/2 粒子.

原子的本征能态与自旋以及多重自旋的组合密切相关. 例如，^{9}Be 的核具有自旋 3/2. 自旋就像磁矩那样和磁场相互作用：在磁场 $\boldsymbol{B}$ 中，具有自旋 $\boldsymbol{S}$ 的电子具有能量 $g_e \boldsymbol{S} \cdot \boldsymbol{B}$，类似地，一个核 $\boldsymbol{I}$ 具有能量 $g_n \boldsymbol{I} \cdot \boldsymbol{B}$. 作为例子，自旋对原子能级的贡献可用图像表示为：



其中我们假设有一个自旋 1/2 电子和一个自旋 3/2 核子. 通过调整入射激光到合适的频率，只要满足守恒定律(7.5.1 节)，这些跃迁都可以被选中. 特别地，角动量守恒意味着当一个光子被原子吸收，在初态和末态之间必然有一个单位的角动量或自旋的改变. 于是这些状态必然有确定的角动量值，这一点需要引起重视.

不像位置或动量这样的连续变量和其他无穷维 Hilbert 空间系统(为表示量子比特需要作人为的截断)，自旋状态为量子信息提供了很好的表示，因为它们本质上属于有限的状态空间.

练习 7.24　磁场中核自旋的能量近似为 $\mu_N B$，其中 $\mu_N = eh/4\pi m_p \approx 5 \times 10^{-27}$ J/T，是核 Bohr 磁子. 计算一个在 $B = 10$T 场中的核自旋的能量，并与 $T = 300$K 时的热能 $k_B T$ 比较.

7.6.1　物理装置

离子阱量子计算机的主要元件是电磁阱、激光器、光探测器和离子.

1. 阱的几何结构与激光器

我们的主要实验装置是，如图 7.7 所示的四柱电极构成的电磁阱. 电极的末段施加与中部不同的偏置电压 U_0，使得离子在轴向被沿 $\hat{z}$ 轴的静电位势 $\Phi_{dc} = kU_0[z^2 - (x^2 + y^2)/2]$ 所约束(k 是几何参数). 不过，由于 Earnshaw 定理断言，静电势能不能在三个维数上同时约束电荷. 故为实现对离子的约束，四个电极中的两个要接地，而另外两个电极则由，产生射频(RF)位势 $\Phi_{rf} = (V_0 \cos\Omega_T t + U_r)(1 + (x^2 - y^2)/R^2)/2$的高频振荡电压驱动，这里 R 是几何参数. 电极各段之间的耦合是电容性的，所以 RF 位势在各段上保持相同. Φ_{dc} 和 Φ_{rf}，经过平均(在 Ω_T)之

后，产生 x,y,z 方向的谐振子势能. 加上离子间的 Coulomb 排斥，可得离子阱中决定 N 个离子运动的 Hamilton 量

$$H=\sum_{i=1}^{N}\frac{M}{2}\left(\omega_x^2x_i^2+\omega_y^2y_i^2+\omega_z^2z_i^2+\frac{|\boldsymbol{p}_i|^2}{M^2}\right)+\sum_{i=1}^{N}\sum_{j>i}\frac{e^2}{4\pi\varepsilon_0|\boldsymbol{r}_i-\boldsymbol{r}_j|} \tag{7.92}$$

其中 M 是每个离子的质量. 典型情况下设计使 $\omega_x,\omega_y\gg\omega_z$，以保证离子都沿 z 轴排列. 当离子数量很多时，离子的几何配置可能变得相当复杂，可能排成折线或其他形式，但我们将只关心排成线状的几个被束缚离子的简单情形.

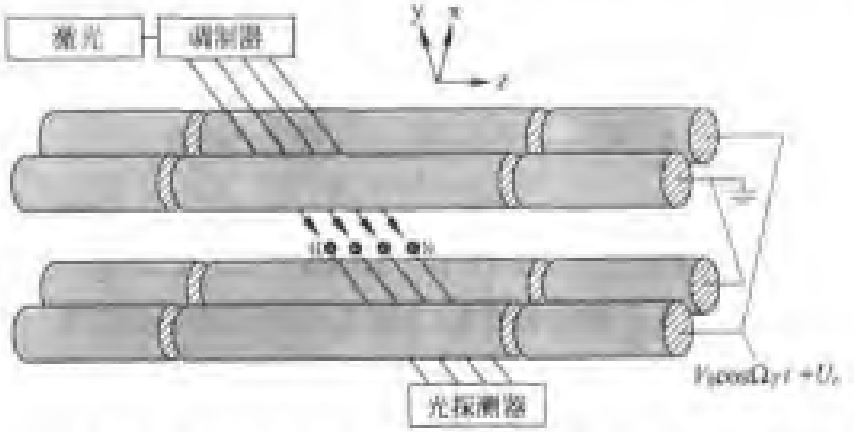


图 7.7 离子阱量子计算机的框图(未按比例)，画出了四个被束缚的离子，处在四根柱形电极产生的势场的中心. 该设备通常置于高度真空中(约为 10^{-8} Pa)，离子是从附近的炉中载入的. 从真空室的窗口入射的调制后的激光，在原子状态上完成运算并用于读出原子状态.

与外界的耦合足够小时，量子系统的行为正如一根弹簧上的质量. 当隔离得足够好时，电磁约束下的离子运动被量子化. 我们首先要弄清量子化的含义，然后再考虑隔离的条件. 如 7.3 节所述，谐振子的能级是以 $\hbar\omega_z$ 为单位均匀分隔的，在离子阱我们关心的区域中，这些本征能态代表着具有质量 NM 的整个离子链作整体运动的不同振动模，称为质心模. 振动能的每个 $\hbar\omega_z$ 量子称为一个声子(phonon)，并可被看作粒子，正如共振腔中电磁辐射的量子是光子.

上述声子描述成立的前提是必须满足一些准则. 首先，与外界环境的耦合必须充分小，使得系统的状态不被热能化过程随机化(从而使其按经典方式演化). 物理上，离子附近的振荡电场和磁场推动离子，引起它们的运动状态在本征能态间随机跃迁. 从技术角度，这样的噪声源几乎是不可避免的，因为，比如说我们没有完美的电压源来驱动约束电极，电源总有一个有限的电阻，而这个电阻要产生 Johnson 噪声，在离子敏感的时间尺度上带来起伏. 电极上的局部电场也有起伏，引起离子的随机运动. 当随机性增强时，离子态的量子性质就消失了，其行为变得用经典的统

计平均可以很好地描述.例如，它们的位置和动量都能被很好地定义，但这在量子系统中却不能同时为真.不过，实践中，大多数技术噪声的确可以被很好地控制到，在大多数实验的时间尺度上，它们不会把被束缚离子加热或退相(dephase)太多的程度.部分重要原因是，只要谐振子近似是成立的，被束缚离子敏感噪声的频率是非常有选择性的，正如能级之间的跃迁只有通过辐射调到正确的频率来选择，只有功率谱密度在 ω_z 附近高的起伏才会影响离子.

为使一维谐振子近似有效，离子被充分冷却也相当重要.对任何方向上相对阱中心的大偏离，真实势能都不是二次的.离子彼此相向运动(而不是一起运动)的高阶振动模必然具有远离于质心模的能量.当这一点成立，并且离子冷却到它们的运动基态时，它们向邻近的高能级状态的跃迁要通过吸收质心声子，这个过程与Mossbaüer效应有关.该效应中因为整个晶体连在一起，晶体中的光子被原子吸收并不产生局部声子.

离子怎样冷却到运动的基态？目标是满足 $k_B T \ll \hbar\omega_z$，其中 T 是反映离子动能的温度.实质上可以利用光子不仅携带能量，而且携带动量 $p=h/\lambda$ 的事实来做到这一点，其中 λ 是光的波长.正如呼啸而来的火车的声调比离去的火车的声调高，向着激光运动的原子的跃迁频率在能量上比离开的原子稍高.如果调节激光，使得它只被迎面而来的原子吸收，那么原子就因光子的反向冲击而变慢，这种方法称为 Doppler 冷却.用适当调整的激光照射被束缚的原子，可以把原子冷却到极限 $k_B T \approx \hbar\Gamma/2$，其中 Γ 是用于冷却的跃迁的辐射宽度.要超越这个极限进一步冷却，常用另一种称为边带冷却(sideband cooling)的方法，如图 7.8 所示，让我们能达到 $k_B T \ll \hbar\omega_z$ 的极限.

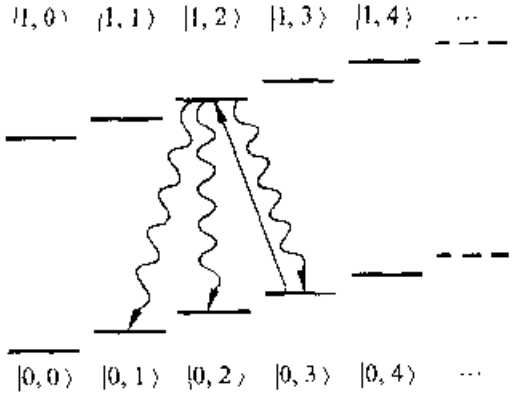


图 7.8 边带冷却法.显示的是 $|0,n\rangle$ 和 $|1,m\rangle$ 之间的跃迁，其中 0 和 1 是两个电子能级，而 n 和 m 是表示离子运动状态的声子能级.激光被调整到具有比电子跃迁少一个声子的能量，比如，$|0,3\rangle$ 状态跃迁到 $|1,2\rangle$ 状态.然后原子自发地衰变为较低能量的 0 状态(波浪线)，随机地(以基本相同的概率)进入 $|0,1\rangle$，$|0,2\rangle$ 或 $|0,3\rangle$ 状态.注意激光实际上引起所有 $|0,n\rangle$ 到 $|1,n-1\rangle$ 的跃迁，因为这些跃迁的能量相同.然而，这个过程不影响 $|0,0\rangle$ 态，并且最终原子会停留在这个状态.

另一必须被满足的准则是，在阱位势中，离子振荡的宽度与入射光的波长相比应该是小的. 这个 Lamb-Dicke 准则习惯上表述为，Lamb-Dicke 参数 $\eta \equiv 2\pi z_0/\lambda$ 的形式，其中 λ 是波长，$z_0 = \sqrt{\hbar/2NM\omega}$ 是阱中离子间空间距离的特征尺寸. Lamb-Dicke 准则要求 $\eta \ll 1$；在量子计算中，这不一定严格满足，但为使单个离子可用不同的激光束分辨出来，而又不使它们的运动状态对完成逻辑运算来说太难以用光学方式激发，我们希望至少有 $\eta \approx 1$.

2. 原子结构

上述阱设备的作用是，让我们能把离子冷却到它们的振动状态，充分接近具有 0 声子（$|0\rangle$），以便作为计算合适的初态. 类似地，离子的内部状态必须被适当地初始化，以便能用来存储量子信息. 让我们考虑这些内部状态，并通过估计它们的相干寿命，了解为什么它们适合表示量子比特.

我们要考虑的，并与被束缚离子有关的原子内部状态是，电子自旋 S 和核自旋 I 的组合 F，这里 $F = S + I$. 描述它的正规理论角动量叠加，不但是理解原子结构需要的重要物理量，而且对量子信息有价值. 如 7.5.1 节所述，一个与原子相互作用的单光子提供或携带一个单位的角动量. 但原子中的角动量有很多来源：轨道、电子自旋和核自旋. 光子能量选择的能级可部分地决定其来源，但光子不能区分不同的来源. 为描述所出现的现象，我们必须选择一个基，使得在其中总角动量是一项惟一确定的状态属性.

例如，考虑两个 1/2 自旋，这两个量子比特空间的计算基是 $|00\rangle$，$|01\rangle$，$|10\rangle$，$|11\rangle$，但为张成状态空间，我们还可以选择基

$$|0,0\rangle_j = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{7.93}$$

$$|1,-1\rangle_j = |00\rangle \tag{7.94}$$

$$|1,0\rangle_j = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{7.95}$$

$$|1,1\rangle_j = |11\rangle \tag{7.96}$$

这些基态是特殊的，因为它们是由 $j_x = (X_1 + X_2)/2$，$j_y = (Y_1 + Y_2)/2$，$j_z = (Z_1 + Z_2)/2$ 以及

$$J^2 = j_x^2 + j_y^2 + j_z^2 \tag{7.97}$$

定义的总角动量算子的本征态. 状态 $|j,m_j\rangle_j$ 是特征值为 $j(j+1)$ 的 J^2 的本征态，并且同时是特征值为 m_j 的 j_z 的本征态. 许多物理上的相互作用会自然地选取这些状态，例如，$\hat{z}$ 方向的磁场中，Hamilton 量 μB_z 中的磁矩 μ 与总角动量，在 $\hat{z}$ 方向的分量 m_j 成比例.

角动量叠加的理论非常复杂也很完善，我们只涉及其皮毛（有兴趣的读者，下

面提供了一些相关的练习，本章末“历史和进一步阅读的材料”中给出了文献的索引）. 不过，从上面的例子中，就已经可以得出一些与量子信息有关的有意义的结论. 我们通常认为，Bell 态那样的纠缠态是物质的非自然状态，因为它们具有奇异和非定域的性质. 然而，状态 $|0,0\rangle_j$ 是一个 Bell 态. 为什么这里大自然偏好这个状态？原因是一种对称性，即涉及磁矩的相互作用在两个自旋交换时，是不变的. 这种对称性实际上在自然界广泛存在，对进行纠缠的测量和运算具有潜在的应用价值.

练习 7.25　证明总角动量算子对 SU(2)服从对易关系 $[j_i,j_k]=i\varepsilon_{ikl}j_l$.

练习 7.26　通过具体写出 J^2 和 j_z 在 $|j,m_j\rangle_j$ 定义的基下的 4×4 矩阵，验证 $|j,m_j\rangle_j$ 性质.

练习 7.27（三自旋角动量状态）　三个 1/2 自旋一起，可以给出具有 $j=1/2$ 和 $j=3/2$ 的全角动量. 证明状态

$$|3/2,3/2\rangle = |111\rangle \tag{7.98}$$

$$|3/2,1/2\rangle = \frac{1}{\sqrt{3}}[|011\rangle+|101\rangle+|110\rangle] \tag{7.99}$$

$$|3/2,-1/2\rangle = \frac{1}{\sqrt{3}}[|100\rangle+|010\rangle+|001\rangle] \tag{7.100}$$

$$|3/2,-3/2\rangle = |000\rangle \tag{7.101}$$

$$|1/2,1/2\rangle_1 = \frac{1}{\sqrt{2}}[-|001\rangle+|100\rangle] \tag{7.102}$$

$$|1/2,-1/2\rangle_1 = \frac{1}{\sqrt{2}}[|110\rangle-|011\rangle] \tag{7.103}$$

$$|1/2,1/2\rangle_2 = \frac{1}{\sqrt{6}}[|001\rangle-2|010\rangle+|100\rangle] \tag{7.104}$$

$$|1/2,-1/2\rangle_2 = \frac{1}{\sqrt{6}}[-|110\rangle+2|101\rangle-|011\rangle] \tag{7.105}$$

构成空间的一个基. 对 $j_z=(Z_1+Z_2+Z_3)/2$（类似地对 j_x,j_y）和 $J^2=j_x^2+j_y^2+j_z^2$，满足 $J^2|j,m_j\rangle=j(j+1)|j,m_j\rangle$ 和 $j_z|j,m_j\rangle=m_j|j,m_j\rangle$. 有得到这些状态的复杂途径，但不动脑筋的直接方法就是把 J^2 和 j_z 的 8×8 矩阵同时对角化.

练习 7.28（超精细状态）　我们将在 7.6.4 节考察铯——那里相关的总角动量涉及一个与电子自旋 $S=1/2$ 结合的核自旋 $I=3/2$，给出 $F=2$ 或 $F=1$. 对于一个自旋 3/2 粒子，角动量算子为

$$j_z=\frac{1}{2}\begin{bmatrix}3&0&0&0\\0&1&0&0\\0&0&-1&0\\0&0&0&-3\end{bmatrix} \tag{7.106}$$

$$i_y=\frac{1}{2}\begin{bmatrix}0 & i\sqrt{3} & 0 & 0\\ -i\sqrt{3} & 0 & 2i & 0\\ 0 & -2i & 0 & i\sqrt{3}\\ 0 & 0 & -i\sqrt{3} & 0\end{bmatrix} \tag{7.107}$$

$$i_z=\frac{1}{2}\begin{bmatrix}-3 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 3\end{bmatrix} \tag{7.108}$$

(1) 证明 i_x,i_y 和 i_z 满足 $SU(2)$对易规则.

(2) 给出 $f_z=i_z\otimes I+I\otimes Z/2$(其中 I 代表相应子空间上的恒等算子),类似地,f_x 和 f_y 以及 $F^2=f_x^2+f_y^2+f_z^2$ 的 8×8 矩阵表示.把 f_z 和 F^2 同时对角化,以得到基态 $|F,m_F\rangle$ 使得 $F^2|F,m_F\rangle=F(F+1)|F,m_F\rangle$ 且 $f_z|F,m_F\rangle=m_F|F,m_F\rangle$.

不同自旋状态的叠加可以存在多久?极限过程称为自发射,它发生在原子从激发态向基态跃迁发出一个光子的时候.发生的时刻是随机的,其速率是我们要估计的.如果把原子放到自由空间中没有任何干扰,原子自发发出光子看上去是一件奇怪的事情,但这个过程是原子和电磁场耦合的一个非常自然的结果.该耦合由 Jaynes-Cummings 相互作用

$$H_I=g(a^\dagger\sigma_-+a\sigma_+) \tag{7.109}$$

描述,如 7.5.2 节所讨论的.前面我们用此模型描述激光如何与原子相互作用,但该模型也描述了甚至没有光学场时原子的情形,考虑与一个不包含光子的单模场耦合的处于激发态的原子,状态为 $|01\rangle$(使用|场,原子〉记号).它不是 H_I 的本征态,因而不能随时间保持定常.酉算子式(7.77)描述了变化的过程,其中我们知道原子以 $p_{\text{decay}}=|\langle 10|U|01\rangle|^2$ 概率衰变为基态,并释放一个光子,其中到原子-场耦合 g 的最低阶,p_{decay} 为

$$p_{\text{decay}}=g^2\frac{4\sin\frac{1}{2}(\omega-\omega_0)^2t}{(\omega-\omega_0)^2} \tag{7.110}$$

ω 是光子的频率,$\hbar\omega_0$ 是原子两个能级的能量差.自由空间的原子与许多不同的光学模相互作用,插入耦合

$$g^2=\frac{\omega_0^2}{2\hbar\omega\epsilon_0c^2}|\langle 0|\mu|1\rangle|^2 \tag{7.111}$$

其中 μ 是原子偶极算子,在全部光学模上积分,并取时间的导数,可得出每秒钟的衰变概率

$$\gamma_{\text{rad}}=\frac{\omega_0^3|\langle 0|\mu|1\rangle|^2}{3\pi\hbar\epsilon_0c^5} \tag{7.112}$$

如果我们取近似 $|\langle 0|\boldsymbol{\mu}|1\rangle| \approx \mu_B \approx 9\times 10^{-24}\,\mathrm{J/T}$，即 Bohr 磁子，并假定 $\omega_0/2\pi \approx 10\mathrm{GHz}$，则 $\gamma_{\mathrm{rad}} \approx 10^{-15}\,\mathrm{sec}^{-1}$，这是一个低于每 3000000 年衰变一个的自发射速率. 这个计算对估计原子状态的寿命有代表性，如读者看到的，理论上超精细状态可以有相当长的相干时间，这与实验普遍一致. 实验中已经观察到几十秒到几十小时的寿命时间.

练习 7.29（自发射）　自发射率式(7.112)可以从式(7.110)和式(7.111)按下列步骤推导.

(1) 求积分

$$\frac{1}{(2\pi c)^3}\frac{8\pi}{3}\int_0^{\infty}\omega^2 p_{\mathrm{decay}}\,\mathrm{d}\omega \tag{7.113}$$

其中 $8\pi/3$ 来源于对极化求和并对立体角 $\mathrm{d}\Omega$ 积分，且 $\omega^2/(2\pi c)^3$ 来源于三维空间中的模密度(提示：可以考虑把积分的下极限扩展到 $-\infty$)；

(2) 结果对 t 求导数，以得到 γ_{rad}.

g^2 的形式来自量子电动力学，有了这个结果，这里的其他结果确实就可由 Jaynes-Cummings 相互作用导出了. 我们再次看到考虑单原子，单光子方法中的性质是如何给出原子的基本性质的，而不需要求助于摄动理论.

练习 7.30（电子状态寿命）　类似对 γ_{rad} 的计算，可以用于估计电子跃迁的期望寿命，即那些涉及能级变化 $\Delta n \neq 0$ 的跃迁. 对这类跃迁，相关的相互作用把原子的电偶极矩和电磁场耦合起来，给出

$$g_{\mathrm{ed}}^2 = \frac{\omega_0^2}{2\hbar\omega\,\varepsilon_0}\,|\langle 0|\boldsymbol{\mu}_{\mathrm{ed}}|1\rangle|^2 \tag{7.114}$$

这给出一个自发射率

$$\gamma_{\mathrm{red}}^{\mathrm{ed}} = \frac{\omega_0^3\,|\langle 0|\boldsymbol{\mu}_{\mathrm{ed}}|1\rangle|^2}{3\pi\hbar\omega\varepsilon_0 c^3} \tag{7.115}$$

给定 $\gamma_{\mathrm{red}}^{\mathrm{ed}}$，取 $\langle 0|\boldsymbol{\mu}_{\mathrm{ed}}|1\rangle \approx q\,a_0$，其中 q 是电荷数，而 a_0 是 Bohr 半径，并假定 $\omega_0/2\pi \approx 10^{15}\,\mathrm{Hz}$. 与超精细状态相比，电子态的衰变快多少？

7.6.2　Hamilton 量

上节给出的谐振电磁阱的简化模型和原子的结构结合起来，为我们提供了离子阱量子信息处理器的简化示意模型. 想象一个双能级单自旋与一个电磁场，通过普通的磁偶极子 $H_I = -\boldsymbol{\mu}\cdot\boldsymbol{B}$ 发生相互作用，其中偶极矩 $\boldsymbol{\mu} = \mu_m \boldsymbol{S}$ 与自旋算子 S 成比例；而磁场是 $\boldsymbol{B} = B_1\hat{x}\cos(kz-\omega t+\varphi)$，$B_1$ 是场强，k 是它在 $\hat{z}$ 方向的动量，ω 是频率，而 φ 是相位. 注意在本节中，我们采用 $S_x = X/2$，$S_y - Y/2$，$S_z = Z/2$ 作为自旋算子，它们与 Pauli 算子相差一个因子 2.

除了通常的电磁相互作用，还存在与振动模的相互作用. 自旋在物理上被限制在一个能量尺度为 $\hbar\omega_z$ 的谐振子势能中(图 7.9)，这样它的位置被量子化，并且我

们必须用一个算子 $z=z_0(a^\dagger+a)$ 来描述它，其中 $a^\dagger$，a 是粒子振动模的提升和递降算子表示声子产生和湮没.

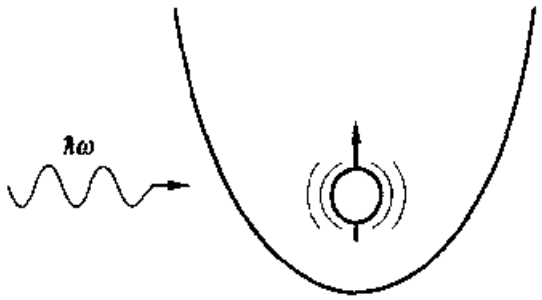


图 7.9 粒子阱的简化示意模型：与电磁辐射相互作用，谐振子势中具有两个内部状态的一个单粒子.

假定粒子被冷却到接近最低振动模，使得它在阱中的振荡宽度小于入射光波长，即 Lamb-Dicke 参数 $\eta=kz_0$ 是小的. 定义自旋的 Rabi 频率为 $\Omega=\mu_m B_1/2\hbar$，并回忆 $S_x=(S_+ +S_-)/2$，我们可导出在小 η 端简化的相互作用 Hamilton 量为

$$H_I=-\boldsymbol{\mu}\cdot\boldsymbol{B} \tag{7.116}$$

$$\approx\left[\frac{\hbar\Omega}{2}(S_+ e^{i(\varphi-\omega t)}+S_- e^{-i(\varphi-\omega t)})\right]$$

$$+\left[i\frac{\eta\hbar\Omega}{2}(S_+ a+S_- a^\dagger+S_+ a^\dagger+S_- a)(e^{i(\varphi-\omega t)}-e^{-i(\varphi-\omega t)})\right] \tag{7.117}$$

括号中第一项来自在 7.5.2 节中看到的，通常的 Jaynes-Cummings Hamilton 量，它出现在自旋在 z 方向为定常时. 然而，它是简化形式且不含光子算子，因为事实上只要 B_1 是一个强相干状态，我们就可以忽略它的量子性质，而得到只描述原子内部状态的演化的一个 Hamilton 量. 实际上场的相干态在与原子相互作用后，不与它纠缠(到极好的近似程度)是相当惊人的，这是一个深奥的结果. 本章末问题 7.3 中读者可以进一步探索这个结果，我们在 7.7.2 节描述共振时还会涉及到这个事实.

通过离子看到的磁场依赖于其位置的事实，括号的第二项描述了离子的运动状态和它的自旋态之间的耦合. 括号中的四项对应四种跃迁(两上两下)，如图 7.10 所示称为红和蓝运动边带.

通过包含自由粒子的 Hamilton 量

$$H_0=\hbar\omega_0 S_z+\hbar\omega_x a^\dagger a \tag{7.118}$$

容易看到这些边带跃迁具有频率 $\omega_0\pm\omega_x$ 的原因. 这个 Hamilton 量引起自旋和声子按照

$$S_+(t)=S_+ e^{i\omega_0 t},\ S_-(t)=S_- e^{-i\omega_0 t} \tag{7.119}$$

$$a^\dagger(t)=a^\dagger e^{i\omega_x t},\ a(t)=ae^{-i\omega_x t} \tag{7.120}$$

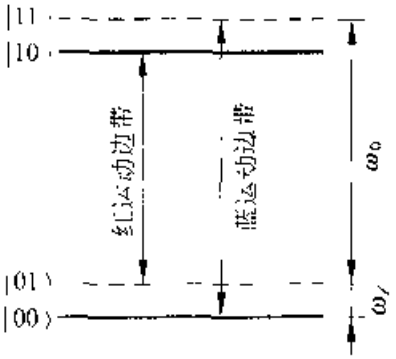


图 7.10　示意性模型的被束缚离子的能级，显示了对应单个声子的产生和湮没的红和蓝运动边带跃迁，存在其他更多运动状态的无穷阶梯，但常常不会涉及，状态的标记为 $|n,m\rangle$，其中 n 表示自旋状态，而 m 表示声子数目。

演化。于是，以 H_0 为参照的框架中，可导出主导项 $H_I'=\mathrm{e}^{\mathrm{i}H_0 t/\hbar}H_I\mathrm{e}^{-\mathrm{i}H_0 t/\hbar}$ 为

$$H_I'=\begin{cases}\mathrm{i}\dfrac{\eta\hbar\Omega}{2}(S_+ a^\dagger \mathrm{e}^{\mathrm{i}\varphi}-S_- a\mathrm{e}^{-\mathrm{i}\varphi}), & \omega=\omega_0+\omega_z\\ \mathrm{i}\dfrac{\eta\hbar\Omega}{2}(S_+ a\mathrm{e}^{\mathrm{i}\varphi}-S_- a^\dagger \mathrm{e}^{-\mathrm{i}\varphi}), & \omega=\omega_0-\omega_z\end{cases}\tag{7.121}$$

其中电磁场的频率 ω 列在右边。

如果我们假定，它们具有共同的，比系统其他振动模能量低得多的，单个质心振动模，那么就很容易把上述模型从一个自旋推广到限制在同样谐振子势中的 N 自旋。该理论的一个直接推广表明，惟一需要修改的是用 $\Omega/\sqrt{N}$ 代替 Ω，因为全部 N 个粒子集合起来一起移动。

7.6.3　量子计算

用被束缚量子进行量子计算，需要我们能够在原子的内部状态上，构造任意酉变换。现在就来说明如何分三步，做到这一点。我们要描述：(1)在原子内部(自旋)状态上如何进行任意的单量子比特运算；(2)在自旋和声子状态间，进行受控双量子比特门运算的一种方法；(3)在自旋和声子间交换量子信息的一条途径。给定这些建造模块，我们接着描述已完成的受控非门实验，并补充状态制备和读出的过程。

1. 单量子比特运算

应用频率为 ω_0 的电磁场来启动内部 Hamilton 项

$$H_I^{\text{interna}}=\frac{\hbar\Omega}{2}(S_+\mathrm{e}^{\mathrm{i}\varphi}+S_-\mathrm{e}^{-\mathrm{i}\varphi})\tag{7.122}$$

通过适当选择 φ 和相互作用时间区间，我们可以进行旋转运算 $R_x(\theta)=\exp(-i\theta S_x)$ 和 $R_y(\theta)=\exp(-i\theta S_y)$. 于是根据定理 4.1，我们可以完成自旋状态上的任意单量子比特运算. 我们在第 j 个粒子上的旋转符号上加一个下标，例如 $R_{xj}(\theta)$.

练习 7.31 从 R_y 和 R_x 构造一个 Hadamard 门.

2. 受控相位翻转门

假设一个量子比特存储在原于内部自旋状态中，并且另一量子比特用 $|0\rangle$ 和 $|1\rangle$ 声子状态存储. 如果是这样，我们能够用酉变换

$$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix} \tag{7.123}$$

执行受控相位翻转门运算. 用如图 7.11 的一个具有三个能级的原子，最容易解释这现象(多出来的能级实质上是不必要的，见问题 7.4). 一束频率为 $\omega_{aux}+\omega_z$ 激光，引起 $|20\rangle$ 和 $|11\rangle$ 状态之间的跃迁，这启动了形如

$$H_{aux}=i\frac{\eta\hbar\Omega'}{2}(S'_+e^{i\varphi}+S'_-e^{-i\varphi}) \tag{7.124}$$

的 Hamilton 量，其中 S'_+ 和 S'_- 表示 $|20\rangle$ 和 $|11\rangle$ 之间的跃迁，并且假定高阶运动状态未被占据. 注意因为这个频率的惟一性，其他跃迁不会被激发. 我们调整激光的相位和持续时间，以获得一个 2π 的脉冲，即在 $|11\rangle$ 和 $|20\rangle$ 张成的空间上的旋转 $R_x(2\pi)$，它恰好是酉变换 $|11\rangle\to-|11\rangle$. 假定不期望的状态如 $|1,2\rangle$ 的概率幅是 0，所有其他状态都不变，这就实现了式(7.123)期望的变换. 我们把此门记作 $C_j(Z)$(表示一个受控 Z 运算)，其中 j 表示门作用的离子. 注意所有离子共享同一声子，就是质心声子，由此，在工程术语中这个量子比特称为声子“总线”量子比特.

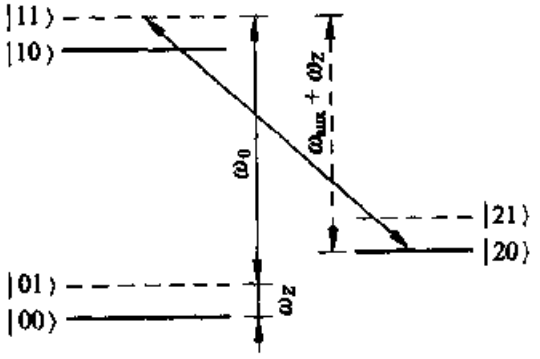


图 7.11 离子阱中三能级原子的能级，每个能级具有两个声子状态. 标号 $|n,m\rangle$ 表示原子状态 n 和声子状态 m. 跃迁 $|20\rangle\leftrightarrow|11\rangle$ 完成受控相位翻转门.

3. 交换门

最后，我们需要某种在原子的内部自旋状态和声子状态之间交换量子比特的方法。这可以通过把激光调到频率 $\omega_0-\omega_z$，并且让相位在$|01\rangle$和$|10\rangle$张成子空间上旋转 $R_y(\pi)$来做到. 该旋转恰好是$|00\rangle$，$|01\rangle$，$|10\rangle$，$|11\rangle$空间上的酉变换

$$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix} \tag{7.125}$$

如果初态是 $a|00\rangle+b|10\rangle$(即声子初始为$|0\rangle$)，则交换后的状态是 $a|00\rangle+b.01\rangle$，于是这就完成了期望的交换运算. 我们把作用在第 j 个离子上的交换门记作 $\overline{\mathrm{SWAP}_j}$，逆运算对应 $R_y(-\pi)$. 从技术上说，由于 $R_y(\pi)$ 的$|10\rangle\langle 01|$项的负号，这不是一个完全的交换运算，但除了相对相位，它等价于一个交换运算(见练习 4.26). 因此，有时称其为映射运算而不说是交换.

4. 受控非门

将这些门组合在一起，使我们可以利用一系列运算

$$\mathrm{CNOT}_{jk}=H_k\,\overline{\mathrm{SWAP}_k}C_j(Z)\mathrm{SWAP}_kH_k \tag{7.126}$$

构造出作用在离子 j(控制) 和 k(目标)上的 CNOT 门(时间从右到左，如通常对矩阵的顺序)，其中 H_k 是 Hadamard 门(由离子 k 上的旋转 R_y 和 R_x 构造). 这非常类似于如式(7.46)中，由分束器和光学 Kerr 介质构造受控非门的方式.

7.6.4　实验

一个被束缚离子的受控非门已被实现(参见“历史和进一步阅读的材料”)，这个实验的具体方法很有启发性. 在实验中，一个$^9Be^+$离子被同轴共振器 RF 离子阱束缚，这与图 7.7 中的线性离子在几何形状上不同，但功能上等价，并与图 7.12 所示的实际离子阱的照片类似. 选择铍，是因为它的超精细和电子能级结构，如图 7.13 所示. $^2S_{1/2}(2,2)$能级(练习 7.28)用作原子的内部量子比特状态，而$|0\rangle$和$|1\rangle$声子状态用作另一个量子比特(图中标记为 $n=0$ 和 $n=1$). 能级$^2S_{1/2}(1,1)$和$^2S_{1/2}(2,2)$之间约为 313 nm 跃迁，不是通过调整单束激光到这个跃迁频率，而是利用两束频率差，来获得跃迁频率的激光. 这个 Raman 跃迁方法降低了对激光相位稳定性的要求. $^2S_{1/2}(2,0)$被用作辅助能级，$^2S_{1/2}$状态具有不同能量，这靠一个加在系统上的 0.18mT 磁场来获得. 被束缚离子在阱中的振动频率为$(\omega_x,\omega_y,\omega_z)/2\pi=(11.2,18.2,29.8)$MHz，基态 $n_z=0$ 波函数的展宽为 7nm，其 Lamb-Dicke 参数大约是 $\eta_z=0.2$. 共振跃迁的 Rabi 频率是 $\Omega/2\pi=140$kHz，两个运动边带的频率是 $\eta_z\Omega/2\pi=30$kHz，辅助跃迁的频率是 $\eta_z\Omega'/2\pi=12$kHz.



图 7.12 显微制造的椭圆形电极离子阱的照片，其中离子已被约束。这个阱中的离子是钡，而不是铍，但基本原理和文中描述的相同（复制得到 IBM Almaden 研究中心的 R. Devoe 和 C. Kurtsiefer 的允许）。

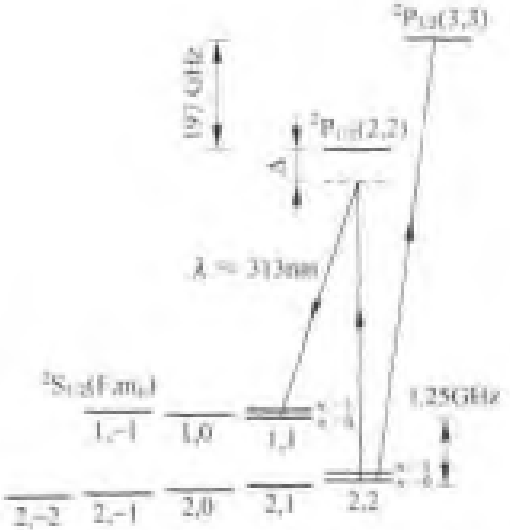


图 7.13 用于离子阱实验的 $^9Be^+$ 能级（复制得到 NIST 的 C. Monroe 的允许）。

离子的状态用 Doppler 和边带冷却来获得，以 95% 概率获得状态 $|00\rangle = |^2S_{1/2}(2,2)\rangle|n_z=0\rangle$，然后用单量子比特运算，把离子的内部与运动状态制备成四个基态 $|00\rangle$，$|01\rangle$，$|10\rangle$，$|11\rangle$ 之一。受控非门由三个脉冲实现。首先是内部状态量子比特上的一个 $R_x(\pi/2)$ 旋转，然后是两个量子比特间的一个受控 Z 运算，最后是

内部状态量子比特上的一个 $R_x(-\pi/2)$ 旋转. 容易证明(练习 7.32)图 7.14 中的这个线路实现了一个受控非门.

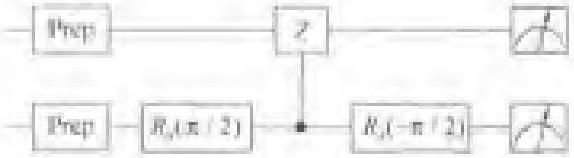


图 7.14　离子阱受控非运算实验的量子线路模型. 顶上的连线表示声子状态,底下的表示量子的内部超精密状态.

计算输出的读取用两个测量实现. 第一个是使用调整到$^2S_{1/2}(2,2)$和$^2P_{3/2}(3,3)$之间循环进行的跃迁圆偏振光时,从离子收集荧光. 这种光与$^2S_{1/2}(1,1)$状态没有明显的耦合,因此观察到的荧光与处于$|0\rangle$状态的内部状态量子比特的概率成比例. 这是一个投影测量. 该测量技术功能强大,因为跃迁循环多次　　离子吸收一个光子,跳到$^2P_{3/2}(3,3)$状态,然后释放一个光子,衰变到它出发的$^2S_{1/2}(2,2)$状态. 这种循环可进行数千次甚至更多,可以得到好的统计值. 第二个测量与第一个类似,但先用一个交换脉冲,来交换运动与内部状态量子比特,这以投影方式测量运动状态量子比特.

这项实验验证了受控非运算的经典真值表,而且原则上,通过制备输入叠加态和测量输出密度矩阵,借助过程层析术可以完全刻画该酉变换(第 8 章). 受控非门在实验用的光强下约要求 50ms. 另一方面,相干时间的测量结果是几百到几千毫秒. 主要的退相干机制包括激光束功率,RF 离子阱驱动频率和电压幅值的不稳定性和外磁场的起伏. 而且,实验仅包含一个单离子和两个量子比特,因此对计算没有用处,为了真正有用,在不同的离子之间一般都要使用受控非门,而不是仅用在单离子和运动态上.

不过,技术上的限制也许能被克服,通过仅间歇地使用短寿命的运动状态,而尽可能利用相干时间长得多的内部原子状态,也可能会延长寿命时间. 把离子数目增加到很大的数目在概念上是可行的. 图 7.15 是 40 个被束缚水银离子的串. 为使

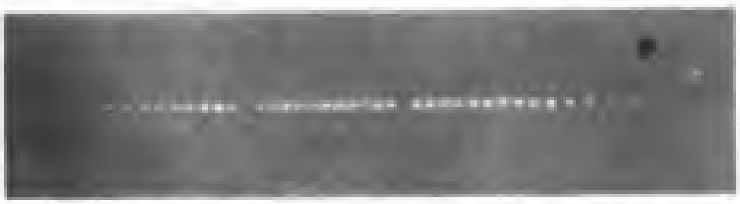


图 7.15　约 40 个被束缚水银离子($^{199}Hg^+$)的荧光图像. 离子约间隔 15μm. 而两个明显的间隙是水银的不响应探测激光的不同的同位素. 复制得到 NIST 的 D. Wineland 的允许.

这样的系统对量子信息处理机器有用.要克服许多困难,但技术上的惊人之举是永不完结的,也许有一天,这类被束缚的离子可能成为量子计算机中的量子比特寄存器.

练习 7.32 证明图 7.14 的线路等价于一个声子作控制量子比特的受控非门(除去一个相对相位).

离子阱量子计算机的总结如下:

- 量子比特表示:原子的超精细(核自旋)状态和被束缚原子的最低能级振动模(声子).
- 酉演化:通过 Jaynes-Cummings 相互作用,可以从自外部操作原子状态的激光脉冲的应用构造任意变换.量子比特通过一个共享的声子状态相互作用.
- 初态制备:把原子冷却(通过束缚和使用光学抽运)到它们的运动基态和超精细基态.
- 输出:测量超精细状态的分布.
- 不足:声子的寿命短,并且离子难以制备为运动基态.

7.7 核磁共振

只要自旋-自旋耦合很强而且能被控制,核自旋系统对量子计算就近乎理想的选择,这是我们上节离子阱的研究得到的一个重要认识.离子阱量子计算机的主要不足是,基于声子调制的自旋-自旋耦合技术缺陷和退相干的问题,克服这一局限性的一个办法是束缚分子而不是单个原子——基于磁偶极子和电子调制的邻近核子间的 Fermi 接触相互作用可以提供自然的强耦合.不过,由于具有很多振动模,单个分子很难被束缚和冷却,因此除特殊情形外,用光来控制和探测被束缚分子的核自旋目前尚不可行.

另一方面,用射频电磁波直接操作和探测核自旋状态是一个成熟的领域,称为核磁共振(NMR).该类技术广泛应用于化学中,例如测量液体、固体和气体的性质,确定分子结构和绘出材料甚至是生物学系统的图像.这许多应用使 NMR 技术相当成熟,可以在实验中对大量的核子进行控制和测量.

然而,NMR 用于量子计算有两个问题.首先,因为核磁矩的微弱性,为产生测量感应信号,需要使用大量分子(超过 10^5).从概念上讲,单个分子可能做成一台好的量子计算机,但对分子的系综如何做到呢?特别地,NMR 测量的输出是所有分子信号的平均,量子计算机系综的平均输出有意义吗?其次 NMR 通常用在室温下的热平衡态物理系统,而这种情况下自旋能量 $\hbar\omega$ 比 k_BT 小得多.这意味着自旋的初态近乎完全随机,如何用一个具有高度熵的混合态的系统进行量子计算?

这两个问题的解决,使 NMR 成为非常有吸引力和启发性的量子计算实现方法,尽管典型系统中热性质带来严重的局限性,但可以从 NMR 学到很多经验.例

如，控制现实的 Hamilton 量，来进行任意酉变换的技术，刻画和克服退相干的方法，和在一个整体系统中实现完整量子算法过程中，对元件组装的考虑等。我们从描述物理设备和涉及的主导 Hamilton 量开始，然后讨论尽管存在热输入状态和系综问题，NMR 用于量子信息处理为什么仍是可能的。最后以量子算法的已经演示的某些实验作结束，并指出这一方法的不足。

7.7.1 物理装置

让我们从对装置的一般描述开始，后面再给出其运行的详细数学模型。这里要讨论的是针对液体样品的脉冲 NMR 系统的两个主要部分，样品和 NMR 谱仪。所用的典型分子包含 n 个自旋 1/2(其他可能的核子有^{13}C、^{19}F、^{15}N、^{31}P)的质子。在当置于 11.7T 磁场时产生约 500MHz 的信号。因为由于化学环境屏蔽效应，分子中了局部磁场的不同分子中不同的核子的频率差可达几千赫兹到几百千赫兹。将分子溶解到溶液中，降低浓度到分子间相互作用可以忽略的程度，得到一个可以很好地描述为 n 量子比特量子计算机系综的系统。

谱仪本身由射频电子系统和一个大的超导磁体构成，在玻璃试管中盛着样品，如图 7.16 所示。沿 $\vec{z}$ 轴方向的磁场 B_z 在约 $1cm^3$ 的范围内仔细调整均匀到 $1/10^6$，正交鞍形或 Helmholtz 线圈放置在横向平面中，使得沿 $\vec{x}$ 和 $\vec{y}$ 方向可以有小的振荡磁场。这些场可以快速进行脉冲开关，以操作核自旋状态。同样的线圈还是调谐电路的一部分，用来拾取由旋进的核子产生的 RF 信号(很像旋转磁体在附近线圈中感应产生交变电流)。

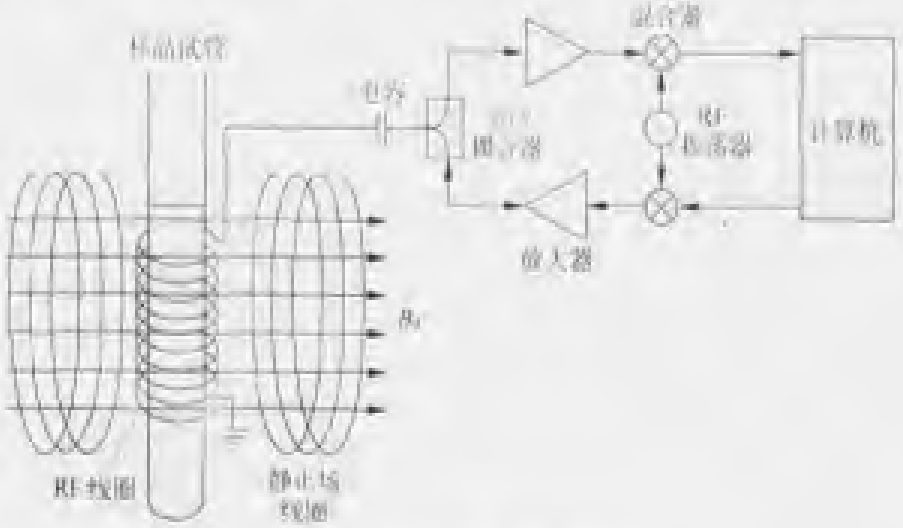


图 7.16 核磁共振设备框图

典型的实验开始要等待很长时间，以使核子达到热平衡，这个过程中为制备好液体样本需要花几分钟。接着在(经典)计算机的控制下，应用 RF 脉冲以进行核子

状态上的期望变换. 大功率脉冲放大器快速开关，及一个灵敏的前置放大器启动，以测量自旋的最终状态. 这个输出，称为自由感应衰减(free induction decay)，对其作 Fourier 变换处理，以得到峰值区域是自旋态函数的频谱(图 7.17).

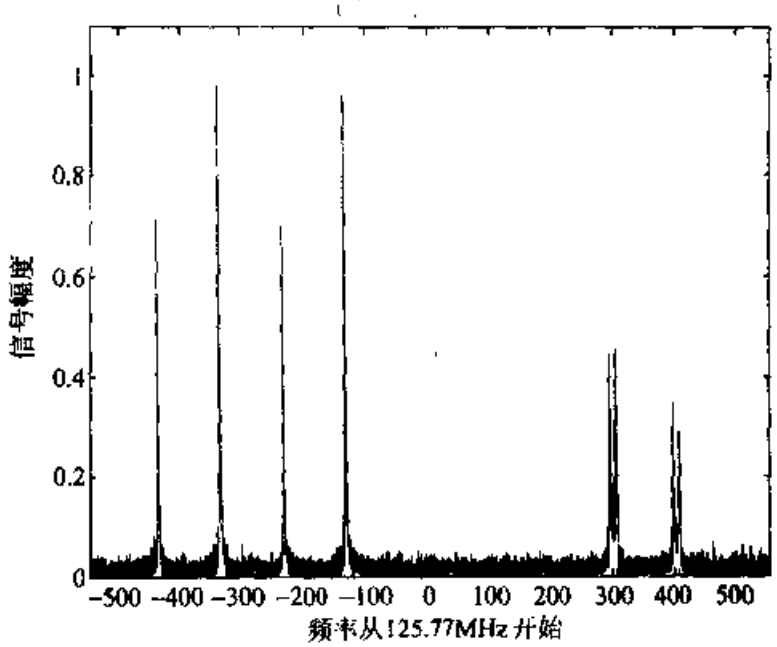


图 7.17 三氯乙烯标记的^{13}C的谱. 左边四条谱线对应与质子相键合的碳核；四条线的出现是因为与质子和第二个碳核的耦合，而第二个碳核自身导致右边的四条排列较紧密的谱线. 第二个碳核离质子较远，因此与之耦合弱得多.

有许多重要的实际问题会导致观测不完美. 例如，静态磁场的空间非均匀性，引起场的不同部分具有不同的频率，这使谱线加粗. 一个甚至更具挑战性的问题是 RF 场的均匀性，该场由必须正交于 B_0 磁体的线圈产生. 这个几何约束和同时保持 B_0 磁体的高度上的均匀性，常常迫使 RF 场是非均匀的和由小线圈产生的，导致对核系统的非完美控制. 而且，脉冲计时和功率，相位和频率的稳定性也是重要的问题，不过，不像离子阱，由于频率更低，更容易控制好这些参数. 在了解了用 NMR 进行量子信息处理的系统和方法的基本数学形式后，我们将在 7.7.4 节讨论这种方法的不完美之处.

7.7.2 Hamilton 量

NMR 的基本理论，可以通过这里叙述的一个或两个自旋的理想模型来了解. 第一步要描述电磁辐射和一个单磁自旋如何相互作用，然后考虑分子中自旋之间耦合的物理性质. 这些工具使我们，可以建立从处于热平衡的初态变换来的磁化输出的模型. 最后，我们描述一个退相干的唯象模型，以及如何用实验确定它的参数 T_1 和 T_2.

1. 单自旋动态

经典电磁场和一个双态自旋的磁相互作用由 Hamilton 量 $H=-\boldsymbol{\mu}\cdot\boldsymbol{B}$ 描述，其中 $\boldsymbol{\mu}$ 是自旋，$B=B_0\hat{z}+B_1(\hat{x}\cos\omega t+\hat{y}\sin\omega t)$ 是典型的实验用磁场，B_0 是静态的而且很大，而 B_1 通常是时变的，而且在强度上比 B_1 小几个数量级，因此传统上用摄动理论来研究这类系统. 不过，这个系统的 Schrödinger 方程可以不用摄动理论而直接解出. 用第 2 章的 Pauli 矩阵技术，可以把 Hamilton 量写作

$$H=\frac{\omega_0}{2}Z+g(X\cos\omega t+Y\sin\omega t) \tag{7.127}$$

其中 g 和 B_1 的场强有关，而 ω_0 与 B_0 有关，X,Y,Z 是普通的 Pauli 矩阵. 定义 $|\varphi(t)\rangle=\mathrm{e}^{\mathrm{i}\omega tZ/2}|\chi(t)\rangle$，使得 Schrödinger 方程

$$\mathrm{i}\partial_t|\chi(t)\rangle=H|\chi(t)\rangle \tag{7.128}$$

可以重新表达为

$$\mathrm{i}\partial_t|\varphi(t)\rangle=\left[\mathrm{e}^{\mathrm{i}\omega tZ/2}H\mathrm{e}^{-\mathrm{i}\omega tZ/2}-\frac{\omega}{2}Z\right]|\varphi(t)\rangle \tag{7.129}$$

由于

$$\mathrm{e}^{\mathrm{i}\omega tZ/2}X\mathrm{e}^{-\mathrm{i}\omega tZ/2}=(X\cos\omega t-Y\sin\omega t) \tag{7.130}$$

可把式(7.129)简化为

$$\mathrm{i}\partial_t|\varphi(t)\rangle=\left[\frac{\omega_0-\omega}{2}Z+gX\right]|\varphi(t)\rangle \tag{7.131}$$

其中右边乘状态的项可以视为有效的旋转框架的 Hamilton 量. 该方程的解是

$$|\varphi(t)\rangle=\mathrm{e}^{-\mathrm{i}\left[\frac{\omega_0-\omega}{2}Z+gX\right]t}|\varphi(0)\rangle \tag{7.132}$$

共振的概念是从这个解的行为中来的，由式(4.8)可将该解看作绕轴为

$$\hat{n}=\frac{\hat{z}+\frac{2g}{\omega_0-\omega}\hat{x}}{\sqrt{1+\left(\frac{2g}{\omega_0-\omega}\right)^2}} \tag{7.133}$$

转角为

$$|\hat{n}|=t\sqrt{\left(\frac{\omega_0-\omega}{2}\right)^2+g^2} \tag{7.134}$$

的一个单量子比特旋转. 当 ω 与 ω_0 相差很大时，自旋受 B_1 场的影响可以忽略，这个旋转的轴接近平行于 $\hat{z}$，而它随时间的演化几乎精确地与自由 Hamilton 量 B_0 的演化相同. 另一方面，当 $\omega_0\approx\omega$ 时，B_0 的贡献可以忽略，并且弱的 B_1 场可以引起相应于绕 $\hat{x}$ 旋转的大的状态变化. 当调到适当频率时，小摄动可以在自旋系统上起的巨大作用是核磁共振中共振的原因. 当然，同样的效应，也是 7.5.1 节中用到过(但未解释)的双能级原子对特别调整的激光场的选择性的核心.

一般地，当 $\omega=\omega_0$ 时，量子比特旋转框架的 Hamilton 量可以写作

$$H = g_1(t)X + g_2(t)Y \tag{7.135}$$

其中 g_1 和 g_2 是所使用的横向 RF 场的函数.

练习 7.33(磁共振) 证明式(7.128)可化简为式(7.129). 什么样的实验框架的 Hamilton 量能引起旋转框架的 Hamilton 量(式(7.135))?

练习 7.34(NMR 频率) 从核 Bohr 磁子出发，计算一个 11.8T 磁场中光子的进动频率. 为在 10ms 内完成 90°旋转，需要 B_1 为多少?

2. 自旋-自旋耦合

我们感兴趣的系统中常有不止一种自旋，^{1}H，^{13}C，^{19}F，^{15}N 都具有核自旋 1/2. 这些自旋通过两个主要机制相互作用：直接偶极耦合和通过键电子调制，间接相互作用. 通过空间的偶极耦合由具有形式

$$H^D_{1,2} = \frac{\gamma_1\gamma_2\hbar}{4r^3}[\sigma_1\cdot\sigma_2 - 3(\sigma_1\cdot\hat{n})(\sigma_2\cdot\hat{n})] \tag{7.136}$$

的相互作用的 Hamilton 量描述，其中 $\hat{n}$ 是连接两个核子的方向的单位向量，而 σ 是磁矩向量(乘以 2). 在低黏性液体中，偶极相互作用很快被平均掉，在数学上，这可通过证明当平均变得迅速，与偶极耦合的能量大小可比时，$H^D_{1,2}$ 关于 $\hat{n}$ 的球面平均趋于 0.

通过键的相互作用，也称为“J 耦合”，是由化学键共享的电子调制的间接相互作用. 核子看到的磁场被它的电子云撼动，而电子云通过电子波函数的重叠与另一核子相互作用(Fermi 接触相互作用). 这个耦合具有形式

$$H^J_{1,2} = \frac{\hbar J}{4}\sigma_1\cdot\sigma_2 = \frac{\hbar J}{4}Z_1Z_2 + \frac{\hbar J}{8}[\sigma_+\sigma_- + \sigma_-\sigma_+] \tag{7.137}$$

我们将对 J 是标量的情形感兴趣(一般地，它可以是一个张量). 在液体和耦合弱，或相互作用的核子具有非常不同的进动频率的情形下，这是一个很好的近似，这种情况描述为

$$H^J_{1,2} \approx \frac{\hbar}{4}JZ_1Z_2 \tag{7.138}$$

练习 7.35(运动收缩) 证明 $H^D_{1,2}$ 关于 $\hat{n}$ 的球面平均为 0.

3. 热平衡

NMR 与我们在本章前面研究的其他物理系统非常不同. 它使用系统的系综，并且基本的测量为系综平均，而且没有把初态制备到一个如基态的特殊状态的复杂过程. 事实上，做到这一点是对目前技术的挑战.

其实初态是热平衡态

$$\rho = \frac{e^{-\beta H}}{Z} \tag{7.139}$$

其中 $\beta=1/k_BT$，且 $Z=tr(e^{-\beta H})$ 是通常的分配函数的归一化因子，使 $\mathrm{tr}(\rho)=1$. 由于在室温下对典型核子不大的场，$\beta\approx10^{-1}$ 可采用对 n 量子比特的高温度近似

$$\rho\approx 2^{-n}[1-\beta H] \tag{7.140}$$

由于自旋-自旋耦合与进动频率相比非常弱，在 Z 基中热态的密度矩阵非常接近于对角形，于是可以被解释为纯态 $|00\cdots0\rangle$，$|00\cdots1\rangle$，…，$|11\cdots1\rangle$ 的混合. 每个系综成员的真实物理状态到底是什么，存在争论，因为一个给定的密度矩阵存在无穷数目的分解. 原则上，若系综成员是可以访问的(单个分子)，则 NMR 物理状态是可测量的，但这在实验上有困难.

练习 7.36(热平衡 NMR 状态)　对 $n=1$ 证明热平衡态为

$$\rho\approx 1-\frac{\hbar\omega}{2k_BT}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \tag{7.141}$$

而对 $J=2$(和 $\omega_1\approx4\omega_0$)，有

$$\rho\approx 1-\frac{\hbar\omega_B}{4k_BT}\begin{bmatrix}5 & 0 & 0 & 0\\ 0 & 3 & 0 & 0\\ 0 & 0 & -3 & 0\\ 0 & 0 & 0 & -5\end{bmatrix} \tag{7.142}$$

4. 磁化输出

实验的主要输出是自由感应信号，在数学上为

$$V(t)=V_0\mathrm{tr}[e^{-iHt}\rho e^{iHt}(iX_k+Y_k)] \tag{7.143}$$

其中 X_k 和 Y_k 只作用在第 k 个量子比特上，而 V_0 是依赖于线圈的几何参数、品质因数和通过样品体积的最大磁通量. 这个信号产生于探测样品在 $\hat{x}-\hat{y}$ 平面中的磁化的拾取线圈，在实验室中，这个信号会以等于核子进动频率的 ω_0 振荡，不过，$V(t)$ 通常与锁定在 ω_0 的频率混合，然后经过 Fourier 变换，使得最终信号如图 7.17 所示.

练习 7.37(耦合自旋的 NMR 谱)　对 $H=JZ_1Z_2$ 和 $\rho=e^{-\beta H}/4\approx\frac{1}{4}[1-\beta\hbar\omega_0\times(Z_1+Z_2)]e^{-\beta H}$，计算 $V(t)$ 若 Hamilton 量为 $H=JZ_1(Z_2+Z_3+Z_4)$，则第一量子比特的谱中有几条线(具有类似初始密度矩阵)，并且它们的相对幅度是多大?

5. 退相干

自由感生衰减的一个突出特征是磁化信号的指数衰减，自由感生衰减的描述超出我们已阐述的简单模型的范围. 一个原因是静态磁场的不均匀性，它导致处理样品的一部分自旋时，得到另外部分的相位. 不均匀性的效应，原则上是可逆的，但使相位不确定化的其他原因本质上是不可逆的. 例如自旋-自旋的耦合对相位的影响. 另一不确定机制是自旋的在环境温度下的热平衡化，该过程涉及能量交换. 对于一个单量子比特状态，这些效应可以用密度矩阵变换模型唯象地刻画，即

$$\begin{bmatrix} a & b \\ b^* & 1-a \end{bmatrix} \rightarrow \begin{bmatrix} (a-a_0)e^{-t/T_1}+a_0 & be^{-t/2T_2} \\ b^* e^{-t/2T_2} & (a_0-a)e^{-t/T_1}+1-a_0 \end{bmatrix} \tag{7.144}$$

其中 T_1 和 T_2 分别称为自旋-点阵(或纵向)和自旋-自旋(或横向)弛豫率，而 a_0 刻画了热平衡状态，它们定义了非平衡态下，经典状态和量子叠加态寿命的主要时间尺度. NMR 系统中计算 T_1 和 T_2 的理论工具很成熟，并且事实上，这些比率的测量，在用 NMR 区分不同种类的化学样品中起重要作用.

NMR 中测量 T_1 和 T_2 的实验方法是众所周知的. 令 $R_x=e^{-iX/4}$ 是绕 $\hat{x}$ 的 90° 脉冲，为测量 T_1，应用 R_x^2，等待 τ 时间，然后应用 R_x. 第一个脉冲把自旋翻转 180°，然后它向返回平衡态方向弛豫一段时间 τ(把这想象为 Bloch 向量向 Bloch 球面的顶部，即基态，回缩)，而最后的 90°脉冲使磁化方向处于被检测的 $\hat{x}-\hat{y}$ 平面. 这个倒置-恢复实验测到的磁化强度 M，随 τ 为指数衰减，$M=M_0[1-2\exp(-\tau/T_1)]$. 为测量 T_2，若只求一阶近似，可以只测峰值的线宽. 更精确的方法是采用 Carr-Purcell-Meiboom-Gill 技术，应用一个 R_x 旋转，然后进行 k 次"等待 $\tau/2$ 时间，应用 R_x^2，等待 $\tau/2$ 时间，应用 R_x^2"的循环. 这一串 180°的脉冲"再聚焦"耦合(7.7.3 节)，并且部分消除了 B_0 场的非均匀性，于是可以更好地估计系统 T_2 的真实值. 观测到的磁化强度按 $M=M_0e^{-kt/T_2}$ 衰减.

6. 多自旋的 Hamilton 量

总结对 NMR Hamilton 量的讨论，可将 n 自旋耦合系统的 H 写作

$$H=\sum_k \omega_k Z_k+\sum_{j,k} H^J_{j,k}+H^{RF}+\sum_{j,k} H^D_{j,k}+H^{env} \tag{7.145}$$

其中首项为自旋在周围磁场中的自由进动，H^D 为式(7.136)中的磁偶极耦合，H^J 为式(7.137)的 J 耦合，H^{RF} 描述式(7.135)的外加射频磁场的效应，H^{env} 描述式(7.144)中导致退相干的环境作用.

为理解操作这个 Hamilton 量的基本原理，我们在下面的讨论中主要考虑简化的 Hamilton 量

$$H=\sum_k \omega_k Z_k+\sum_{j,k} Z_j\otimes Z_k+\sum_k g_k^x(t)X_k+g_k^y(t)Y_k \tag{7.146}$$

与更一般形式式(7.145)处理的思想相同.

7.7.3 量子计算

量子信息处理需要对制备成适当初态的系统进行酉变换. 当前系统面临三个问题：首先，在由 Hamilton 量式(7.146)描述的 n 耦合自旋系统中，如何实现任意酉变换？其次，NMR 的热状态式(7.140)怎样用作计算的适当初态？第三，我们在最近三章中研究的量子算法，要求用投影测量来获得输出结果，而对 NMR，容易的只是获得进行系综平均的测量. 我们如何解决系综的输出测量问题？本节将回答这些问题.

1. 再聚焦

NMR 中有名的再聚焦，或许是对式(7.146)类型 Hamilton 量，进行任意酉变换的最有趣的一项可行技术. 考虑简单的双自旋 Hamilton 量 $H=H^{\rm sys}+H^{\rm RF}$，其中

$$H^{\rm sys}=aZ_1+bZ_2+cZ_1Z_2 \tag{7.147}$$

如 7.7.2 节所示，当施加一个适当频率的强大 RF 场时，我们有很好的近似

$$e^{-iHt/\hbar}\approx e^{-iH^{\rm RF}t/\hbar} \tag{7.148}$$

这使我们以足够高保真度，进行任意的单量子比特运算. 定义

$$R_{x1}=e^{-i\pi X_1/4} \tag{7.149}$$

为自旋 1 上绕 $\hat{x}$ 轴 90°的旋转，对自旋 2 也可类似定义. 容易验证 180°旋转 R_{x1}^2 具有特殊的性质

$$R_{x1}^2e^{-iaZ_1}R_{x1}^2=e^{iaZ_1} \tag{7.150}$$

这个过程被称为再聚焦，因为它翻转了时间演化的方向，使得 Bloch 球面上从某一点上出发的不同频率的自旋，又回到 Bloch 球面上的同一点. 以这种方式应用的 180°脉冲，称为再聚焦脉冲. 注意在上述表达式中，a 可以是一个算子或常数(只要不包含作用在自旋 1 上的算子)，于是

$$e^{-iH^{\rm sys}t/\hbar}R_{x1}^2e^{-iH^{\rm sys}t/\hbar}R_{x1}^2=e^{-2icZ_1t/\hbar} \tag{7.151}$$

运用在自旋 2 上的另一组再聚焦脉冲，可消除这一剩余项. 再聚焦因而是，一项消除自旋间耦合项的演化以及彻底消除演化的有用技术.

练习 7.38(再聚焦)　具体证明式(7.150)是对的(利用 Pauli 矩阵的反对易性).

练习 7.39(三维再聚焦)　怎样的一组脉冲，可以对任意单自旋 Hamilton 量 $H^{\rm sys}=\sum_k\sigma_k\sigma_k$ 下的演化再聚焦?

练习 7.40(偶极相互作用的再聚焦)　给出一串脉冲，使双自旋偶极耦合 $H_{1,2}^{\rm D}$ 变成简单得多式(7.138).

2. 受控非门

利用再聚焦脉冲和单量子比特脉冲容易实现受控非门. 让我们来看，对具有 Hamilton 量式(7.147)的双自旋系统是如何做的. 由式(7.46)的构造，我们知道能够实现酉变换

$$U_{CZ}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix} \tag{7.152}$$

就可以了. 因为 $ie^{iZ_1Z_2\pi/4}e^{-iZ_1\pi/4}e^{-iZ_2\pi/4}=U_{CZ}$，从一个时段为 $\hbar\pi/4c$ 的演化，加上若干单量子比特脉冲，就可直接得到受控非门.

练习 7.41(NMR 受控非门)　具体给出单量子比特旋转的序列，它由在

Hamilton量式(7.147)下演化的两个自旋直接受控非门的自旋实现.你可以从式(7.46)开始,但结果可以在减少单量子比特旋转数目方面被简化.

3. 时间、空间和逻辑标记

能够用RF脉冲,以高保真度实现自旋系统上的任意酉变换,是NMR在量子计算上最吸引人的方面之一.然而,主要的不足是初态通常为式(7.140)的热状态.当然,尽管这状态的熵高,花一定代价,量子计算还是可以完成的.能完成它,有两种技术称为时间和逻辑标记.

时间标记,有时称为时间平均,它基于两个重要的事实:量子运算是线性的,并且NMR中可以观测量的迹为0(参考2.2.5节量子测量的背景知识).设一个双自旋系统,从密度矩阵

$$\rho_1 = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{bmatrix} \tag{7.153}$$

出发,其中 a,b,c 和 d 是满足 $a+b+c+d=1$ 的任意正数.我们可以用从受控非门构造的线路 P,来得到置换后的状态

$$\rho_2 = P\rho_1 P^\dagger \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & d & 0 \\ 0 & 0 & 0 & b \end{bmatrix} \tag{7.154}$$

类似地

$$\rho_3 = P^\dagger \rho_1 P \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & d & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & c \end{bmatrix} \tag{7.155}$$

应用酉量子运算 U 到每个状态上,可得(可能在不同时间进行的三次分开的实验中)$C_k = U\rho_k U^\dagger$.由线性

$$\sum_{k=1,2,3} C_k = \sum_k U\rho_k U^\dagger \tag{7.156}$$

$$= U\left[\sum_k \rho_k\right] U^\dagger \tag{7.157}$$

$$= (4a-1)U \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} U^\dagger + (1-a) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{7.158}$$

在NMR中,只能观测到 $\mathrm{tr}(M)=0$ 的可观测量 M(如Pauli算子 X 和 Y),于是

$$\mathrm{tr}\left(\sum_k C_k M\right)=\sum_k \mathrm{tr}(C_k M) \tag{7.159}$$

$$=(1a-1)\mathrm{tr}\left\{U\begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}U^{\dagger}M\right\} \tag{7.160}$$

$$=(4a-1)\mathrm{tr}(U\mid 00\rangle\langle 00\mid U^{\dagger}) \tag{7.161}$$

我们发现，三次实验的测量信号之和将与我们把原系统制备为纯态$|00\rangle\langle 00|$，而不是式(7.153)那样的任意状态所得到的结果成比例. 只要对足够多的实验结果求和，在退相干发生之前，有足够长的酉运算相干时间，对任意规模的任意状态的系统，就总是可以做到这一点. 注意，不同的 C_k 实验，也可以在三个不同的系统或一个系统的不同部分同时进行. 这在实验上是可行的，可以在单一样品上应用规则变化的梯度磁场，这种技术的变化称为空间标记.

练习 7.42(时间标记置换)　给出一个量子线路，完成把式(7.153)的 ρ_1 变到式(7.154)的 ρ_2 的必要置换 P 和 $P^{\dagger}$.

逻辑标记基于类似的观察，但不要求进行多次实验. 设我们有一个包含三个几乎相同自旋的处于状态

$$\rho=\delta I+\alpha\begin{bmatrix}6&0&0&0&0&0&0&0\\0&2&0&0&0&0&0&0\\0&0&2&0&0&0&0&0\\0&0&0&-2&0&0&0&0\\0&0&0&0&2&0&0&0\\0&0&0&0&0&-2&0&0\\0&0&0&0&0&0&-2&0\\0&0&0&0&0&0&0&-6\end{bmatrix} \tag{7.162}$$

$$\approx\left(\delta' I+\alpha'\begin{bmatrix}2&0\\0&-2\end{bmatrix}\right)^{\otimes 3} \tag{7.163}$$

的系统，其中 δI 指不可观测的背景自旋(由于观测量的测量的迹为 0)，并且 $\alpha\ll\delta$ 是一个小常数. 我们可以应用执行置换 $\hat{P}$ 的酉运算，给出

$$\rho'=\hat{P}\rho\hat{P}^{\dagger}=\delta I+\alpha\begin{bmatrix}6&0&0&0&0&0&0&0\\0&-2&0&0&0&0&0&0\\0&0&-2&0&0&0&0&0\\0&0&0&-2&0&0&0&0\\0&0&0&0&-6&0&0&0\\0&0&0&0&0&2&0&0\\0&0&0&0&0&0&2&0\\0&0&0&0&0&0&0&2\end{bmatrix} \tag{7.164}$$

注意该矩阵上方的 4×4 块具有形式

$$\begin{bmatrix} 6 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -2 \end{bmatrix} = 8\,|00\rangle\langle 00| - 2I \tag{7.165}$$

其中 I 指 4×4 的单位阵. 正如时间标记，我们发现，如果计算在这样一个状态上进行，对此例为状态 $|000\rangle$，$|001\rangle$，$|010\rangle$，$|011\rangle$，则产生正比于原系统制备为纯态 $|00\rangle\langle 00|$ 所得的结果. 实验上，进行 $\tilde{P}$ 是可能的，并且把信号和这组状态分离也是可能的.

具有形式 $\rho=2^{-n}(1-\varepsilon)I+\varepsilon U|00\cdots0\rangle\langle 00\cdots0|U^{\dagger}$（其中 U 是任意酉运算）的状态，称为有效纯态或伪纯态. n 是量子比特的数目，但一般而言，Hilbert 空间的维数不必是 2 的幂. 有许多方法来制备这样的状态，但都需要付出某种代价. 我们在 7.7.4 节会回到这个问题. 只要系统与它的高温环境的耦合很小，有效纯态就使我们从较高温度的平衡态观测得到温度为 0 的动态，这正是有效纯态用在 NMR 量子计算中的方式.

练习 7.43（逻辑标记置换） 给出一个量子线路，实现把式(7.163)的 ρ 变为式(7.165)的 ρ' 的置换 $\tilde{P}$.

练习 7.44（n 自旋的逻辑标记） 设有一系统，包含 n 个几乎相同的，具有 Zeeman 频率 $\hbar\omega$，处于温度 T 的热平衡态 ρ 的自旋. 用逻辑标记，可以从 ρ 构造的最大有效初态是什么（提示：利用具有 $n/2$ Hamming 权标记的状态）?

4. 量子算法结果的系综输出

我们已说明如何在一个具有 Hamilton 量式(7.146)的 n 自旋系统上进行任意酉变换，并且知道如何从一个热状态制备一个，可看作低熵基态的定义良好的输入. 不过为完成量子计算的要求，我们必须找到测量系统计算结果的办法. 困难在于典型量子算法输出是一个随机数，其分布给出解决问题的信息. 不幸的是随机变量的均值可能不提供任何相关信息. 若在 NMR 量子计算机上不做任何修改地执行量子算法，输出的就是均值，因为量子算法在分子的大系综上进行，而不是在一个单 n 自旋分子上进行.

下面以例子来说明这个困难. 量子因子分解算法输出一个随机有理数 c/r，其中 c 是一个未知整数，而 r 是期望的结果（也是整数）. 一般地，可以用一个投影测量得到 c/r，然后进行经典连分数算法，以高概率得到 c(5.3.1 节). 然后就把结果代到原问题中来，检查答案，如果失败就重复整个算法. 不过不幸的是，如果只有系综的平均，由于 c 几乎是均匀分布的，均值 $\langle c/r\rangle$ 将不给出有用的信息.

对所有基于隐含子群问题（第 5 章）的量子算法都适用的一个简单的解决办法，是把需要的所有经典后续处理步骤都附加到量子算法后面. 这总是可能的，因

为量子计算是经典计算的超集. 在上述例子中，我们只要求每个量子计算机（每个分子）执行连分数算法，然后在每个量子计算机上检查结果，而且只有在验证中成功的计算机产生输出. 最后的系综平均的测量就给出$\langle r\rangle$.

7.7.4　实验

NMR 方法最令人激动的方面是，已进行的一小批量子计算与量子信息任务实例的实验实现. 在对 NMR 总结的本节，我们简要地描述已进行过的展示状态层析术、基本逻辑门和量子搜索算法的三个实验，以及这些方法的不足.

1. 状态层析

如何调试量子计算机？经典计算机的分析是通过在不同时刻对内部状态的测量进行的. 相应地，对量子计算机，一项核心技术是测量密度矩阵的能力，这称为状态层析术.

单量子比特的密度矩阵可表示为

$$\rho=\frac{1}{2}\left[1+\sum_k r_k\sigma_k\right] \tag{7.166}$$

其中 σ_k 是 Pauli 矩阵，而 r_k 是实三元向量. 由于 Pauli 矩阵的迹正交性质

$$\mathrm{tr}(\sigma_j\sigma_k)=2\delta_{jk} \tag{7.167}$$

可知 ρ 可从三个测量结果

$$r_k=\langle\sigma_k\rangle=\mathrm{tr}(\rho\sigma_k) \tag{7.168}$$

重构.

在通常 NMR 中的观测之前，加上适当的单量子比特脉冲，使我们能够确定 $\langle\sigma_k\rangle$，然后得到 ρ. 类似结果对大量的自旋也成立. 实际中，仅测量 ρ 和单位阵的迹为 0 的偏差是方便的，这称为偏差密度矩阵. 图 7.18 给出两个和三个自旋的结果的例子.

练习 7.45（用 NMR 的状态层析）　令实验 k 的电压测量结果是 $V_k(t)=V_0\,\mathrm{tr}[\mathrm{e}^{-iHt}M_k\rho M_k^{\dagger}\mathrm{e}^{iHt}(iX_k+Y_k)]$，证明对双自旋，九次实验，其中 $M_0=I$，$M_1=R_{x1}$，$M_2=R_{y1}$，$M_3=R_{x2}$，$M_4=R_{x2}R_{x1}$，$M_5=R_{x2}R_{y1}$ 等，提供了重构 ρ 的足够数据.

练习 7.46　对三自旋，多少次实验是充分的？多少次是必要的？

2. 量子逻辑门

由于多方面原因，三氯甲烷中的质子-碳双量子比特称为单量子比特和双量子比特门的极好实例. 在约为 11.8T 磁场中，两个自旋的频率约为 500MHz 和 125MHz 可以很好分离和定位. 两个核的 215Hz J 耦合频率也很合适，它远低于单量子比特 RF 脉冲的时间尺度，而又远快于弛豫时间尺度. 在典型实验中，质子

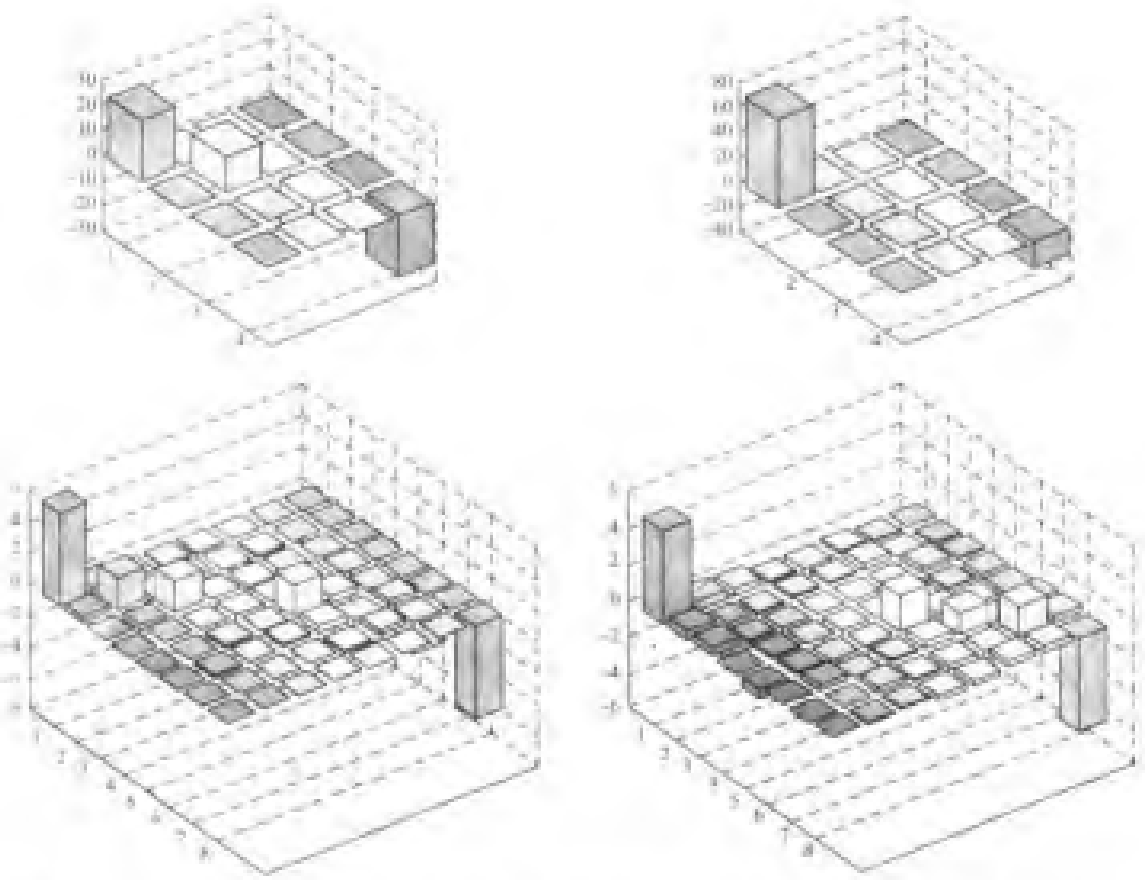


图 7.18 实验测量的偏差密度矩阵，垂直单位是任意的，只显示了实部，虚部相对都很小。（左上）质子和三氯甲烷（$^{13}CHCl_3$）中碳核的双量子比特在 11.78T 磁场中的热平衡态，0.5ml，0.2mol 样品在丙酮-d_6 中稀释，除气，火封于薄壁 5mm 玻璃管中。（右上方）用三氯甲烷做时间标记产生的双量子比特如式(7.161)的有效纯态。（左下方）三氟氯乙烯中的三氟核的三量子比特热平衡态。（右下方）用逻辑标记从三自旋系统产生的如式(7.164)的有效纯态。

和碳的 T_1 分别接近 18s 和 25s，而 T_2 是 7s 和 0.3s，碳的 T_2 短的原因是，三个氟核四偶极子的相互作用，但取最短的 T_2 寿命和 J 耦合的乘积显示，在失去量子相干之前仍可实现 60 个门。

双自旋系统的 Hamilton 量可用式(7.147)进行很好的近似，但用一个实验的技巧可以将其大大简化。把两个振荡器严格调到质子和碳的旋转频率，我们得到在振荡器定义的旋转框架中，简化的 Hamilton 量

$$H = 2\pi\hbar J Z_1 Z_2 \tag{7.169}$$

其中 $J = 215\text{Hz}$。该 Hamilton 量使受控非门的实现相当简单。除了一个单量子比特相位，进行 CNOT 变换的一个量子线路如图 7.19 所示，其中还给出了产生 Bell 态的线路和实验得到的测量结果。

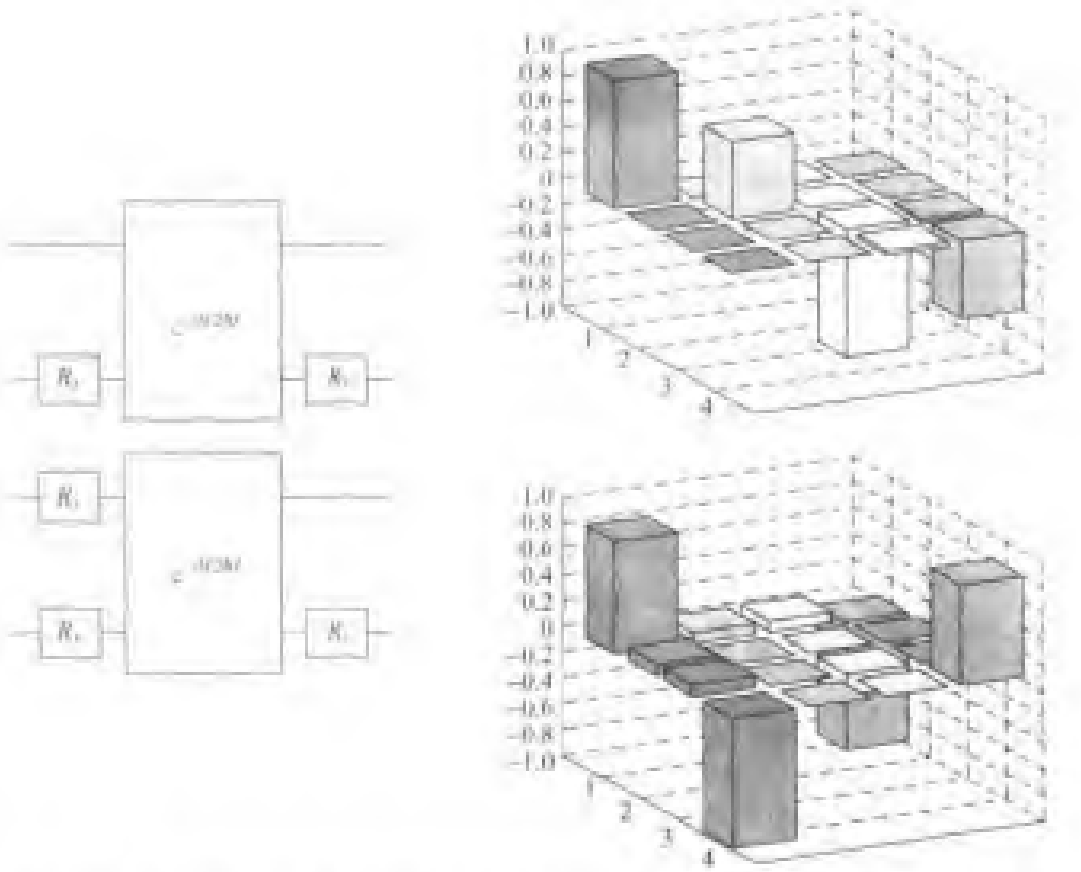


图 7.19 用 NMR 实现的量子线路和测得的输出偏差密度矩阵的实部. 在这些线路中，R_x 和 R_y 表示绕 $\hat{x}$ 和 $\hat{y}$ 进行 90°旋转的单量子比特门，用约 10ms 长的 RF 脉冲实现，$e^{-i\pi ZZ/4}$ 的双量子比特框是一个持续 $1/2J\approx 2.3$ms 的自由演化.（上方）受控非线路和对应热状态输入的输出，显示对角元 $|10\rangle$ 和 $|11\rangle$ 的交换，正如 CNOT 门的经典真值表所预期的.（下方）产生 Bell 态 $(|00\rangle-|11\rangle)/\sqrt{2}$ 的线路和对应于输入制备为有效纯态 $|00\rangle$ 的输出.

练习 7.47（NMR 受控非门） 验证图 7.19 上方所示线路，除了一个单量子比特相位，完成受控非门运算，即它在经典输入状态上进行适当作用，可通过施加一个额外的单量子比特 R_z 来变成受控非门. 给出采用相同模块，实现 CNOT 门的另一线路.

练习 7.48 验证图 7.19 左下方线路能产生 Bell 态 $(|00\rangle-|11\rangle)/\sqrt{2}$.

练习 7.49（NMR 交换门） NMR 的一个重要化学应用是测量自旋的连接，即分子中的质子、碳原子和磷原子怎样相互邻接. 完成这项任务的脉冲称为 INADEQUATE（即 incredible natural abundance double quantum transfer 实验）. 从量子计算角度可以理解为在任意两个共振之间施加 CNOT，如果 CNOT 起作用，两个核子必相邻. 序列中用到的另一个模块如 TOCSY（全相关光谱学）是交换

运算，不过并非只用量子门就能描述，用 $e^{-H/2kJ}$，R_x 和 R_y 运算就可实现交换门（可以从图 1.7的线路开始）.

3. 量子算法

Grover 量子搜索算法是 NMR 量子计算的另外一个简单例子. 对四个元素规模的问题（$n=2$ 量子比特），给定集合 $x=\{0,1,2,3\}$，除一点 x_0 使 $f(x)=1$ 外，其余 $f(x)=0$. 我们的目标是找出 x_0. 经典算法通过平均 2.25 次计算 $f(x)$的值，可以完成. 相应地，量子算法只一次计算 $f(x)$的值就可找到 x_0（第 6 章，特别是盒子 6.1）.

我们需要三个算子：黑箱算子 O（基于函数 $f(x)$进行相位翻转）、双量子比特 $H^{\otimes 2}$ 上的 Hadamard 算子，和条件相移算子 P. 黑箱 O 翻转对应子 x_0 的基元素的符号，如对 $x_0=3$，即

$$O=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix} \tag{7.170}$$

把时间 $t=1/2J$（对三氯甲烷是 2.3ms）的演化 $e^{iH/2kJ}$ 记作 τ，可知对 $x_0=3$ 的情况，$O=R_{y1}\bar{R}_{x1}\bar{R}_{y1}R_{y2}\bar{R}_{x2}\bar{R}_{y2}\tau$（除了一个不相关的全局相位因子）. $H^{\otimes 2}$ 就是两个单量子比特 Hadamard 运算，$H_1\otimes H_2$，其中 $H_k=R_{xk}^2\bar{R}_{yk}$. 并且算子 P

$$P=\begin{bmatrix}1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&-1\end{bmatrix} \tag{7.171}$$

可以实现为 $P=R_{y1}R_{x1}\bar{R}_{y1}R_{y2}R_{x2}\bar{R}_{y2}\tau$. 基于这些结果可构造 Grover 迭代，$G=H^{\otimes 2}PH^{\otimes 2}O$. 通过消去明显的抵消项，可化简该算子（见练习 7.51）. 令 $|\psi_k\rangle=G^k|00\rangle$ 是初态经过 k 次反复运用 Grover 迭代后的状态，可知幅度 $\langle x_0|\psi_k\rangle\approx\sin[(2k+1)\theta]$，其中 $\theta=\arcsin(1/\sqrt{2})$. 这里的周期性是量子搜索算法的一个基本性质，也是实验中要测试的特征. 对双量子比特和 $x_0=3$ 情形，应有 $|11\rangle=|\psi_1\rangle=-|\psi_4\rangle=|\psi_7\rangle=-|\psi_{10}\rangle$，如果舍弃所有符号，则周期为 3.

练习 7.50 只用单量子比特旋转和 $e^{-iH/2kJ}$，对 $x_0=0,1,2$ 实现黑箱 O.

练习 7.51 证明 Grover 迭代，通过适当消去单量子比特旋转可以化简，对 x_0 的四种可能情形，可得

$$G=\begin{cases}\bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau R_{x1}\bar{R}_{y1}R_{x2}\bar{R}_{y2}\tau, & x_0=3\\ \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau R_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau, & x_0=2\\ \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau \bar{R}_{x1}\bar{R}_{y1}R_{x2}\bar{R}_{y2}\tau, & x_0=1\\ \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau, & x_0=0\end{cases} \tag{7.172}$$

图 7.20 给出 U 的头七次迭代的偏差密度矩阵 $\rho_{dx}=|\psi_x\rangle\langle\psi_x|-\mathrm{tr}(|\psi_x\rangle\times\langle\psi_x|)/4$的理论和测量结果，如所预期的，$\rho_{21}$ 清楚地明显对应于 $x_0=3$ 的状态 $|11\rangle$，对 x_0 的其他可能值，通过重复实验可获得类似的结果。测量每个密度矩阵需要$9\times3=27$次重复实验，9 次层析重构，3 次纯态制备。

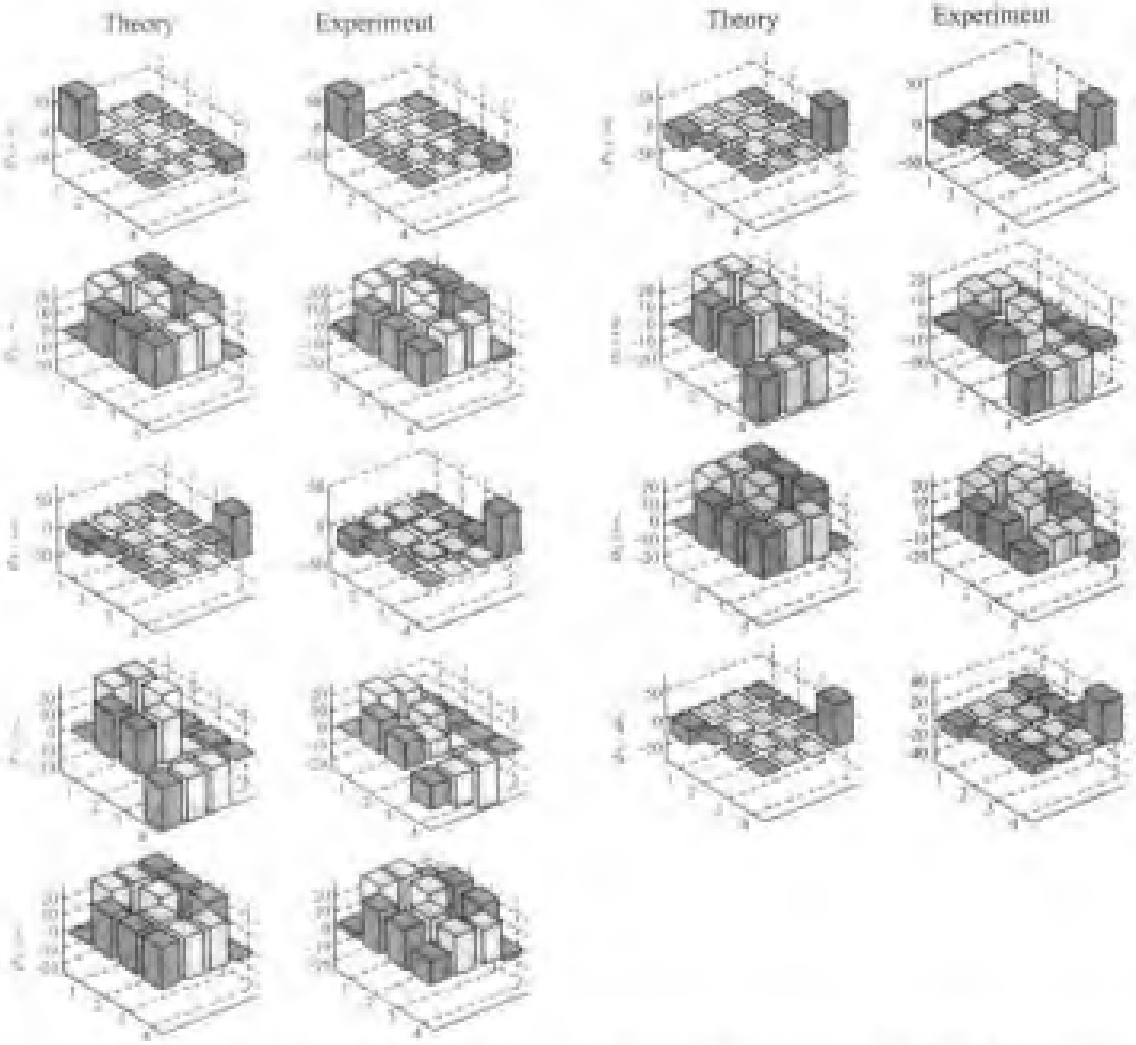


图 7.20　对在三氯甲烷中碳和氢自旋上进行的，Grover 算法七个步骤的偏差密度矩阵（单位任意）的理论和实验结果。可明显看到一个周期为 4 次迭代的三个完整的循环。只画出了实部（虚部理论上是 0，对实验结果的贡献小于 $12\|\rho_{theory}-\rho_{expt}\|/\|\rho_{theory}\|$。

对 $n=7$ 最长的计算，不超过 35ms，肯定会落在相干时间之内。Grover 算法的周期性在图 7.20 中可清楚地看到，理论和实验非常符合，只进行单次实验就能获得很高的信噪比（典型情形下好于 $10^4:1$）。数值仿真显示 7%～44%的误差是由磁场不均匀，测量中的磁性衰减和旋转校准不良（到不能忽略的程度）引起的。

4. 不足

量子计算的整体系综 NMR 实现，已成功展示于七个量子比特系统上所进行的量子算法和量子信息任务，这给人很深印象，不过，这种方法的核心——时间、空间和逻辑标记技术却存在严重局限性.

这些标记技术的根本目的是，把信号和热平衡态的偶然处于 $|00\cdots0\rangle$ 分量（或任何其他标准的高概率状态）的自旋子集分开. 时间和空间标记是通过把信号相加，来消去除期望状态之外的所有状态；逻辑标记则在 Hilbert 空间和纯性之间作折衷. 然而不管用什么方法，也无法增加热平衡态 $|00\cdots0\rangle$ 分量的概率

$$p_{00\cdots0} = \frac{1}{Z}\langle 00\cdots0 \mid \mathrm{e}^{-\beta H} \mid 00\cdots0\rangle \tag{7.173}$$

取 $H = \sum_k \omega Z_k$，我们发现对一个 n 自旋分子，$p_{00\cdots0}$ 正比于 $n2^{-n}$. 这意味着对于定常的状态温度，整个信号随用标记技术“蒸馏”到有效纯态的量子比特数目按指数衰减.

另外一方面的局限在于把分子作为量子计算机. 分子相当于计算机体系结构，决定着对什么样的量子比特对（或组）发生相互作用（相应地，RF 脉冲充当软件）. 不是所有量子比特都必须连接，这非常重要. 因为相互作用不能被关闭，除非进行再聚焦；而且，量子比特是通过不同频率进行寻址的，但随核子数目的增加很快就变得困难起来. 有一个解决办法就是采用元胞自动机型的体系结构，例如两端不同中间为重复规则序列的 $X-A-B-C-A-B-C-\cdots-A-B-C-Y$ 式的一维链. 在这个体系结构中，只有不同的字母是可寻址的，看起来似乎是非常受限制的计算模型，然而，已经证明，它是通用的，仅仅是多项式减速. 当进行诸如量子搜索的任务时，精确的减速量自然是很重要的，因为该算法也仅为二次加速.

克服标记技术局限性的方法也是有的，一种可能的办法是通过某种物理机制将核子极化. 已经用光抽运（类似图 7.8 中离子的冷却）极化铷原子的电状态实现，铷原子通过形成短寿命的 van der Waals 分子把极化传给氙原子核. 对氦也做到了. 对分子做类似的极化也是可以想象的，尽管技术上很有挑战性. 另一可能方法是使用不同的标记方案，逻辑标记本质上是一种压缩算法，通过舍弃系综成员，增加系综处于一个状态的相对概率. 已开发出的可以达到熵极限的改进方案，能从初始处于使得 $p=(1-\mathrm{e}^{-\Delta E/k_{\mathrm{B}}T})/2$ 的温度 T 的 n 自旋分子给出 $nH(p)$ 个纯量子比特，其中 ΔE 是自旋翻转能量. 这个方案不需要任何指数费用，压缩可用多项式数目的基本运算做到. 不过除非 p 相对很小，它是不够的，现今在好的螺线管磁系统中 $p\approx0.4999$.

虽然有上述不足，NMR 还是为量子算法提供了实验床，并说明为进行量子计算，其他实现方法必须具备的基本技术. 图 7.21 给出了一些已经用于演示量子计

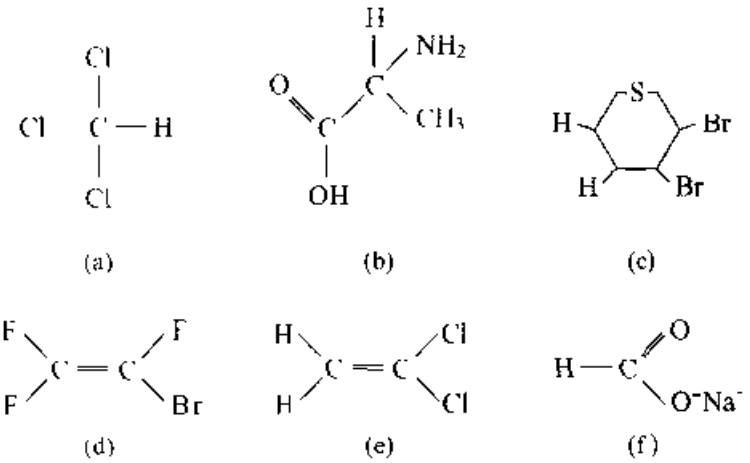


图 7.21 已用于展示进行不同量子计算与量子信息任务的一些简单分子.(a)三氯甲烷：两个量子比特，质子和碳，已用于实现 Deutsch-Jozsa 算法和双量子比特搜索.(b)丙氨酸：三量子比特，由碳主干组成，已用于说明纠错.注意三个碳核由于周围化学环境的不同而具有不同的频率(例如氧的电负性使电子远离附近的碳).(c)2,3-二溴磷噻粉：双量子比特，由两个质子组成，用于模拟截断的简单谐振子的四个层次.这里，两个质子与硫原子的距离不同，因而有不同的频率.(d)三氟氯乙烯：三量子比特，三个氟原子，用于演示逻辑标记和叠加态$|000\rangle+|111\rangle/\sqrt{2}$的生成.(e)三氯乙烯：三量子比特，质子和两个碳，用于演示隐形传态，把质子的状态传到最右端的碳.(f)钠甲酸盐：双量子比特，质子和碳，用于演示双量子比特差错检测编码.在这个分子中，通过改变背景温度改变与溶剂的交换速率.钠基团可用于调节两个量子比特的 T_2 时间使之基本相同.

算与量子信息任务的分子.NMR 的思想也是结合化学、物理学、工程和数学的一个充满新事物的领域，毫无疑问，结合不同学科的创新会促进该技术的发展.

5. NMR 量子计算机

• 量子比特表示：原子核的自旋.

• 西演化：任意变换由强磁场中施加于自旋的磁场脉冲构造，自旋之间的耦合通过相邻原子间化学键提供.

• 初态制备：通过将自旋置于强磁场使之极化，然后使用“有效纯态”制备技术.

• 输出的读取：测量由进动磁矩感应的电压信号.

• 不足：有效纯态制备方案使信号的量子比特数目指数减少，除非初始极化率足够高.

7.8 其他实现方案

本章中我们只描述了量子计算机实现的部分想法.我们的例子说明了所有实现都遇到的基本要求和挑战:量子信息的鲁棒表示,酉运算的应用,基准输入状态的制备和输出的测量.

简单谐振子的例子强调,为什么数字表示非常关键:每个单位(qubit,qutrit,qudit 或其他任何名称)的量子信息必须存放在物理上分开的自由度,否则,某些资源(如能量)就没有充分利用.这个例子也为研究本章其余部分量子比特的实现提供了数学基础.单光子近乎理想的量子比特,但它们相互作用需要的非线形光学材料,在不引起相干损失条件下,很难获得.C-QED 技术用单原子产生光子相互作用,可以解决这个问题,但更重要的是,这类技术引入了双能级原子的概念,以及基于物理学对称性选择规则来保持量子比特表示的思想,如偶极选择.

这个思想的自然推广是,用本质上只有两个状态的自旋 1/2 粒子来表示量子比特.这正是采用束缚离子把量子比特存到电子和核自旋中所用的方法,不过这种方法的困难在于,用于调节自旋间相互作用的物质振荡的中心——光子——只有很短的相干时间.可通过化学键形成核自旋强耦合的分子解决这个问题,但单分子的自旋共振信号,对目前技术来说,太弱而无法检测到.NMR 量子计算通过用 $O(10^{18})$ 分子的整体系综生成有效纯态来解决这个问题,并可在实验室中演示简单的量子算法.但不提供初始极化,这方面的计算能力将以信号强度为代价,随量子比特的数目指数下降.

这些例子说明,给出量子计算机的好的物理实现需要高度技巧,并需要考虑各种折衷.以上方案都不尽人意,没有一种可以使我们在近期内实现大规模的量子计算机,然而,这并不排除存在其他实现方案的可能性.下面就在这最后一节中简略介绍其中几种.

按表示量子比特的物理自由度是对实现分类的一个好的方法.回忆图 7.1:几乎所有具有量子化单位的量都可以作为量子比特,但如我们看到的,基本物理学量子,如光子和自旋,是特别好的选择.

另一个可以作为量子比特表示的基本量子单位是电荷.现代电子学提供了甚至在单电子水平上产生、控制和测量电荷的高超技术.例如,从半导体材料,金属甚至是小分子制造出的量子点,可用作约束带电量子的静电势的三维盒子,可通过观察 Coulomb 阻挡效应来验证这一点.实验中发现,通过电容 C 的量子点的电导,作为量子点的偏置电压函数,它是按离散步长增加的,每增加一个电子需要 $e^2/2C$ 的能量.与光子不同,(纯)电荷不能被消灭,电荷只能移动,因此带电态量子比特必须采用某种类似于 7.4.2 节中双轨表示的形式,$|0\rangle$ 和 $|1\rangle$ 状态分别对应于两个量子

点有电荷或在一个单量子点内的两个状态.

正如单光子，在带电态量子比特上的单量子比特运算可用静电门(对应光学移相器)和或者用子移动电子的单模波导耦合器(对应分束器)，或者用作量子点的隧道结实现. 电荷与其他电荷具有长程的 Coulomb 相互作用（单电荷产生的势在距离 r 处为 $V(r)=e/4\pi\varepsilon r$)，故远处的电荷可以调制局部电荷的相位，很像光子间的 Kerr 相互作用. 于是受控 Coulomb 相互作用，可用来进行双量子比特运算. 最后，单电荷可直接测量，现代场效应晶体管很容易探测到单电荷在沟道中运动，并且在约为 100mk 温度下，单个晶体管可以探测电荷的精度，在频率 f 为 200MHz 范围内优于 $10^{-4}e/\sqrt{f}$. 不幸的是，远处非受控电荷的运动会引起退相，这个以及其他如由光子相互作用引起的散射机制，使带电态的相干时间相对较短，为几百飞秒到几百皮秒.

超导体中的电荷载体也曾被建议用于表示量子比特. 某些金属在低温下，两个电子可以通过一个光子的相互作用形成一个具有电荷 $2e$ 的 Cooper 对. 正像电子可以被限制于量子点中，Cooper 对也可以被限制在静电盒子里，使得盒子中的 Cooper 对的数目是一个好量子数，并可用于表示量子信息. 单量子比特运算，可以通过静电门调节盒子位势和耦合的盒子间的 Josephson 结来实现. 这些结还可用于把量子比特耦合起来，而其强度可以用与超导干涉回路适当耦合的外磁场调节. 最后，量子比特的测量可通过测量电荷完成. 这种超导体量子比特表示有意义的原因在于，Cooper 对的相对鲁棒性，据估计主要的退相干机制是偶然的电磁光子发射，这或许会让相干时间超过 1ms，相对几百皮秒的典型动态时间尺度要长些. 不幸的是，正像电荷表示，寄生电荷(准粒子)的背景起伏对量子比特的相干有很大取消作用. 解决这个问题的一个方法是，选用磁通量量子比特表示. 这种表示中，量子比特状态对应于通过超导回路装置定位磁通量左右手定向. 这里，退相干是背景磁场起伏引起的，它预期比静电场情形平静得多.

磁相互作用的定域性对量子比特表示是很好的性质，因此我们回到自旋. 对自旋，还是利用固态技术的方案. 一个相当大的量子点，甚至包含许多电子的量子点，可以表现得像一个自旋 1/2 的对象，其中自旋由一个单额外电子承载. 该自旋态可以通过在低温下，强磁场中使自旋的翻转能 ΔE 远大于 k_BT 达到的平衡来制备. 如 7.7 节所述，通过施加局部磁场脉冲，可以实现对单个自旋的操作，而耦合的量子比特运算可用受控 Heisenberg 耦合实现

$$H(t)=J(t)\boldsymbol{S}_1\cdot\boldsymbol{S}_2=\frac{1}{4}[X_1X_2+Y_1Y_2-Z_1Z_2] \tag{7.174}$$

其中 $\boldsymbol{S}$ 是自旋算子(Pauli 算子除以 2)，而 $J(t)=4\tau_0^2(t)/u$，u 是量子点的电荷能量，τ_0 是由放置于量子点之间的局部静电门控制的隧道矩阵元素. 这个相互作用在等价于受控非门(见练习 7.52)的意义下是通用的. 理论上，自旋状态可以通过，

允许自旋承载电子穿越到输出顺磁量子点，或依赖于自旋方式穿越一个“自旋阀”，到达输出静电计来测量. 困难在于在实践中实现这样的测量，在目前技术条件下，尚未完成在半导体中高保真量进行单自旋的测量.

练习 7.52(Heisenberg Hamilton 量的通用性) 证明通过在 Heisenberg 耦合 Hamilton 量(7.174)中打开 $J(t)$ 适当时间，可实现互换运算 U，得到 $U=\exp(-\mathrm{i}\pi \boldsymbol{S}_1 \cdot \boldsymbol{S}_2)$. 打开这个时间的一半，得到的 $\sqrt{\mathrm{SWAP}}$ 门是通用的. 计算这个变换，并说明如何用它结合单量子比特运算，获得受控非门.

最终，采用足够先进的技术，或许可以放置、控制和测量半导体中的单核自旋，使下述计划成为可能. 假想可以把单个磷原子(核自旋 1/2)精确地放置到硅(核自旋 0)晶片中，位于光刻的静电门以下. 这些门允许对围绕磷掺杂剂的电子云进行操作，通过调整磷核得到的磁场，实现单量子比特运算. 在分隔磷掺杂剂区域上方的其他门，可用于人为制造，非常类似于化学键的连接临近磷的电子分布，进而允许进行双量子比特运算. 尽管这个方案在工艺上面临巨大的挑战，例如，门的间隔在 100×10^{-10} m 以内，而磷掺杂剂必须被准确定位为有序阵列，但至少这个计划为量子计算和较传统计算技术的结合给出了一条可能的途径.

在我们描述的量子计算机的实现方案中，引起最多注意的是基于固态技术的方案. 当然，人们还在提出原子、分子和光学量子计算机的方案，使用诸如光频点阵(交叉光束约束下，从原子制造的人工晶体)和 Bose 冷凝物等领域前沿的系统，将来我们或许甚至会看到用介子、夸克、胶子或者甚至是黑洞的量子计算计划. 设想某种固态量子计算机的目的是多方面的. 据估计自从 20 世纪 40 年代后期晶体管发明以来，硅技术的投资已超过 1 万亿美元. 凝聚态物质系统在新的物理学中有很多例子，如超导性，量子 Hall 效应，Coulomb 阻碍(在人们普遍认为对经典物理学已完全了解之后的很长时间后，发现的一个经典效应).

本章主要集中在量子计算机的实现上，但所给出的基本元素对量子的许多其他应用也是有用的. 量子密码系统及其实验实现在 12.6 节描述. 量子隐形传态和超密编码的实验结果的参考资料在本章末的“历史和进一步阅读的材料”中给出. 量子通信和量子计算之间的一般接口，包括如分布式量子计算的挑战，这类系统的新算法和新的实验实现，无疑将继续成为未来一个内容丰富的研究领域.

量子计算和通信装置的许多吸引人的地方，自然在于它们作为信息技术的经济前景. 但如我们在本章看到的，量子计算与量子信息也提出关于物理系统的新问题，并为理解物理系统提供了不同的视角. 这些新思想体现了一种从传统的多体、统计和热力学研究物理系统的角度走出来的需要，不论是对原子还是凝聚态物质系统的研究，它们代表在单个量子水平上关注物理系统动态性质的新的机会. 我们希望通过说明这类方法的丰富性，可以促使读者以算法方式看待物理学.

问题 7.1(有效时间标记) 你能构造一个有效线路(要求 $O(\mathrm{poly}(n))$ 个门)循

环置换 $2^n \times 2^n$ 对角密度矩阵的除 $|0^n\rangle\langle 0^n|$ 项的所有对角元吗？

问题 7.2(用线性光学进行计算)　用单光子进行量子计算时，设代替 7.4.1 节双轨表示的是状态的一元表示，其中 $|00\ldots01\rangle$ 为 0，$|00\ldots010\rangle$ 是 1，$|00\ldots0100\rangle$ 是 2，直到 $|10\ldots0\rangle$ 为 2^n-1.

(1) 证明这些状态上的任意酉变换，可以只用分束器和移相器(没有非线性介质)构造.

(2) 构造一个分束器和移相器构成的线路，完成单量子比特的 Deutsch-Jozsa 算法.

(3) 构造一个分束器和移相器构成的线路，完成双量子比特搜索算法.

(4) 证明一般地，任意酉变换需要指数个(对 n)元件实现.

问题 7.3(基于 Jaynes-Cummings 相互作用的控制)　通过外部的经典自由度对小型量子系统的鲁棒和精确的控制对量子计算非常重要. 在不引起原子叠加状态太严重的退相干前提下，通过光脉冲来控制原子状态是相当引人瞩目的. 在本问题中，我们来考察为此需要什么样的近似处理. 从与单模电磁场耦合的单个原子的 Jaynes-Cummings Hamilton 量

$$H = a^{\dagger}\sigma_{-} + a\sigma_{-} \tag{7.175}$$

开始，其中 $\sigma_{\perp}$ 作用在原子上，而 $a, a^{\dagger}$ 作用在场上.

(1) 对 $U=\mathrm{e}^{\mathrm{i}\theta H}$，计算

$$A_n = \langle n \mid U \mid \alpha \rangle \tag{7.176}$$

其中 $|\alpha\rangle$ 和 $|n\rangle$ 分别是相容状态和场的数本征态，A_n 是原子状态上的一个算子，应能得到

$$A_n = \mathrm{e}^{-|\alpha|^2/2}\frac{|\alpha|^2}{n!}\begin{bmatrix} \cos(\theta\sqrt{n}) & \dfrac{\mathrm{i}\sqrt{n}}{\alpha}\sin(\theta\sqrt{n}) \\ \dfrac{\mathrm{i}\alpha}{\sqrt{n+1}}\sin(\theta\sqrt{n+1}) & \cos(\theta\sqrt{n+1}) \end{bmatrix} \tag{7.177}$$

练习 7.17 的结果或许会有帮助.

(2) 在 α 大(不失一般性取 α 为实数)时的近似是有用的. 考虑概率分布

$$p_n = \mathrm{e}^{-x}\frac{x^n}{n!} \tag{7.178}$$

其有均值 $\langle n\rangle = x$ 和标准差 $\sqrt{\langle n^2\rangle - \langle n\rangle^2} = \sqrt{x}$. 把变量换为 $n = x - L\sqrt{x}$，并用 Stirling 近似公式

$$n! \approx \sqrt{2\pi n}n^n\mathrm{e}^{-n} \tag{7.179}$$

导出

$$p_L \approx \frac{\mathrm{e}^{-L^2/2}}{\sqrt{2\pi}} \tag{7.180}$$

(3) 最重要的项是 $n=|\alpha|^2$ 时的 A_n. 定义 $n=a^2+L\alpha$,对

$$a=y\sqrt{\frac{1}{y^2}+\frac{L}{y}},b=y\sqrt{\frac{1}{y^2}+\frac{L}{y}+1} \tag{7.181}$$

其中 $y=1/\alpha$,证明

$$A_L\approx\frac{e^{-L^2/4}}{(2\pi)^{1/4}}\begin{bmatrix}\cos a\varphi & ia\sin a\varphi\\ (i/b)\sin b\varphi & \cos b\varphi\end{bmatrix} \tag{7.182}$$

这里 $\theta=\varphi/\alpha$. 再验证所期望的

$$\int_{-\infty}^{\infty}A_L^{\dagger}A_L\mathrm{d}L=I \tag{7.183}$$

(4) 对原子的理想酉变换为

$$U=\begin{bmatrix}\cos\alpha\theta & i\sin\alpha\theta\\ i\sin\alpha\theta & \cos\alpha\theta\end{bmatrix} \tag{7.184}$$

A_L 与 U 差多少? 尝试估计作为 y Taylor 级数的保真度

$$F=\min_{|\psi\rangle}\int_{-\infty}^{\infty}|\langle\psi|U^{\dagger}A_L|\psi\rangle|^2\mathrm{d}L \tag{7.185}$$

问题 7.4(具有双能级原子的离子阱逻辑) 7.6.3 节描述的受控非门,为简单起见采用了一个三能级原子. 本问题将说明借助更复杂的办法,不用这个三能级也是有可能的. 令 $\gamma_n^{\mathrm{blue},j}(\theta)$ 表示,蓝边带频率 $\omega=\Omega+\omega_z$ 的光脉冲照到第 j 个粒子上 $\theta\sqrt{N}/\eta\Omega$ 时间所完成的运算,类似对红边带也可定义. $\hat{n}$ 表示在 $\hat{x}-\hat{y}$ 平面中的旋转轴,由入射光相位的设置来控制. 当考虑的粒子清楚时,上标 j 可忽略. 特别地,

$$\gamma_n^{\mathrm{blue}}(\theta)=\exp\left[\left(e^{i\varphi}|00\rangle\langle 11|+e^{-i\varphi}|11\rangle\langle 00|+e^{i\varphi}\sqrt{2}|01\rangle\langle 12|+e^{-i\varphi}\sqrt{2}|12\rangle\langle 01|+\cdots\right)\frac{i\theta}{2}\right] \tag{7.186}$$

其中 $\hat{n}=\hat{x}\cos\varphi+\hat{y}\sin\varphi$,右矢中的两个标号,从左到右分别表示内部和运动状态,$\sqrt{2}$因子来源于对 Bose 态有 $a^{\dagger}|n\rangle=\sqrt{n+1}|n+1\rangle$.

(1) 证明当运动状态初始为 $|0\rangle$ 时,$S^j=\gamma_y^{\mathrm{red},j}(\pi)$ 完成离子 j 的内部和运动状态的互换.

(2) 求 θ 值,使得 $\gamma_n^{\mathrm{blue}}(\theta)$ 作用在由 $|00\rangle$,$|01\rangle$,$|10\rangle$ 和 $|11\rangle$ 张成的计算子空间的任意状态上,使其仍在该子空间,要求对任意轴 $\hat{n}$ 成立.

(3) 证明如果 $\gamma_n^{\mathrm{blue}}(\varphi)$ 停留在计算子空间中,那么 $U=\gamma_o^{\mathrm{blue}}(-\beta)\gamma_n^{\mathrm{blue}}(\theta)\gamma_o^{\mathrm{blue}}(\beta)$ 对任意选取的转角 β 和轴 α 也停留在该计算子空间中.

(4) 求 α 和 β 的值使 U 为对角的. 特别地,得到非常有用的如下算子

$$\begin{bmatrix}e^{-i\pi/\sqrt{2}} & 0 & 0 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & e^{i\pi/\sqrt{2}}\end{bmatrix} \tag{7.187}$$

(5) 证明式(7.187)描述了一个非平凡的门，从它和单量子比特运算，可以构造两个离子的内部状态间的受控非门. 你能够想出一串脉冲序列进行 CNOT 运算而不要求运动状态初始化为|0⟩吗?

第 7 章总结　量子计算机：物理实现

- 实现量子计算的四项基本要求：(1)量子比特的表示；(2)可控的酉演化；(3)初始量子比特状态的制备，(4)最终量子比特状态的测量.
- 单光子可作为量子比特好的选择，使用|01⟩和|10⟩作为逻辑 0 和 1，但允许单光子相互作用的传统非线性光学材料，不可避免地会吸收或散射光子.
- C-QED 是使单个原子和单个光子发生很强的相互作用的一项技术，它提供了一种用一个原子调节单光子间相互作用的机制.
- 离子阱可以冷却到其电子和核自旋状态能够用激光脉冲控制的程度，通过用质心声子耦合自旋状态，可以实现不同离子间的逻辑门运算.
- 核自旋是近乎理想的量子比特，并且只要其自旋状态可以被控制和测量，单分子将是近乎理想的量子计算机. 核磁共振用大量分子的系综，使得这在室温下成为可能，不过代价是制备过程的不理想带来的信号损失.

历史和进一步阅读的材料

为什么很难建造量子计算机? 请参考 DiVincenzo[DiV95a]的文章，他给出了满意的回答，图 7.1 是根据这篇文章绘制的. DiVincenzo 还给出了实现量子计算机的五条准则，与 7.2 节讨论的原则类似.

7.3 节的量子简单谐振子是量子力学的基本问题，在任何标准的教科书中都可找到，如文献[Sak95]. Lloyd[Llo94]讨论了 7.3.3 节中给出的量子计算的一般性的充要条件.

7.4 节的光学量子计算机以量子光学体系为主要理论工具，可以在许多教科书中找到，文献[Luo73, Gar91]是其中非常出色的两本. 为更多了解基本的光学和光技术，例如起偏器、分束器、光子探测器等，可参考教材如[ST91]. Campos、Saleh 和 Tiech[CST89]研究了单光子区域的分束器. 和本章内容有关的 $SU(2)$与两个耦合的谐振子之间的联系，首先由 Schwinger[Sak95]描述. 量子比特的双轨表示的概念是 Yurke 提出的，并被 Chuang 和 Yamamoto[CY95]用于描述进行 Deutsch-Jozsa 算法(如练习 7.13)的一台完整的计算机(使用非线性 Kerr 介质). 量子-光学 Fredkin 门是 Yamamoto、Kitagawa、Igeta[YKI88]和 Milburn[Mil89a]首先给出的. Imamoglu 和 Yamamoto[IY94]以及 Kwiat、Steinberg、Chiao、Eberhard 与 Petroff[KSC+94]讨论了光

学量子计算机需要的单光子产生和探测技术. Kitagawa 和 Ueda[KU91]讨论了类似的用 Coulomb 相互作用代替 Kerr 相互作用以及一个采用电光学的机制. Watanabe 和 Yamamoto[WY90]研究了经典的失谐非线性光学材料在单量子水平上的根本局限性. Cerf、Adami 和 Kwiat 研究了用(指数多的)线性光学元件进行的量子逻辑的仿真[CAK98]. Reck、Zeilinger、Bernstein 和 Bertaini 的早期很有影响的论文[RZBB94]描述了类似的结构,但没有明确地与量子计算联系起来. Kwiat、Mitchell、Schwindt 和 White 曾用线性光学器件构造出 Grover 算法的光学仿真过程,但当规模增大时需要指数多的资源[KMSW99]. 关于不同距离上的光通信能量的讨论可参考 Miller[Mil98].

Allen 和 Eberly[AE75]曾写过一本关于双能级原子和光学共振非常好的书. 7.5.4节描述的实验由 Turchette、Hood、Lang、Mabuchi 和 Kimble 在 Caltech 于 1995 年完成[THL+95],Turchette 的博士论文[Tur97]还给出了详细的描述,该实验中用的单光子称为飞行量子比特. 原子态用作量子比特,而原子通过光学腔的不同方法是 Domokos、Raimond、Brune 和 Haroche[DRBH95]提出的,它是基于 Davidovich、Mali、Brune、Raimond 和 Haroche 给出的,用单个原子把相干态切换到腔中的思想[DRBH87,DMB+93].

离子阱量子计算的思想是 Cirac 和 Zoller 提出的[CZ95],7.6.1 节关于这个思想的讨论也从 Steane[Ste97]以及 Wineland、Monroe、Itano、Leibfried、King 和 Meekof[WMI+98]的文章收益很多. Earnshow 定理可以从 Laplace 方程推导出来,如他的原始论文[Ear42],也可参考现代电磁学教材如 Rmo、Whinnery 和 van Duzer 的[RWvD84]. 图 7.8 是参考文献[Ste97]的图 6 绘制的. 图 7.7 参考了文献[WMI+98]. 7.6.4 节的实验是 Monroe、Meekhof、Koing、Itano 和 Wineland 在 Boulder,Colorado 的美国国家标准技术研究所(NIST)完成的[MMK+95]. 图 7.15 的复制得到 Wineland 的允许[WMI+98]. Brewer、DeVoe 和 Kallenbach 展望了用大型平面微离子阱阵列作为规模可行的量子计算机的方案,这正是图 7.12 所示的那类离子阱. James 深入研究了离子阱中的加热和其他退相干机制[Jam98]. Plenio 和 Knight 也在一定程度上研究了离子阱量通信中退相干的影响,他们还考虑了如双能级近似失效的效应[PK98].

DiVincenzo 首先建议在量子计算中使用核自旋[Div95b],并指出熟知的非常古老的 ENDOR(电子核子双共振)脉冲序列实质上是受控非门的一个实例. 不过,如何在室温下用核子的系综进行量子计算的问题,直到 Cory、Fahmy 和 Havel[CFH97]以及 Gershenfeld 和 Chuang[GC97]意识到能够制备有效纯态,才得以解决. 也有必要认识到量子算法可以修改来允许系综输出的读取,这个问题的解决由文献[GC97]提出,并在 7.7.3 节给出. 关于 NMR 的优秀教科书有 Ernst、Bodenhausen 和 Wokaun 的[EBW87]和 Slichter 的[Sli96]. Warren 曾写了一篇批评 NMR 量子计

算的文章[War97]，有趣的是，在同一文章中，他鼓吹使用电子自旋共振(ESR)来做量子计算. 时间标记是 Knill、Chuang 和 Laflamme[KCL98] 提出的. Chuang、Gershenfeld、Kubinec 和 Leung 讨论了7.7.4节的 NMR 逻辑门，和 Bell 态制备线路[CGKL98]. 7.7.4节 Grover 算法的实现是 Chuang、Gershenfeld 和 Kubinec[CGK98] 给出的，图7.20取自他们的文章. Linden、Kupce 和 Freeman 注意到互换门可能是量子计算对 NMR 的一项有用的贡献，并为它设计了脉冲序列[LKF99]. 图 7.18 的显示逻辑标记的三自旋数据取自 Vandersypen、Yannoni、Sherwood 和 Chuang 的文章[VYSC99]. Yamaguchi 和 Yamamoto 创造性地将 NMR 的思想推广到使用晶格[YY99]. 图 7.21 所示分子属于 (1) Chuang、Vandersypen、Zhou、Leung 和 Lloyd[CVZL98]，(2)Cory、Mass、Price、Knill、Laflamme、Zurek 和 Havel[CMP+98]，(3)Somroo、Tseng、Havel、Laflamme 和 Cory[STH+99]，(4)Vandersypen、Yannoni、Sherwood 和 Chuang[VYSC99]，(5)Nielsen、Knill 和 Laflamme[NKL98]，(6)Leung、Vandersypen、Zhou、Sherwood、Yannoni、Kubinec 和 Chuang[LVZ+99]. Jones、Mosca 和 Hansen 也在小分子上实现了不同的量子算法[JM98,JMH98]. 达到熵极限的最优标记方案是 Schulman 和 Vazirani[SV99]设计的.

对 NMR 方法用于量子信息处理的各种批评已经平息. Schack 和 Caves[SC99] 或许是最全面的讨论，它是根据 Braunstein、Caves、Jozsa、Linden、Popescu 和 Schack[BCJ+99]较早的工作. 这项工作的主要技术性结论由 Vidal 和 Tarrach[Vid99]以及 Zyczkowski、Horodecki、Sanpera 和 Lewenstein[ZHSL98]得到，另外可参考 Linden 和 Popescu 的讨论[LP99].

量子计算机的实现方案太多了，不可能在此一一提及. 故只选了几种，引用文献的参考文献是更多文章的一个好的索引. Lloyd 曾展望了量子计算机的许多实现，包括聚合物系统[Llo93]. Nakamura、Pashkin 和 Tsai 曾展示单个 Cooper 对量子比特的控制和 Rabi 振荡的观测[NPT99]. Mooij、Orlando、Levitov、Tian、van der Waal 和 Lloyd 研究了用超导通量表示量子比特[MOL+99]. Platzman 和 Dykman 创造性地提出，用束缚在液氦表面的电子表示量子比特[PD99]. 7.8 节的基于自旋的量子点量子比特实现是 Loss 和 DiVincenzo[LD98]提出的，练习 7.52 属于他们. Huibers、Switkes、Marcus、Campman 和 Gossard 的文章是，量子点的相干时间方面的一个很好的起点[HSM+98]. Imamoglu、Awschalom、Burkard、DiVincenzo、Loss、Sherwin 和 Small 曾提出，以 C QED 技术控制下的量子点中电子自旋实现量子计算机[IAB+99]. 磷为掺杂剂的基于硅的核自旋量子计算机是 Kane 提出的[Kan98]. Vrijin、Yablonovitch、Wang、Jiang、Balandin、Roychowdhury、Mor 和 DiVincenzo[VYW+99]推广到，使用掩埋在硅锗异质结结构中的电子自旋. 最后，Brennen、Caves、Jessen 和 Deutsch[BCJD99]提出了，用束缚于远失谐光频点阵中的中性原子实现量子计算.

量子隐形传态已经用单光子和核自旋作为量子比特在实验中实现，如第 1 章末的“历史和进一步阅读的材料”所描述的. 这些实现中，Furusawa、Sorensen、Braunstein、Fuchs、Kimble 和 Polzik[FSB+98]的实现，也是本章内容中值得特别注意的. 因为它没有采用量子信息的有限 Hilbert 空间表示(如量子比特)，而是使用无穷维 Hilbert 空间，其中连续变量(如位置和动量，如 7.3.2 节)对量子状态进行参数化. 这种隐形传态的方法最初是 Vaidman[Vai94]提出的，随后被 Braunstein 和 Kimble[BK98a]发展. 连续变量表示还被 Braunstein 和 Kimble[BK99]推广到超密编码，并独立地被 Braunstein[Bra98]和 Lloyd 与 Slotine[LS98]推广到量子纠错，被 Lloyd 和 Braunstein[LB99]推广到计算.

APPENDIX A

附 录 A

概率论基础

这里收录了概率论的一些基本定义和结果. 我们假定读者对这些内容已有所了解,对这些结果不熟悉的读者,应该如练习建议的那样,花时间去证明它们.

随机变量(random variable)是概率论最基本的概念. 一个随机变量 X 以概率 $p(X=x)$ 取若干值中的一个值 x,我们用大写字母表示随机变量,用小写字母 x 表示随机变量的取值. 我们还常用记号 $p(x)$ 代替 $p(X=x)$,而不把"$X=$"显式写出. 本书只研究取有限个值的随机变量,并且总是假设这一点成立. 有时为了方便,要考虑取向量值的随机变量,例如在集合 (i,j) 中,$i=1,\cdots,m_1$,$j=1,\cdots,m_1$.

给定 $X=x$ 条件下,$Y=y$ 的条件概率(conditional probability)定义为

$$p(Y=y \mid X=x)=\frac{p(X=x,Y=y)}{p(X=x)} \tag{A.1}$$

其中 $p(X=x,Y=y)$ 是 $X=x$ 和 $Y=y$ 的概率. 当 $p(X=x)=0$ 时,我们约定 $p(Y=y|X=x)=0$. 我们常采用记号 $p(y|x)$,而不写出"$Y=$"和"$X=$". 如果 $p(X=x,Y=y)=p(X=x)p(Y=y)$ 对所有的 x 和 y 成立. 随机变量 X 和 Y 称为独立(indenpdendent). 注意当 X 和 Y 独立时,对所有的 x 和 y 有 $p(y|x)=p(y)$.

Bayes 律把给定 X 下 Y 的条件概率和给定 Y 下 X 的条件概率联系起来

$$p(x \mid y)=p(y \mid x)\frac{p(x)}{p(y)} \tag{A.2}$$

这里出现的概率 $p(y)$,常被下面讨论的全概率公式重新表达.

练习 A.1 证明 Bayes 律.

全概率公式是概率论中最常用的结果之一. 它的内容是:如果 X 和 Y 是两个随机变量,那么 Y 的概率,可以用 X 的概率以及 X 下的 Y 的条件概率表示

$$p(y)=\sum_x p(y \mid x)p(x) \tag{A.3}$$

其中求和是对 X 的所有可能取值进行的.

练习 A.2 证明全概率公式.

随机变量 X 的期望(expectation),平均(average) 和均值(mean)定义为

$$\mathrm{E}(X) \equiv \sum_x p(x)x \tag{A.4}$$

其中求和是对 X 的所有可能取值进行的.

练习 A.3 证明存在一个满足 $x \geqslant \mathrm{E}(X)$ 的值 x,使得 $p(x)>0$.

练习 A.4 证明 $\mathrm{E}(X)$ 对 X 是线性的.

练习 A.5 证明对独立的随机变量 X 和 Y 成立

$$\mathrm{E}(XY) = \mathrm{E}(X)\mathrm{E}(Y)$$

随机变量 X 的方差(variance)定义为

$$\mathrm{var}(X) \equiv \mathrm{E}[X-\mathrm{E}(X)]^2 = \mathrm{E}(X^2)-\mathrm{E}(X)^2 \tag{A.5}$$

标准偏差(standard deviation)定义为 $\Delta(X) \equiv \sqrt{\mathrm{var}(X)}$,它是随机变量关于均值分散程度的一个度量. Chebyshev 不等式定量地描述了,在什么意义下标准偏差是随机变量取值分散程度的度量. 该不等式说对任意 $\lambda>0$ 和具有有限方差的随机变量 X,有

$$p(|X-\mathrm{E}(X)| \geqslant \lambda\Delta(X)) \leqslant \frac{1}{\lambda^2} \tag{A.6}$$

因此随 λ 趋于无穷,偏离均值超过 λ 标准偏差的概率将减小.

练习 A.6 证明 Chebyshev 不等式.

本书正文包含概率论的许多其他结果,包括 Chernoff 界(盒子 3.4)Fano 不等式和大数律.

历史和进一步的阅读材料

概率论的好教材很多. 我们特别推荐 Girmmett 和 Stirzaker 写的教材[GS92]可作为概率论和随机过程的许多基本概念的极好入门书. 从更为纯数学的角度看,Williams 的书[Wil91]是现代概率论的优秀引论,该书以鞅的优美理论为重点. 最后,Feller 深入浅出的经典两卷本[Fel68a,Fel68b]是概率论思想非常出色的引论.

APPENDIX B

附 录 B

群 论

在量子计算与量子信息的研究中，群的数学理论应用有若干方面. 第 5 章中求阶，因子分解和求周期算法的推广都是基于隐含子群问题，量子信息中的量子纠错的稳定子框架也是基于初等群论. 附录 D 中描述的数论用到群 Z_n^* 的性质，并且，贯彻全书的量子线路是间接应用 Lie 群的例子. 本附录概述群论的基本内容. 由于群论研究的主题很宽，我们着重在对许多基本概念和重要定义的总结上，而不去作太多的解释.

B.1 基 本 定 义

群$(G,\cdot)$是一个具有二元群乘积运算"$\cdot$"的非空集合 G. 群乘积运算满足如下性质：(封闭性) $g_1\cdot g_2\in G$，对所有 $g_1,g_2\in G$ 成立；(结合律) $(g_1\cdot g_2)\cdot g_3=g_1\cdot(g_2\cdot g_3)\in G$，对所有 $g_1,g_2,g_3\in G$ 成立；(有单位元)存在 $e\in G$，使得 $\forall g\in G, g\cdot e=e\cdot g=g$；(有逆)对所有 $g\in G$，存在 $g^{-1}\in G$ 使得 $g\cdot g^{-1}=e$ 并且 $g^{-1}\cdot g=e$. 我们常省略"$\cdot$"而把 $g_1\cdot g_2$ 写成 g_1g_2. 我们也常说群 G 而不明确指出它的乘积运算，但该运算一定要有定义.

群 G 称为有限，如果 G 元素的个数是有限的. 有限群 G 的阶(order)定义为它包含的元素个数，记作 $|G|$. 如果 $g_1g_2=g_2g_1$ 对所有 $g_1,g_2\in G$ 成立，称群 G 为 Abel 的. 有限 Abel 群的一个简单例子是整数模 n 的加法群 Z_n，其中乘法运算为模和的运算. 容易验证该运算满足封闭性和结合律公理，并且有单位元 0，因为对所有 x，$x+0=x(\mathrm{mod}\ n)$，并且每个 $x\in G$ 都有逆 $n-x$，因为 $x+(n-x)=0(\mathrm{mod}\ n)$.

一个元 $g\in G$ 的阶定义为，使得 g^r(g 自乘 r 次)等于单位元 e 的最小正整数.

H 是群 G 的子群，如果 H 是 G 的子集合，并且在与 G 相同的乘积运算下构成群.

定理 B.1(Lagrange 定理) 如果 H 是有限群 G 的子群，则 $|H|$ 整除 $|G|$.

练习 B.1 证明对有限群的任意元素 g，总存在正整数 r，使得 $g^r=e$. 换言之，这类群的每个元素都有阶.

练习 B.2 证明 Lagrange 定理.

练习 B.3 证明每个元素 $g\in G$ 的阶整除 $|G|$.

如果 g_1 和 g_2 是 G 的元素,那么 g_2 关于 g_1 的共轭就是元素 $g_1^{-1}g_2g_1$. 如果 H 是 G 的子群,那么,如果 $g^{-1}Hg=H$ 对所有 $g\in G$ 成立,它称为正规于群(normal subgroup). 群 G 中一个元 x 的共轭类 G_x 定义为 $G_x\equiv\{g^{-1}xg|g\in G\}$.

练习 B.4 证明若 $y\in G_x$,则 $G_y=G_x$.

练习 B.5 证明若 x 是 Abel 群 G 的元,则 $G_x=\{x\}$.

非 Abel 群的一个有趣例子是,n 量子比特上的 Pauli 群. 对单量子比特,Pauli 群定义为,由所有 Pauli 阵再配上乘积因子 $\pm 1,\pm i$ 组成

$$G_1\equiv\{\pm I,\pm iI,\pm X,\pm iX,\pm Y,\pm iY,\pm Z,\pm iZ\} \tag{B.1}$$

这组矩阵在矩阵乘积下构成群. 读者也许会问为什么不去掉乘积因子 $\pm 1,\pm i$. 原因是为保持 G_1 在乘法下的封闭性,以成为合格的群. n 量子比特上的一般 Pauli 群定义为,由 Pauli 阵的全部 n 重张量积,配以乘积因子 $\pm 1,\pm i$ 组成.

B.1.1 生成元

采用待研究群的生成元,往往可以使群的研究大大简化. 如果 G 的每个元都可以写成 $g_1,\cdots,g_l$ 中若干元素(允许重复)的乘积形式,并记为 $G=\langle g_1,\cdots,g_l\rangle$,称群 G 的一组元 $g_1,\cdots,g_l$ 生成(generate)群 G. 例如,$G_1=\langle X,Z,iI\rangle$,因为 G 的每个元都可写作 X,Z,iI 的乘积. 另一方面,$\langle X\rangle=\{I,X\}$ 是 G_1 的子群,因为并非 G_1 的所有元都可以写成 X 的幂的形式. 用作群生成元的记号 $\langle\cdots\rangle$,可能会与 2.2.5 节引入的观测平均的记号相混淆,不过实际的上下文总是很清楚的.

采用生成元描述群的优点是,它提供群的简洁的描述. 设群 G 的大小为 $|G|$,那么很容易证明,存在一组 $\log(|G|)$ 的元生成 G. 为此,令 $g_1,\cdots,g_l$ 为群 G 的一组元,而 g 是不在 $\langle g_1,\cdots,g_l\rangle$ 中的一个元. 令 $f\in\langle g_1,\cdots,g_l\rangle$,则 $fg\notin\langle g_1,\cdots,g_l\rangle$,因为否则 $g=f^{-1}fg\in\langle g_1,\cdots,g_l\rangle$,导出矛盾. 因此,对每个 $f\in\langle g_1,\cdots,g_l\rangle$ 对,会有一个元 fg,它在 $\langle g_1,\cdots,g_l,g\rangle$ 中而不在 $\langle g_1,\cdots,g_l\rangle$ 中,所以把 g 添加到 $\langle g_1,\cdots,g_l\rangle$ 中会是被生成的群的规模翻倍(甚至增加更多). 于是 G 必然有包含至多 $\log(|G|)$ 个元素的生成元集合.

B.1.2 循环群

循环群(cyclic group)G 有一个元 a,使得任意元 $g\in G$ 都可表为 a^n 形式,其中 n 是某个整数,a 称为 G 的生成元(generator),并且我们写作 $G=\langle a\rangle$. 由 $g\in G$ 生成的一个循环子群 H 指由 $\{e,g,g^2,\cdots,g^{r-1}\}$ 构成的群,其中 r 是 g 的阶,即 $H=\langle g\rangle$.

练习 B.6 证明任意素数阶的群是循环的.

练习 B.7 证明循环群的每个子群都是循环的.

练习 B.8 证明若 $g\in G$ 具有有限阶 r,则当且仅当 $m=n(\mathrm{mod}\ r)$ $g^m=g^n$.

B.1.3 陪集

由 $g\in G$ 确定的群 G 子群 H 的左陪集(left coset)定义为,集合 $gH\equiv\{gh|h\in H\}$,右陪集可类似定义.通常,陪集是左还是右可以从上下文看出.对如 Z_n 的群运算为加法的群,习惯上把子群 H 对 $g\in Z_n$ 的陪集写成 $g+H$ 形式.一个特定的陪集 gH 的元素称为该陪集的代表元.

练习 B.9 陪集定义了元素间的一种等价关系.证明当且仅当存在某个 $h\in H$ 使得 $g_2=g_1h$,则 $g_1,g_2\in G$ 在 G 中属于 H 的同一个陪集.

练习 B.10 G 中有多少 H 的陪集.

B.2 表 示

令 M_n 为 $n\times n$ 复矩阵的集合.一个矩阵群就是在矩阵乘法下,满足群的条件的 M_n 中矩阵的一个集合.我们把这类群中的单位元记作 I.一个群 G 的一个表示 ρ,定义为 G 映射到某个矩阵群的一个保持群乘积的函数.特别地,$g\in G$ 映到 $\rho(g)\in M_n$,使得 $g_1g_2=g_3$ 蕴含 $\rho(g_1)\rho(g_2)=\rho(g_3)$.如果映射是多对一的,就称为同态(homomorphism);如果是一对一的,则称为同构(isomorphism).映入 M_n 的表示 ρ 具有维数 $d_\rho=n$.这里定义的表示也称为矩阵表示,还有更一般的表示,但对我们来说矩阵表示就足够用了.本附录剩下的内容里遇到的所有群 G 都假定为有限群.

B.2.1 等价性与可约性

等价性和可约性(reducibility)是两个重要的概念.矩阵群 $G\subset M_n$ 的特征标(character)是一个由 $\chi(g)=\mathrm{tr}(g)$ 定义的群函数,其中 $g\in G$,$\mathrm{tr}(\cdot)$ 是矩阵上常用的迹函数.它具有如下性质:(1)$\chi(I)=n$,(2)$|\chi(g)|\leqslant n$,(3)$|\chi(g)|=n$ 蕴含 $g=e^{i\theta}I$,(4)χ 在 G 的任意给定共轭类上都是常数,(5)$\chi(g^{-1})=\chi^*(g)$,(6)$\chi(g)$ 对所有的 g 都是代数数(algebraic number).如果两个矩阵群是同构的,它们称为等价,并且同构下的相应元具有相同的特征标.

练习 B.11(特征标) 证明特征标的上述性质.

练习 B.12(酉矩阵群) 酉矩阵群仅由酉矩阵(满足 $U^\dagger U=I$)组成,证明每个矩阵群都等价于某个酉矩阵群.如果一个群的表示仅由酉矩阵构成,我们将该表示称为酉表示.

M_n 中的矩阵群 G 称为是完全可约的，如果它等价于另外一个块对角型的矩阵群 H. 块对角指所有元 $m\in H$，对某个 $m_1\in M_{n_1}$，$m_2\in M_{n_2}$，具有形式 $\mathrm{diag}(m_1, m_2)$. 如果不存在这样的等价，则矩阵群称为不可约. 下面是不可约矩阵群的一条有用性质：

引理 B.2(Schur 引理) 令 $G\subset M_n$ 和 $H\subset M_k$ 是同阶的两个矩阵群，$|G|=|H|$. 如果存在 $k\times n$ 矩阵 S，使得 $Sg_i=h_iS$ 对某个顺序下全体 $g_i\in G$ 和 $h_i\in H$ 成立，那么要么 S 是零矩阵，要么 $n=k$ 并且 S 是一个非奇异方阵.

练习 B.13 证明每个不可约 Abel 矩阵群都是一维的.

练习 B.14 证明如果 ρ 是群 G 的一个不可约表示，则 $|G|/d_\rho$ 是整数.

下面的定理将不可约性与特征标联系起来.

定理 B.3 矩阵群 G 不可约，当且仅当

$$\frac{1}{|G|}\sum_{g\in G}|\chi(g)|^2=1 \tag{B.2}$$

B.2.2 正交性

表示理论的关键定理是下面的定理.

定理 B.4(基本定理) 每个群 G 恰好有 r 个不等价的不可约表示，其中 r 是 G 的共轭类的数目. 并且如果 $\rho^p\in M_{d_p}$ 和 ρ^q 是其中两个，那么矩阵元满足正交关系

$$\sum_{g\in G}[\rho^p(g)]^{-1}_{ij}[\rho^q(g)]_{kl}=\frac{|G|}{d_p}\delta_{pq}\delta_{jk}\delta_{il} \tag{B.3}$$

其中 $\delta_{pq}=1$ 如果 $\rho^p=\rho^q$，否则为 0.

练习 B.15 利用基本定理证明特征标是正交的，即

$$\sum_{i=1}^{r}r_i(\chi_i^p)^*\chi_i^q=|G|\delta_{pq},\quad \sum_{p=1}^{r}(\chi_i^p)^*\chi_j^p=\frac{|G|}{r_i}\delta_{ij} \tag{B.4}$$

其中 p,q 和 δ_{pq} 的含义与定理中相同，χ_i^p 是第 p 个不可约表示的特征标，在 G 的第 i 个共轭类上的取值，而 r_i 是第 i 个共轭类的大小.

练习 B.16 S_3 是三个元的置换群. 设将置换依次排成分别映 123 到：123，231，312，213，132 和 321. 证明 S_3 有两个一维不可约表示，一个是平凡的，另一个是 1，1，1，−1，−1，−1，依次对应于上述六个置换. 再证明存在一个二维不可约表示，具有矩阵

$$\begin{bmatrix}1&0\\0&1\end{bmatrix},\frac{1}{2}\begin{bmatrix}-1&-\sqrt{3}\\\sqrt{3}&-1\end{bmatrix},\frac{1}{2}\begin{bmatrix}-1&\sqrt{3}\\-\sqrt{3}&-1\end{bmatrix}$$

$$\begin{bmatrix}-1&0\\0&1\end{bmatrix},\frac{1}{2}\begin{bmatrix}1&\sqrt{3}\\\sqrt{3}&-1\end{bmatrix},\frac{1}{2}\begin{bmatrix}1&-\sqrt{3}\\-\sqrt{3}&-1\end{bmatrix}, \tag{B.5}$$

验证这些表示是正交的.

B.2.3 正规表示

数 1 是所有群的一个一维矩阵表示,但它是平凡的.一个表示称为忠实(faithful),如果表示的矩阵群与原来的群是同构的.正规表示是任意群按如下方式构造出的一个忠实表示.令 $v=[g_1,g_2,\cdots,g_{|G|}]^T$ 为 G 中元素组成的一个列向量,用元 $g\in G$ 乘以 v 的每个分量对向量的元进行置换,该置换可以用一个通过矩阵相乘作用在 v 上的 $|G|\times|G|$ 矩阵表示.对应于或许不同置换的 $|G|$ 个这样的矩阵,构成矩阵乘积下 G 的一个忠实表示.

练习 B.17 证明正规表示是忠实的.

练习 B.18 证明正规表示的特征标,除了在单位元的表示上为 $\chi(I)=|G|$,对其他元的表示均为 0.

把任意表示分解成不可约表示的张量和,要服从如下定理.

定理 B.5 如果 ρ 是具有特征标 χ 的 G 的任意表示,而 ρ^i 是 G 的不等价的具有特征标 χ^i 的不可约表示,那么 $\rho=\bigoplus_i c_i\rho^i$,其中$\bigoplus$表示直和,$c_i$ 是由

$$c_i=\frac{1}{|G|}\sum_{r=1}^{r}r_r(\chi_r^i)^*\chi_r \tag{B.6}$$

确定的数.

练习 B.19 利用定理 B.5,证明正规表示包含 d_ρ 个不可约表示.于是如果 R 为正规表示,而 $\hat{G}$ 为不等价的不可约表示的集合,那么

$$\chi^R=\sum_{\rho\in\hat{G}}d_\rho\chi^\rho \tag{B.7}$$

练习 B.20 正规表示的特征标,在除包含 G 中单位元 e 的共轭类 i 外为零.证明

$$\sum_{\rho\in\hat{G}}d_\rho\chi^\rho(g)=N\delta_{gr} \tag{B.8}$$

练习 B.21 证明 $\sum_{\rho\in\hat{G}}d_\rho^2=|G|$.

B.3 Fourier 变换

令 G 为 N 阶有限群,f 为把群元素映射为复数的函数.对 G 的 d_ρ 维不可约表示 ρ,我们定义 f 的 Fourier 变换 $\hat{f}$ 为

$$\hat{f}(\rho)\equiv\sqrt{\frac{d_\rho}{N}}\sum_{g\in G}f(g)\rho(g) \tag{B.9}$$

注意对于矩阵表示 ρ，$\hat{f}(\rho)$把矩阵映射为矩阵. 令 $\hat{G}$ 为 G 的不等价的不可约表示的完全集合，我们定义 $\hat{f}$ 的逆 Fourier 变换为

$$f(g)=\frac{1}{\sqrt{N}}\sum_{\rho\in\hat{G}}\sqrt{d_\rho}\,\mathrm{tr}(\hat{f}(\rho)\rho(g^{-1})) \tag{B.10}$$

因为 $\sum_\rho d_\rho^2=N$，f 和 $\hat{f}$ 都可以表为长度为 N 的复向量. 注意上式中的系数要使若 $\hat{G}$ 由酉表示组成，则 Fourier 变换也使酉的.

上述定义可以通过把式(B.9)代入式(B.10)来理解. 我们得到

$$f(g)=\frac{1}{N}\sum_{\rho\in\hat{G}}\sum_{g'\in G}d_\rho f(g')\mathrm{tr}(\rho(g')\rho(g^{-1})) \tag{B.11}$$

$$=\frac{1}{N}\sum_{\rho\in\hat{G}}\sum_{g'\in G}d_\rho f(g')\mathrm{tr}(\rho(g'g^{-1})) \tag{B.12}$$

$$=\frac{1}{N}\sum_{g'\in G}f(g')\sum_{\rho\in\hat{G}}d_\rho\chi^\rho(g'g^{-1}) \tag{B.13}$$

利用式(B.8)，我们可以简化式(B.13)为期望的

$$f(g)=\sum_{g'\in G}f(g')\delta_{g'g} \tag{B.14}$$

练习 B.22 把式(B.10)代入式(B.9)，并证明可得到 $\hat{f}(\rho)$.

练习 B.23 把 Abel 群 G 表示为 $g\in[0,N-1]$，用加法作为群运算，并定义 $\rho_h(g)=\exp[-2\pi igh/N]$作为 g 的表示. 该表示是一维的，于是 $d_\rho=1$. 证明于 G 相关的 Fourier 变换是

$$\hat{f}(h)=\frac{1}{\sqrt{N}}\sum_{g=0}^{N-1}f(g)\mathrm{e}^{-2\pi igh/N},\ f(h)=\frac{1}{\sqrt{N}}\sum_{g=0}^{N-1}\hat{f}(g)\mathrm{e}^{2\pi igh/N} \tag{B.15}$$

练习 B.24 利用练习 B.16 的结果构造 S_3 上的 Fourier 变换，并将其表示为 6×6 的酉阵.

历史和进一步阅读的材料

有许多群论的优秀教材，并且几乎所有代数方面的书都有一章讲群论，这里的讨论从 Lomont 的有限群教材[Lom87]借用了很多内容. Hammermesh 写的[Ham89]是物理学中群论的标准参考书. 群上的 Fourier 变换的讨论并不多见. Diaconis 和 Rockmore 写过一篇关于有效计算群上 Fourier 变换的好文章[DR90]，他们的大部分结果也被收到 Fässler 和 Steifel 的文献[FS92]中. Beth[Bet84]和 Clausen[Cla89]也分别独立地发现了群上的快速 Fourier 变换.

APPENDIX C

附 录 C

Solovay-Kitaev 定理

第 4 章我们证明了，任意酉运算，可以在使用单量子比特与受控非门构成的线路的量子计算机上实现，这类通用性结果的重要性在于，它们保证量子计算表面上不同的模型之间的等价性. 例如，通用性结果可以保证，程序员能够设计出包含四个输入输出量子比特门的量子线路，并可以相信这些门能够用固定数目的受控非门和单量子比特门来模拟.

受控非和单量子比特门的通用性不尽如人意的地方在于，单量子比特门构成一个连续类，而将在下册给出的容错量子计算只适用于门一组离散集合. 幸好在第 4 章，可以用门的一个有限集合(如受控非门、Hadamard 门 H、相位门 S 和 $\pi/8$ 门)，以任意精度近似任意的单量子比特门. 我们还示意性地说明了近似给定的单量子比特门到 $1/\varepsilon$ 精度，仅需要有限集合中 $\Theta(1/\varepsilon)$ 数目的门. 进而，在下册中我们证明受控非、Hadamard、相位和 $\pi/8$ 门可以以容错方式实现.

本附录证明这种近似可以达到较 $\Theta(1/\varepsilon)$ 快得多的收敛速率. Solovay-Kitaev 定理表明，对任意的单量子比特门 U 和给定的 $\varepsilon > 0$，可以以某个固定有限门集合中 $\Theta(\log^c(1/\varepsilon))$ 数目的门近似 U 到 ε 精度，其中 c 是近似等于 2 的小常数. c 的最优值尚属未知，因此我们将给出 c 近似等于 4 时，Solovay-Kitaev 定理的证明. 并在本附录末的问题中概要描述可以把 c 降到接近 2 的方法. 我们还要证明 c 不可能小于 1，而在 1 和 2 之间确定 c 的最优值是一个公开问题.

为明确 Solovay-Kitaev 定理的重要性，设想量子计算机程序员为解某个问题设计了一个使用 $f(n)$ 个门的算法. 假设设计的算法，使用许多不在通常容错的受控非、Hadamard、相位和 $\pi/8$ 范围内的其他门. 以容错方式实现算法需要多少门? 如果整个算法的允许误差为 ε，那么单个门必须达到允许误差 $\varepsilon/f(n)$. 由第 4 章的示意性说明，在算法中使用的每个门，都需要用容错集合中 $\Theta(f(n)/\varepsilon)$ 个门近似，因而总费用为 $\Theta(f(n)^2/\varepsilon)$，随算法需要的门的数目多项式增长. 而根据 Solovay-Kitaev 定理，算法中的每个门可以用容错集合中 $O(\log^c(f(n)/\varepsilon))$ 数量的门，容错算法的总费用为 $O(f(n)\log^c(f(n)/\varepsilon))$，仅比原始算法有对数多项式增长. 对于许

多问题，这种对数多项式费用是相当可以接受的，而非常不希望是第 4 章示意性论证提供的多项式费用.

为更准确叙述 Solovay-Kitaev 定理，需要定义一些名词和术语. 回忆 $SU(2)$ 是行列式为 1 的全体单量子比特酉矩阵的集合. 我们把注意力集中在 $SU(2)$，因为除去一个无关紧要的全局相位因子，所有单量子比特门都可以写成 $SU(2)$ 中元的乘积. 设 $\mathcal{G}$ 是 $SU(2)$ 元的一个有限集合，$\mathcal{G}$ 是代表量子计算机程序员用来模拟所有其他门的基本门的有限集合. 为具体起见，可把 $\mathcal{G}$ 视为包含容错集合 H，S 和 T，加上适当的全局相位，以保证其行列式等于 1. 为方便起见，假设 $\mathcal{G}$ 包含它自身的逆，即如果 $U\in\mathcal{G}$，那么 $U^\dagger\in\mathcal{G}$. 对容错集，这意味着把 $S^\dagger=S^3$ 和 $T^\dagger=T^7$ 添加到集合中，恰好都可由原集合中的门表出. $\mathcal{G}$ 中元的一个长度为 l 的字，就是一个乘积 $g_1g_2\cdots g_l\in\mathcal{G}$，其中对每个 i 都有 $g_i\in\mathcal{G}$. 我们把 $\mathcal{G}_l$ 定义为长度至多为 l 的字的集合，而把 $\langle\mathcal{G}\rangle$ 定义为具有有限长度的字的集合.

我们还需要某种距离的概念，来量化近似酉矩阵的含义. 具体采用哪种测度并不太重要. 对我们而言，使用下册中的迹距离(trace distance)，$D(U,V)\equiv \mathrm{tr}|U-V|$，是方便的，其中 $|X|\equiv\sqrt{X^\dagger X}$. 事实上，这个定义与下册中的定义差一个因子 2. 采用不同的归一化因子的原因是，如所要展示的(把 $SU(2)$ 的元视为空间的点很有帮助)，这样更容易表达 Solovay-Kitaev 定理的几何直观含义. $SU(2)$ 的子集 S 称为在 $SU(2)$ 中稠密，如果对任意的 $U\in SU(2)$ 和 $\varepsilon>0$，总存在一个元 $s\in S$ 使得 $D(s,U)<\varepsilon$. 设 S 和 W 是 $SU(2)$ 的子集，如果 W 中的每个点与 S 中某个点的距离在 ε 之内，那么 S 称为是 W 的一个 ε 网，其中 $\varepsilon>0$. 我们的兴趣在于随 l 增加，$\mathcal{G}_l$ "填充" $SU(2)$ 的速度有多快. 即对多大的 ε，$\mathcal{G}_l$ 是 $SU(2)$ 的 ε 网? Solovay-Kitaev 定理断言其实随 l 增加，ε 减小的速度很快.

练习 C.1 第 4 章中我们用了距离测度 $E(U,V)=\max_{|\psi\rangle}\|(U-V)|\psi\rangle\|$，其中最大是对所有纯态 $|\psi\rangle$ 取的. 证明当 U 和 V 是单量子比特旋转时，$U=R_{\hat{n}}(\theta)$，$V=R_{\hat{n}}(\varphi)$，$D(U,V)=2E(U,V)$，因此 Solovay-Kitaev 定理中无论是采用迹距离还是 $E(\cdot,\cdot)$ 并不要紧.

定理 C.1 (Solovay-Kitaev 定理) 令 $\mathcal{G}$ 为 $SU(2)$ 中包含自身逆的一个有限集，使得 $\langle\mathcal{G}\rangle$ 在 $SU(2)$ 中稠密，令 $\varepsilon>0$ 为给定. 那么对 $l=O(\log^c(1/\varepsilon))$，$\mathcal{G}_l$ 是 $SU(2)$ 的一个 ε 网，其中 $c\approx 4$.

如前所述，c 的最优值比 4 小些，但对此情况的证明比较方便. 在问题 3.1 中，我们解释了对更小的 c 值如何修改证明. 证明的第一部分是证明当 l 增加时，$\mathcal{G}_l$ 的点在单位阵的小邻域内变得非常稠密，这是从下面的引理得出的一个结论. 为叙述引理，我们把 S_ε 定义为 $SU(2)$ 中满足 $D(U,I)\leqslant\varepsilon$ 的所有点 U.

引理 C.2 令 $\mathcal{G}$ 为 $SU(2)$ 中包含自身逆的一个有限集，使得 $\langle\mathcal{G}\rangle$ 在 $SU(2)$ 中稠密. 存在独立于 $\mathcal{G}$ 的绝对常数 ε_0，使得对任意 $\varepsilon\leqslant\varepsilon_0$，如果 $\mathcal{G}_l$ 是 S_ε 的 ε^2 网，那么 $\mathcal{G}_{6l}$ 是

$S_{\sqrt{C}\varepsilon^2}$ 的一个 $C\varepsilon^4$ 网，这里 C 是某个常数.

我们很快就要证明引理 C.2，但先来看看它怎样蕴含 Solovay-Kitaev 定理. 证明分两步. 第一步是反复应用引理 C.2，证明随字长 l 增大，原点的邻域会很快被充满. 由于 $\mathcal{G}$ 在 $SU(2)$ 中稠密，可以找到 l_0 使得 $\mathcal{G}_{l_0}$ 是 $SU(2)$，从而也是 S_{ε_0} 的 ε_0^4 网. 将引理 C.2 用于 $\varepsilon=\varepsilon_0$ 和 $l=l_0$，蕴含 $\mathcal{G}_{5l_0}$ 是 $S_{\sqrt{C}\varepsilon_0^{3/2}}$ 的 $C\varepsilon_0^4$ 网. 对 $\varepsilon=\sqrt{C}\varepsilon_0^{3/2}$ 和 $l=5l_0$，再次应用引理 C.2 蕴含 $\mathcal{G}_{25l_0}$ 是 $S_{\sqrt{C}(\sqrt{C}\varepsilon_0^{3/2})^{3/2}}$ 的 $C(\sqrt{C}\varepsilon_0^{3/2})^4$ 网. 将这个过程迭代 k 次，可知 $\mathcal{G}_{5^k l_0}$ 是 $S_{\varepsilon(k)}$ 的 $\varepsilon(k)^2$ 网，其中

$$\varepsilon(k)=\frac{(C\varepsilon_0)^{(3/2)^k}}{C} \tag{C.1}$$

不失一般性，假设 ε_0 取得使 $C\varepsilon_0<1$，于是 $\varepsilon(k)$ 随 k 增加非常快地减小. 同时还需要注意，若 ε_0 选得足够小时，$\varepsilon(k)^2<\varepsilon(k+1)$.

令 U 为 $SU(2)$ 的任意元. 第二步是利用图 C.1 中转换的思想，以 $\mathcal{G}$ 中元素的乘积近似 U. 令 $U_0\in\mathcal{G}_{l_0}$ 是 U 的一个 $\varepsilon(0)^2$ 近似，定义 V 使得 $VU_0=U$，即 $V\equiv UU_0^\dagger$，于是 $D(V,I)=\mathrm{tr}|V-I|=\mathrm{tr}|(U-U_0)U_0^\dagger|=\mathrm{tr}|U-U_0|<\varepsilon(0)^2<\varepsilon(1)$. 根据上述反复迭代，应用引理 C.2 的讨论，可找到 V 的 $\varepsilon(1)^2$ 近似 $U_1\in\mathcal{G}_{5l_0}$. 于是 U_1U_0 是

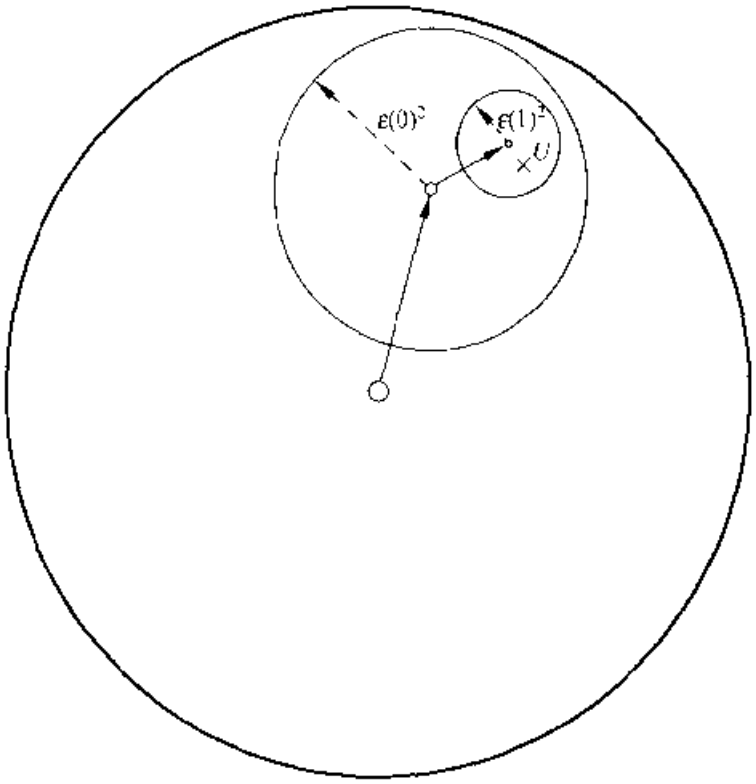


图 C.1　Solovay-Kitaev 定理证明中用到的转换步骤. 为近似任意单量子比特门，我们首先用 $\mathcal{G}$ 中的 l_0 个门近似到 $\varepsilon(0)^2$ 距离. 然后通过增加 $5l_0$ 个门把整体精度提高到好于 $\varepsilon(1)^2$，并如此继续，很快收敛到 U.

U 的一个 $\epsilon(1)^2$ 近似. 定义 V' 使得 $V'U_1U_0=U$，即 $V'\equiv UU_0^\dagger U_1^\dagger$，于是 $D(V',I)=\mathrm{tr}|V'-I|=\mathrm{tr}|(U-U_1U_0)U_0^\dagger U_1^\dagger|=\mathrm{tr}|(U-U_1U_0)|<\epsilon(1)^2<\epsilon(2)$. 迭代应用引理 C.2 可以找到 V' 的 $\epsilon(2)^2$ 近似 $U_2\in \mathcal{G}_5{}^2{}_{l_0}$，并且 $U_2U_1U_0$ 是 U 的 $\epsilon(2)^2$ 近似. 如此进行下去，可构造 $U_k\in \mathcal{G}_5{}^k{}_{l_0}$ 使得 $U_kU_{k-1}\cdots U_r$ 是 U 的 $\epsilon(k)^2$ 近似.

总之，任意门 U 可以用 $l_0+5l_0+\cdots+5^kl_0<\frac{5}{4}5^kl_0$ 个门的序列近似到 $\epsilon(k)^2$ 精度. 为近似到期望的精度 ϵ，我们必须选择 k，使得

$$\epsilon(k)^2<\epsilon \tag{C.2}$$

代入式(C.1)可重写为

$$\left(\frac{3}{2}\right)^k<\frac{\log(1/C^2\epsilon)}{2\log(1/C\epsilon_0)} \tag{C.3}$$

于是为近似到 ϵ 需要的门数量满足($c=\log 5/\log(3/2)\approx 4$)

$$\text{门数量}<\frac{5}{4}5^kl_0=\frac{5}{4}\left(\frac{3}{2}\right)^{kc}l_0<\frac{5}{4}\left(\frac{\log(1/C^2\epsilon)}{2\log(1/C\epsilon_0)}\right)^c l_0 \tag{C.4}$$

即为近似到 ϵ 需要的门数量为 $O(\log^c(1/\epsilon))$，Solovay-Kitaev 定理证明完成.

引理 C.2 的证明用到有关 $SU(2)$ 元乘积的一些基本事实. 现在就来回顾. 引理的关键思想是研究单位矩阵的邻域，从而大大简化了 $SU(2)$ 相当复杂的乘积运算. 更确切地说，设 U 和 V 是 $SU(2)$ 的元，且定义 U 和 V 的群对易式(group commutator)为

$$[U,V]_{\mathrm{gp}}\equiv UVU^\dagger V^\dagger \tag{C.5}$$

设 U 和 V 都接近单位阵，于是可分别写成 $U=\mathrm{e}^{-iA}$ 和 $V=\mathrm{e}^{-iB}$，其中 A 和 B 是对某个小 ϵ 成立 $\mathrm{tr}|A|,\mathrm{tr}|B|\leqslant\epsilon$ 的 Hermite 矩阵. 把 $\mathrm{e}^{\pm iA}$ 和 $\mathrm{e}^{\pm iB}$ 展开到 A 和 B 的二次可得

$$D([U,V]_{\mathrm{gp}},\mathrm{e}^{-[A,B]})=O(\epsilon^3) \tag{C.6}$$

其中 $[A,B]=AB-BA$ 是通常的矩阵对易式(事实上是 $SU(2)$ Lie 代数的对易式). 因此，在单位阵的邻域内，我们可以用简单得多的矩阵对易式代替群对易式的研究.

对量子比特而言，矩阵对易式确实具有特殊的好形式. $SU(2)$ 的任意元素可以对某个实向量 a 写作 $U=u(a)\equiv\exp(-ia\cdot\sigma/2)$. 类似地，对某个实向量 b 成立 $V=u(b)=\exp(-ib\cdot\sigma/2)$. 回忆练习 2.40 有

$$[a\cdot\sigma,b\cdot\sigma]=2i(a\times b)\cdot\sigma \tag{C.7}$$

从式(C.6)我们看到

$$D([U,V]_{\mathrm{gp}},u(a\times b))=O(\epsilon^3) \tag{C.8}$$

现在证明引理 C.2 的思路就很容易理解了. 为完整起见，将与近似有关的大部分细节在后面叙述. 这里只是给出主要思路，如图 C.2 所示. 设我们希望近似

S_U 中的 $U-u(x)$. 练习 C.4 中将看到像 $D(U,I)$ 这样的迹距离等于(准确到一个小的修正量)Euclid 距离 $\|x\|$，于是有很好的近似 $|x\|\leqslant\varepsilon^2$. 我们总是可以选长度至多为 ε 的 y 和 z，使得 $x=y\times z$. 取 y_0 和 z_0，使得 $u(y_0)$ 和 $u(z_0)$ 分别以 ε^2 近似 y 和 z. 应用(C.6)到对易式 $[u(y_0),u(z_0)]_{gp}$，可以得到 U 的一个 $O(\varepsilon^3)$ 近似. 这给出了 S_U 的一个 $O(\varepsilon^3)$ 网. 为完成引理的证明，我们应用类似于 Solovay-Kitaev 定理证明主体中的转换步骤，得到采用 $5l$ 个门的 $S_{O(\varepsilon^2)}$ 任意元素的 $O(\varepsilon^4)$ 近似.

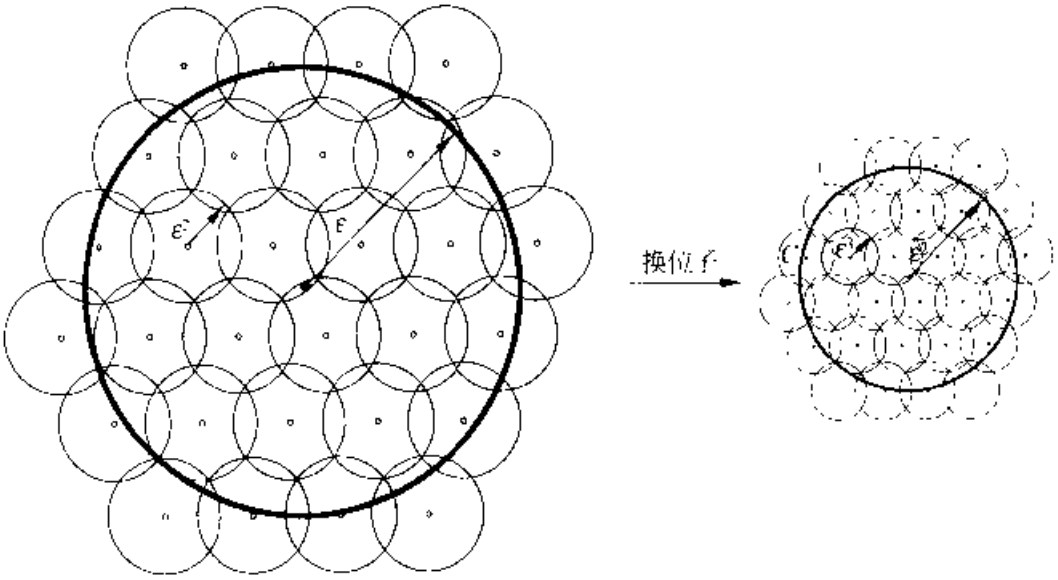


图 C.2 证明引理 C.2 的主要思路. 取 S_ε 中元 U_1 和 U_2 的群换位子可以更紧密地填充 S_{ε^2}. 注意右图中圈的密度应该比画的更大，因为左图中每一对圈都对应右边一圈，图中降低密度只是为了效果的清晰. 通过应用转换步骤(未画出)得到 $S_{5\varepsilon^2}$ 可以完成引理的证明.

练习 C.2 设 A 和 B 是 Hermite 矩阵，满足 $\mathrm{tr}|A|,\mathrm{tr}|B|\leqslant\varepsilon$. 证明对充分小的 ε，存在常数 d，使得

$$D([e^{iA},e^{iB}]_{gp},e^{[A,B]})\leqslant d\varepsilon^3 \tag{C.9}$$

从而证明了式(C.6)(评注：为实用的目的估计 d 的界或许有意义).

练习 C.3 令 x 和 y 是两个任意的实向量，证明

$$D(u(x),u(y))=2\sqrt{2}\sqrt{1-\cos(x/2)\cos(y/2)-\sin(x/2)\sin(y/2)\hat{x}\cdot\hat{y}} \tag{C.10}$$

其中 $x\equiv\|x\|$，$y\equiv\|y\|$，而 $\hat{x}$ 和 $\hat{y}$ 分别是 x 和 y 方向的单位向量.

练习 C.4 证明对 $y=0$ 的情形，$D(u(x),u(y))$ 的公式退化为

$$D(u(x),I))=4\sin\left|\frac{x}{4}\right| \tag{C.11}$$

练习 C.5 证明当 $x,y\leqslant\epsilon$ 时

$$D(u(x),u(y)) = \| x-y \| + O(\epsilon^3) \tag{C.12}$$

证明（引理 C.2）

设 $\mathcal{G}_l$ 是 S_ϵ 的一个 ϵ^2 网. 证明的第一步是，证明存在某个常数 C，使得 $[\mathcal{G}_l,\mathcal{G}_l]_{gp}$ 为是 S_{ϵ^2} 的一个 $C\epsilon^3$ 网.

令 $U\in S_{\epsilon^2}$，并取 x，使 $U=u(x)$. 由练习 C.4 可知 $x\leqslant \epsilon^2+O(\epsilon^6)$. 选择任意一对长度至多为 $\epsilon+O(\epsilon^5)$ 的向量 y 和 z，使得 $x=y\times z$. $\mathcal{G}_l$ 是 S_ϵ 的 ϵ^2 网，故在 $\mathcal{G}_l\cap S_\epsilon$ 中选取 U_1 和 U_2，使得

$$D(U_1,u(y)) < \epsilon^2+O(\epsilon^5) \tag{C.13}$$

$$D(U_2,u(z)) < \epsilon^2+O(\epsilon^5) \tag{C.14}$$

并且令 y_0 和 z_0 满足 $U_1=u(y_0)$ 和 $U_2=u(z_0)$. 由练习 C.4 可知 $y_0,z_0\leqslant\epsilon+O(\epsilon^3)$. 我们的目的是证明 $D(U,[U_1,U_2]_{gp})$ 小于 $C\epsilon^3$，利用三角不等式

$$D(U,[U_1,U_2]_{gp}) \leqslant D(U,u(y_0\times z_0)) + D(u(y_0\times z_0),[U_1,U_2]_{gp}) \tag{C.15}$$

由练习 C.2，第二项至多为 $d'\epsilon^3$，其中因为考虑到 $y_0,z_0<\epsilon+O(\epsilon^3)$ 而不是 $y_0,z_0<\epsilon$ 的可能贡献 d' 是比 d 稍大的常数. 以 $U=u(x)$ 代入，利用引理 C.5，引入适当的常数 d''，并进行简单的代数运算得到

$$\begin{aligned}
D(U,[U_1,U_2]_{gp}) &\leqslant D(u(x),u(y_0\times z_0)) + d'\epsilon^3 && \text{(C.16)}\\
&= \| x-y_0\times z_0 \| + d''\epsilon^3 && \text{(C.17)}\\
&= \| y\times z-y_0\times z_0 \| + d''\epsilon^3 && \text{(C.18)}\\
&= \| [(y-y_0)+y_0]\times[(z-z_0)+z_0] \\
&\quad - y_0\times z_0 \| + d''\epsilon^3 && \text{(C.19)}\\
&\leqslant (d''+2)\epsilon^3+O(\epsilon^4) && \text{(C.20)}\\
&\leqslant C\epsilon^3 && \text{(C.21)}
\end{aligned}$$

其中 C 是适当选取的常数.

引理证明的第二步是应用像 Solovay-Kitaev 定理证明中的转换步骤. 特别地，给定 $U\in S_{\sqrt{C\epsilon^3}}$，可以找到 $\mathcal{G}_l$ 中的元 V 使得 $D(U,V)\leqslant\epsilon^2$，于是 $UV^\dagger\in S_{\epsilon^2}$. 然后在 $\mathcal{G}_l$ 中找到 W_1 和 W_2，使得 $D([W_1,W_2]_{gp},UV^\dagger)\leqslant C\epsilon^3$，因此

$$D([W_1,W_2]_{gp}V,U) \leqslant C\epsilon^3 \tag{C.22}$$

证明完成.

练习 C.6 有固定基本门的集合 $\mathcal{G}$，给出一个对给定的单量子比特酉门描述 U 和期望精度 $\epsilon>0$，有效计算 ϵ 近似 U 的 $\mathcal{G}$ 门序列.

本附录的分析相当粗糙，事实上可以做远为严格的分析. $O(\log^c(1/\epsilon))$ 界中指数 c 的最好值就是一个特别有意思的问题，不难证明 c 不能小于 1. 为此，设想有

$SU(2)$中 N 个半径全为ϵ 的小球，对某个不重要的常数，这些球的体积的数量级为 ϵ^d. 因此，如果这些球要去覆盖 $SU(2)$，N 必须在 $\Omega(1/\epsilon^d)$数量级. 设我们考虑$\mathcal{G}$中所有 g 门序列 $U_1U_2\cdots U_g$，显然这些序列产生至多 $|\mathcal{G}|^g$ 个不同的酉运算. 所以必有 $|\mathcal{G}|^g=\Omega(1/\epsilon^d)$. 这蕴含门数量的期望下界，为

$$g=\Omega\left(\log\left(\frac{1}{\epsilon}\right)\right) \tag{C.23}$$

问题 C.1 下述问题概述为，在 ϵ 范围逼近期望目标需要的门的数量，对任意 $c>2$ 达到界 $O(\log^c(1/\epsilon)\log^c(\log(1/\epsilon)))$的更细致构造过程.

(1) 设对 $0<\delta<\epsilon\leqslant\epsilon_0$ 和充分小的 ϵ_0，N 是 S_ϵ中的一个 δ 网，证明对某个常数 d，$[N,N]_{gp}$是 S_{ϵ^2} 中的一个 $d\delta\epsilon$ 网.

(2) 设对 $0<\delta<\epsilon\leqslant\epsilon_0$，$\mathcal{G}_l$是 S_ϵ中的一个 δ 网. 证明$\mathcal{G}_4{}_l$是 S_{ϵ^4} 中的一个 $d^k\delta\epsilon^{2^k}$ 网.

(3) 设 k 由

$$k\equiv\left\lceil\log\left(\frac{\log(1/\epsilon)}{\log(1/\epsilon_0)}\right)\right\rceil \tag{C.24}$$

定义，并设可以找到 l，使得$\mathcal{G}_l$为 S_{ϵ_0} 中的一个 δ_0 网，其中

$$d^k\delta_0=\epsilon_0 \tag{C.25}$$

证明$\mathcal{G}_4{}^k{}_l$是 $S_{\epsilon_0}^{4^k}$ 中的一个 ϵ 网.

(4) 利用已证明的 Solovay-Kitaev 定理版本，证明取 $l=O(k^c)$对本问题的前面部分是足够的，其中 $c=\log(5)\log(3/2)$是已证明的 Solovay-Kitaev 定理中指数上出现的常数.

(5) 结合前面的结果证明，$SU(2)$中任意门可用 $O(\log^2(1/\epsilon)\log^c(\log(1/\epsilon)))$数量的门 ϵ 近似.

(6) 证明任意的 $c>2$，都可以出现在前面结果的结论中.

问题 C.2 若存在，找出渐近快于前面问题结果的近似过程. 理想情况下，该过程应该 (1)达到近似需要的门数量的下界 $\Omega(\log(1/\epsilon))$，并且 (2)提供构造这样的门序列的有效算法.

问题 C.3 给定单量子比特门的一个可容错执行，并且生成单量子比特门集的稠密子集的有限集合$\mathcal{G}$，例如 $\pi/8$ 和 Hadamard 门. 设计一个简洁，有效并且比较紧凑的方法，对任意给定的单量子比特门和某个 $\epsilon>0$，不考虑全局相位，给出用该容错集中的门序列构成的 U 的 ϵ 近似.

历史和进一步阅读的材料

本附录的结果来源于 Solovay1995 年未发表的手稿，以及 Kitaev 独立的工作，Kitaev 在[Kit97b]中给出了概略的证明. 在同一论文中，Kitaev 注意到这个结果可以

推广到 $SU(2)$ 之 2 外的许多其他 Lie 群. 粗略地说，证明中用到的 $SU(2)$ 的关键性质是 $[S_\epsilon, S_\epsilon] \supseteq S_{\Omega(\epsilon^2)}$，因此这个事实成立的其他 Lie 群也服从某种形式的 Solovay-Kitaev 定理. 例如 Solovay-Kitaev 定理对单位行列式的 $d \times d$ 酉矩阵的 Lie 群 $SU(d)$ 也是对的. 了解到这个结果后，Solovay 随后也对他的证明做了类似的推广. 我们的表示从 1999 年 Freedman 的一次演讲以及与 Freedman、Kitaev 和 Solovay 的讨论中受益很多.

APPENDIX D

附 录 D

数 论

为掌握密码系统以及量子计算机怎样用于破解密码系统，了解一些基本的数论知识是有必要的，本附录就来概述一些数论的基本事实.

D.1 基础知识

我们从基本概念和术语开始. 整数集就是集合$\{\cdots,-2,-1,0,1,2,\cdots\}$，记作$\mathbf{Z}$. 我们偶尔提到自然数，即非负整数，但更多时候直接采用非负整数或正整数的说法，以明确是否包含0的区别.

设n是整数，如果存在整数k使得$n=dk$，整数d整除n(记作$d|n$)，这时d称为n的因子(factor，divisor). 注意1和n总是n的因子. 当d不能整除n时，记作$d\nmid n$. 例如$3|6,3|18$，但$3\nmid 5$，和$3\nmid 7$.

练习 D.1(传递性) 证明若$a|b,b|c$，则$a|c$.

练习 D.2 证明若$d|a,d|b$，则d也整除a和b的线性组合$ax+by$，其中x和y是整数.

练习 D.3 设a和b是正整数，证明若$a|b$则$a\leqslant b$，就此推导如果$a|b$和$b|a$，则$a=b$.

素数(prime number)是大于1且只有1和自身为其因子的整数，前几个素数是$2,3,5,7,11,13,17,\cdots$每个正整数都可惟一地表为素数的乘积. 这或许是关于正整数最重要的一个事实. 这个结果有一个令人印象深刻的名字，算术基本定理(fundamental theorem of arithmatic).

定理 D.1(算术基本定理) 令a为任意大于1的整数，则a具有素因子分解形式

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \tag{D.1}$$

其中$p_1,\cdots,p_n$是互不相同的素数，而$a_1,\cdots,a_n$是正整数. 而且，不计因子顺序，该素因子分解式还是惟一的.

证明 强烈建议从未看到过证明的读者自己来证明它. 如果无法证明,则可在任何一本初等数论教材中找到该证明,参见本附录末的"历史和进一步阅读的材料"提供的参考文献.

对小的整数用尝试法很容易找出其素因子分解,例如 $20=2^2 \cdot 5^1$. 对大数虽然进行过无数的努力,去发现求素因子分解的有效算法,但我们仍未找到经典计算机上这样的算法.

练习 D.4 求 697 和 36300 的素因子分解式.

D.2 模算术与 Euclid 算法

我们都很熟悉普通算术,在了解数的性质时另一种模算术(modular arithmatic)极其有用. 我们假设读者熟悉初等的模算术,因此在讨论更现代的理论之前,只是很快地回顾一下基本概念和术语.

模算术可以理解为余数(remainder)的算术,若用 7 除 18,答案是 2,余 4. 更正式地,对任给的整数 x 和 n,x 总可以(惟一地)写成

$$x = kn + r \tag{D.2}$$

的形式,其中 k 是非负整数,是 x 除以 n 的结果,余数 r 在 0 到 $n-1$(包含这两个数)范围之内. 模算术是只关心余数的普通算术,我们用符号(mod n)表示我们进行的是模算术. 例如,我们有 $2=5=8=11 \pmod 3$,因为 2,5,8 和 11 被 3 除有相同的余数(2). 记号"(mod n)"提醒我们进行的是相对于 n 的模算术.

模算术中加法、乘法和减法运算的定义是显然的,但如何定义除法也许未必显然. 为明白除法是怎样进行的,我们引入数论中另一个关键概念,两个整数的最大公因子(greatest common divisor). a 和 b 的最大公因子是,同时为 a 和 b 因子的整数中最大的一个,记作 $\gcd(a,b)$. 例如,18 和 12 的最大公因子是 6. 为确认这一点的简单办法是,列举 18 的正因子(1,2,3,6,9,18)和 12 的正因子(1,2,3,4,6,12),并取出两个列表中最大的公共元. 对大数而言,这个方法非常没效率和不实用. 幸运的是,求最大公因子有远为有效的办法,称为 Euclid 算法. 下面将对它进行说明.

定理 D.2($\gcd$ 的表示定理) a 和 b 的最大公因子是,能够写成 $ax+by$ 形式的正整数中最小的一个,其中 x 和 y 是整数.

证明 令 $s=ax+by$ 为可以写成这种形式的最小正整数. 因为 $\gcd(a,b)$ 同时是 a 和 b 的因子,故它也是 s 的因子,于是 $\gcd(a,b) \leqslant s$. 我们要通过证明 s 同时是 a 和 b 的因子来说明 $s \leqslant \gcd(a,b)$. 采用反证法. 设 s 不是 a 的因子. 则 $a=ks+r$,其中 r 在 1 到 $s-1$ 范围内. 重写该方程,并利用 $s=ax+by$,可以看到 $r=a(1-kx)+b(-ky)$ 是一个可以写成 a 和 b 线性组合的正整数,并且小于 s. 但这与 s 是

可以写成 a 和 b 线性组合的最小正整数的定义矛盾，因此可知 s 必可整除 a. 由对称性，s 也必然是 b 的因子. 证明完成.

推论 D.3 设 c 可以整除 a 和 b，则 c 可以整除 $\gcd(a,b)$.

证明 由定理 D.2，对某两个整数 x 和 y，有 $\gcd(a,b)=ax+by$. 因为 c 可以整除 a 和 b，它必然整除 $ax+by$.

什么时候一个数 a 在模算术中有乘法逆？即给定 a 和 n，何时存在 b，使得 $ab\equiv 1 \pmod n$？例如，注意 $2\cdot 3\equiv 1 \pmod 5$，于是在模 5 算术中数 2 具有乘法逆 3. 另一方面，尝试法显示 2 没有模 4 的乘法逆. 模算术中求乘法逆，事实上与 gcd 通过互质(co primality)的概念相联系. 整数 a 和 b 称为互质，如果它们的最大公因子是 1. 例如 14 和 9 互质，因为 14 的正因子是 1,2,7 和 14，而 9 的因子是 1,3 和 9. 下述推论刻画了利用互质，给出的模算术中乘法逆的存在性.

推论 D.4 令 n 是大于 1 的整数，一个整数 a 有模 n 的乘法逆，当且仅当 $\gcd(a,n)=1$，即 a 和 n 互质.

证明 设 a 有一个模 n 的乘法逆，记作 a^{-1}，那么对某个整数 k 有 $aa^{-1}=1+kn$，因此 $aa^{-1}+(-k)n=1$. 从定理 D.2 可知 $\gcd(a,n)=1$. 反过来，若 $\gcd(a,n)=1$，则必存在整数 a^{-1} 和 b，使得 $aa^{-1}+bn=1$，因此 $aa^{-1}\equiv 1 \pmod n$.

练习 D.5 对素数 p，证明所有在 1 和 $p-1$ 之间的整数都有模 p 的乘法逆. 1 到 p^n-1 之间，哪些整数具有模 p^n 的乘法逆？

练习 D.6 求 17 模 24 的乘法逆.

练习 D.7 求 $n-1$ 模 n^2 的乘法逆，其中 n 是任意大于 1 的整数.

练习 D.8(逆的惟一性) 设 b 和 b' 是 a 模 n 的乘法逆，证明 $b\equiv b' \pmod n$.

下述定理是求两个正整数最大公因子 Euclid 有效算法的关键.

定理 D.5 令 a 和 b 是整数，并令 r 是 a 除以 b 的余数，那么只要 $r\neq 0$，必有

$$\gcd(a,b)=\gcd(b,r) \tag{D.3}$$

证明 我们通过证明两边相互整除，来证明等式成立，为证左边，整除右边. 注意对某个 k 有 $r=a-kb$. 因为 $\gcd(a,b)$ 整除 a 和 b 以及它们的线性组合，因此 $\gcd(a,b)$ 整除 r. 由推论 D.3，$\gcd(a,b)$ 整除 $\gcd(b,r)$. 为证右边整除左边，注意 $\gcd(b,r)$ 整除 b，且因为 $a=r+kb$ 是 b 和 r 的线性组合，于是 $\gcd(b,r)$ 也整除 a. 由推论 D.3，$\gcd(b,r)$ 整除 $\gcd(a,b)$.

练习 D.9 说明如果 a 和 b 的素因子分解为已知，如何求 $\gcd(a,b)$. 求 6825 和 1430 的素因子分解，并用它们来计算 $\gcd(6825,1430)$.

求两个正整数 a 和 b 的最大公因子的 Euclid 算法工作如下. 首先，对 a 和 b 排序使得 $a\geqslant b$. 用 b 去除 a，得到结果 k_1 和余数 r_1：$a=k_1b+r_1$，有定理 D.5 $\gcd(a,b)=\gcd(b,r_1)$. 接着进行第二次除法，让 b 充当 a，r_1 充当 b：$b=k_2r_1+r_2$. 由定理 D.5，$\gcd(a,b)=\gcd(b,r_1)=\gcd(r_1,r_2)$. 接着，第三次除法，让 r_1 充当 a，r_2 充当

$b, r_1 = k_2 r_2 + r_3$. 由定理 D.5, $\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \gcd(r_2,r_3)$. 如此继续，每次用最近一次的余数除上一次的余数，得到新的结果和余数. 算法在得到的余数为 0，即 $r_m = k_{m+1} r_{m+1}$ 时停止. 我们有 $\gcd(a,b) = \gcd(r_m, r_{m+1}) = r_{m+1}$，于是算法返回 r_{m+1}.

作为例子，我们用 Euclid 算法求 gcd(6825,1430)

$$6825 = 4 \times 1430 + 1105 \tag{D.4}$$

$$1430 = 1 \times 1105 + 325 \tag{D.5}$$

$$1105 = 3 \times 325 + 130 \tag{D.6}$$

$$325 = 2 \times 130 + 65 \tag{D.7}$$

$$130 = 2 \times 65 \tag{D.8}$$

由此可知 gcd(6825,1430)=65.

利用 Euclid 算法，可以有效地求出适合 $ax+by=\gcd(a,b)$ 的整数 x 和 y. 第一阶段是如前所述，运行 Euclid 算法的步骤. 第二阶段从 Euclid 算法倒数第二行开始，涉及到对算法较早行一系列代入，如下面的例子所示

$$65 = 325 - 2 \times 130 \tag{D.9}$$

$$= 325 - 2 \times (1105 - 3 \times 325) = -2 \times 1105 + 7 \times 325 \tag{D.10}$$

$$= -2 \times 1105 + 7 \times (1430 - 1 \times 1105) = 7 \times 1430 - 9 \times 1105 \tag{D.11}$$

$$= 7 \times 1430 - 9 \times (6825 - 4 \times 1430) = -9 \times 6825 + 37 \times 1430 \tag{D.12}$$

即 $65 = 6825 \times (-9) + 1430 \times 37$，为期望的表示.

Euclid 算法消耗怎样的资源？设 a 和 b 都可以表示为至多 L 比特的比特串，显然除数 k_i 或余数 r_i 都不可能长于 L 比特，所以可以假设所有计算是在 L 比特算术中进行. 资源分析中的关键事实是 $r_{i+2} \leqslant r_i/2$，为证明这个事实我们考虑两种情况.

- $r_{i+1} \leqslant r_i/2$. 显然 $r_{i+2} \leqslant r_{i+1}$，命题得证.
- $r_{i+1} > r_i/2$. 在这种情况下 $r_i = 1 \times r_{i+1} + r_{i+2}$，于是 $r_{i+2} = r_i - r_{i+1} \leqslant r_i/2$.

由于 $r_{i+2} \leqslant r_i/2$，故 Euclid 算法核心的辗转相除，至多进行 $2\lceil \log a \rceil = O(L)$ 次，每次辗转相除需要 $O(L^2)$ 个运算，因此 Euclid 算法的总消耗是 $O(L^3)$ 的. 求 x 和 y 使得 $ax+by=\gcd(a,b)$，需要略微增加一点消耗：进行 $O(L)$ 次代入，每次代入涉及 $O(L^2)$ 的算术运算，总费用为 $O(L^3)$.

Euclid 算法还可用于有效计算模算术中的乘法逆，这个过程已包含在推论 D.4 的证明中，现在就明确给出. 设 a 与 n 互质，我们要求模 n 的 a^{-1}. 为此，利用 Euclid 算法以及 a 和 n 的互质性，找出整数 x 和 y 使得

$$ax + ny = 1 \tag{D.13}$$

注意 $ax = (1-ny) = 1 \pmod n$，即 x 是 a 模 n 的乘法逆. 另外，该算法是高效的，只需要 $O(L^3)$ 个步骤，其中 L 是 n 的比特数.

既然我们知道如何有效计算模算术中的乘法逆，求解如下简单的线性方程就不难了.

$$ax + b = c \pmod{n} \tag{D.14}$$

设 a 和 n 互质，那么用 Euclid 算法可以有效求出 a 模 n 的乘法逆 a^{-1}，并且进而求得上述方程的解

$$x = a^{-1}(c-b) \pmod{n} \tag{D.15}$$

被称为中国剩余定理(Chinese remainder theorem)的重要结果，大大扩展了我们能够求解的方程的范围，使我们能够有效求解模算术中的方程组.

定理 D.6(中国剩余定理) 设 $m_1, \cdots, m_n$ 是满足其中任何数对 m_i 和 m_j $(i \neq j)$ 都互质的一组正整数，那么方程组

$$x = a_1 \pmod{m_1} \tag{D.16}$$

$$x = a_2 \pmod{m_2} \tag{D.17}$$

$$\cdots\cdots$$

$$x = a_n \pmod{m_n} \tag{D.18}$$

有解，并且该方程组的两个解模 $M = m_1 m_2 \cdots m_n$ 相等.

证明 采用构造方程组解的方法来证明. 定义 $M_i = M/m_i$，并且注意到 m_i 与 M_i 互质. M_i 模 m_i 有逆，记为 N_i. 定义 $x = \sum a_i M_i N_i$. 为验证 x 是方程组的解，注意 $M_i N_i = 1 \pmod{m_i}$ 以及当 $i \neq j$ 时，$M_i N_i = 0 \pmod{m_j}$，于是 $x = a_i \pmod{m_i}$，从而证明了解的存在性.

设 x 和 x' 都是方程组的解，则对每个 i 都有 $x - x' = 0 \pmod{m_i}$. 于是对每个 i，m_i 都整除 $x - x'$，故 $x = x' \pmod{M}$，如所欲证.

Euclid 算法和中国剩余定理是算法数论中仅有的两个成功故事. 具有讽刺意味的是，它们在引向 RSA 密码系统的一系列想法中扮演重要角色，而 RSA 密码系统所依赖的安全性正是，基于数论中执行某些算法任务的困难性. 我们现在转向了解 RSA 密码系统所需要的数论背景. 关键的思想是经典数论中的一个著名结果，Fermat 小定理—— 不要和 Fermat 最终定理(Fermat last theorm)混淆—— 以及 Euler 对 Fermat 小定理的推广.

引理 D.7 设 p 是素数，且 k 是 1 到 $p-1$ 之间的整数，那么 p 整除 $\binom{p}{k}$.

证明 考虑恒等式

$$p(p-1)\cdots(p-k+1) = \binom{p}{k} k(k-1)\cdots 1 \tag{D.19}$$

因为 $k \geq 1$，左边(从而右边)可以被 p 整除，由于 $k \leq p-1$，项 $k(k-1)\cdots 1$ 不能被 p 整除，于是 $\binom{p}{k}$ 必可被 p 整除.

定理 D.8(Fermat 小定理) 设 p 是素数,而 a 是任意整数,那么 $a^p=a(\mathrm{mod}\ p)$. 如果 a 不能被 p 整除,那么 $a^{p-1}=1(\mathrm{mod}\ p)$.

证明 定理的第二部分可由第一部分推出,因为如果 a 不能被 p 整除,那么 a 具有模 p 的逆,于是 $a^{p-1}=a^{-1}a^p=a^{-1}a=1(\mathrm{mod}\ p)$. 我们对正的 a(a 非正的情况很容易推出)采用归纳法证明定理的第一部分. 当 $a=1$ 时,我们有 $a^p=1=a(\mathrm{mod}\ p)$,如所要求的. 设结果对 a 成立,即 $a^p=a(\mathrm{mod}\ p)$. 考虑 $a+1$ 的情形,由二项式展开,得

$$(1+a)^p=\sum_{k=0}^{p}\binom{p}{k}a^k \tag{D.20}$$

由引理 D.7,只要 $1\leqslant k\leqslant p-1$,就有 p 整除 $\binom{p}{k}$,于是除第一和最后一项外,其他项模 p 的和中都为 0,有 $(1+a)^p=(1+a^p)(\mathrm{mod}\ p)$. 应用归纳假设 $a^p=aa(\mathrm{mod}\ p)$ 可知 $(1+a)^p=(1+a)(\mathrm{mod}\ p)$,如所欲证.

基于 Euler φ 函数,Euler 对 Fermat 小定理作了重要的推广. $\varphi(n)$ 定义为与 n 互质的,小于 n 的正整数的个数. 例如,所有小于素数 p 的正整数都与 p 互质,故 $\varphi(p)=p-1$. 小于 p^n,不与 p^n 互质的整数为 p 的倍数:$p,2p,3p,\cdots,(p^{n-1}-1)p$,故可导出

$$\varphi(p^n)=(p^n-1)-(p^{n-1}-1)=p^{n-1}(p-1) \tag{D.21}$$

进而,如果 a 和 b 互质,那么根据中国剩余定理可证明

$$\varphi(ab)=\varphi(a)\varphi(b) \tag{D.22}$$

为此,考虑方程组 $x=x_a(\mathrm{mod}\ a)$,$x=x_b(\mathrm{mod}\ b)$. 将中国剩余定理用于此方程组可知,满足 $1\leqslant x_a<a$,$1\leqslant x_b<b$,$\gcd(x_a,a)=1$,$\gcd(x_b,b)=1$ 的数对 (x_a,x_b),与满足 $1\leqslant x<ab$,$\gcd(x,ab)=1$ 的整数 x 一一对应. 共有 $\varphi(a)\varphi(b)$ 个数对 (x_a,x_b) 和 $\varphi(ab)$ 个 x,于是可推知(D.22).

式(D.21))和(D.22))合起来,蕴含 $\varphi(n)$ 基于 n 素因子分解 $n=p_1^{a_1}\cdots p_k^{a_k}$ 的公式

$$\varphi(n)=\prod_{j=1}^{k}p_j^{a_j-1}(p_j-1) \tag{D.23}$$

练习 D.10 求 $\varphi(187)$.

练习 D.11 证明

$$n=\sum_{d|n}\varphi(d) \tag{D.24}$$

其中和是在 n 的所有正因子上取的,包括 1 和 n(提示:首先对 $n=p^a$ 证明该结果,然后用 φ(D.22)的乘积性质完成证明).

Fermat 小定理有如下 Euler 给出的漂亮的推广.

定理 D.9 设 a 与 n 互质,那么 $a^{\varphi(n)}=1(\mathrm{mod}\ n)$.

证明 首先用在 α 上的归纳证明 $a^{\varphi(p^\alpha)}=1 \pmod{p^\alpha}$. 对 $\alpha=1$，结果就是 Fermat 小定理. 假设结果对 $\alpha \geqslant 1$ 成立，于是

$$a^{\varphi(p^\alpha)}=1+kp^\alpha \tag{D.25}$$

对某个整数 k 成立. 由式(D.21)

$$a^{\varphi(p^{\alpha+1})}=a^{p^\alpha(p-1)} \tag{D.26}$$

$$=a^{p\varphi(p^\alpha)} \tag{D.27}$$

$$=(1+kp^\alpha)^p \tag{D.28}$$

$$=1+\sum_{j=1}^{p}\binom{p}{j}k^j p^{j\alpha} \tag{D.29}$$

利用引理 D.7，易知 $p^{\alpha+1}$ 整除和中的每一项，故

$$a^{\varphi(p^{\alpha+1})}=1 \pmod{p^{\alpha+1}} \tag{D.30}$$

归纳证明完成. 注意任意的 $n=p_1^{\alpha_1}\cdots p_m^{\alpha_m}$，每个 j，$a^{\varphi(n)}=1 \pmod{p_j^{\alpha_j}}$，因为 $\varphi(n)$ 是 $\varphi(p_j^{\alpha_j})$ 的倍数. 应用中国剩余定理证明中的构造方法，可知方程组 $x=1 \pmod{p_j^{\alpha_j}}$ 的任意解必然满足 $x=1 \pmod{n}$，因此 $a^{\varphi(n)}=1 \pmod{n}$.

记 Z_n^* 为 Z_n 中具有模 n 逆的所有元素的集合，即 Z_n 中与 n 互质的全部元素的集合. 易知 Z_n^* 构成乘积下大小为 $\varphi(n)$ 的群，即它包含乘法单位元，Z_n^* 中元的乘积仍在 Z_n^* 中，以及 Z_n^* 对乘积逆运算封闭(附录 B 给出初等群论的概述). Z_n^* 非显然的结构出现在 n 是奇素数 p 的幂，即 $n=p^\alpha$ 时. 事实上 $Z_{p^\alpha}^*$ 是一个循环(cyclic)群，即 $Z_{p^\alpha}^*$ 中存在一元 g，当任意其他元 x 都可以对某个非负整数 k 写成 $x=g^k \pmod{n}$ 形式时，生成 $Z_{p^\alpha}^*$.

定理 D.10 令 p 为奇素数，α 为正整数，则 $Z_{p^\alpha}^*$ 是循环的.

证明 证明这个事实稍微超出一点本书范围. 可以在许多包含一定量的数论内容的教材中找到，例如可参考 Knuth[Knu98a]第 3.2 节，特别是 16 至 23 页.

练习 D.12 验证 Z_n^* 构成模 n 乘法运算下的大小为 $\varphi(n)$ 的群.

练习 D.13 令 a 为 Z_n^* 的任意元，证明 $S \equiv \{1, a, a^2, \cdots\}$ 构成 Z_n^* 的子群，并且 S 的大小为满足 $a^r=1 \pmod{n}$ 的最小 r 值.

练习 D.14 设 g 是 Z_n^* 的一个生成元，证明 g 的阶必为 $\varphi(n)$.

练习 D.15 Lagrange 定理(定理 B.1)是群论的一个基本结果，它说子群的大小必然整除群的阶. 利用 Lagrange 定理给出定理 D.9 的另一种证明，即证明 $a^{\varphi(n)}=1 \pmod{n}$ 对任意 $a \in Z_n^*$ 成立.

D.3 因子问题向求阶问题的归约

在经典计算机上求数的因子问题事实上等价于另一个问题，求阶问题. 这个等价性很重要，因为事实上量子计算机可以迅速求解求阶问题，从而可以快速求因

子.本节我们说明两个问题的等价性,并着重子从求因子到求阶的归约.

设 N 是一个正整数,x 与 N 互质,$1\leqslant x<N$,x 模 N 的阶定义为使得 $x^r=1 \pmod N$ 的最小正整数 r.求阶问题就是对给定的 x 和 N,确定 r.

练习 D.16 利用定理 D.9,证明 x 模 N 的阶必可整除 $\varphi(N)$.

从求因子到求阶的归约分两步.第一步是证明,如果能够找到方程 $x^2=1 \pmod N$ 的一个非平凡解 $x\neq \pm 1 \pmod N$,那么就可以求出 N 的一个因子.第二步是证明随机选取与 N 互质的 y,那么很有可能具有偶数的阶 r,使得 $y^{r/2}\neq \pm 1 \pmod N$,子是 $x\equiv y^{r/2} \pmod N$ 是方程 $x^2=1 \pmod N$ 的解.

定理 D.11 设 N 为 L 比特长的合数,x 是方程 $x^2=1 \pmod N$ 在 $1\leqslant x\leqslant N$ 范围内的非平凡解,即既不满足 $x=1 \pmod N$ 也不满足 $x=N-1=-1 \pmod N$.那么 $\gcd(x-1,N)$ 和 $\gcd(x+1,N)$ 中至少有一个是 N 的非平凡因子,而且可以用 $O(L^3)$ 次运算得到.

证明 因为 $x^2=1 \pmod N$,N 必整除 $x^2-1=(x+1)(x-1)$,因此 N 必与 $x+1$ 或 $x-1$ 有公因子.但根据 $1<x<N-1$,有 $x-1<x+1<N$,可知该公因子不可能是 N 本身.我们可以利用 Euclid 算法计算 $\gcd(x-1,N)$ 和 $\gcd(x+1,N)$,于是可以用 $O(L^3)$ 次运算获得 N 的一个不平凡因子.

引理 D.12 令 p 为奇素数,令 2^d 为整除 $\varphi(p^\alpha)$ 的 2 的最高次幂,那么 2^d 整除从 $Z_{p^\alpha}^*$ 中随机选取的元模 p^α 的阶的概率精确地为 $\frac{1}{2}$.

证明 注意到 $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$ 为偶数,因为 p 是奇数,于是 $d\geqslant 1$.由定理 D.10,存在 $Z_{p^\alpha}^*$ 的生成子 g,于是任意元可写作 $g^k \pmod{p^\alpha}$ 形式,k 为从 1 到 $\varphi(p^\alpha)$ 的整数.令 r 为 g^k 模 p^α 的阶.考虑两种情况.第一种情况是当 k 为奇数时,从 $g^{kr}=1 \pmod{p^\alpha}$ 时,我们可推知 $\varphi(p^\alpha)\mid kr$,子是 $2^d\mid r$,因为 k 是奇数.第二种情况是当 k 为偶数时,那么

$$g^{k\varphi(p^\alpha)/2}=\left(g^{\varphi(p^\alpha)}\right)^{k/2}=1^{k/2}=1 \pmod{p^\alpha} \tag{D.31}$$

可得 $r\mid \varphi(p^\alpha)/2$,由此可导出 2^d 不能整除 r.

总之,$Z_{p^\alpha}^*$ 可以划分成相同大小的两个集合:可以写成 k 为奇数的 g^k,有 $2^d\mid r$,其中 r 是 g^k 的阶;和可以写成 k 为偶数的 g^k,有 $2^d\nmid r$.因此 2^d 整除从 $Z_{p^\alpha}^*$ 中随机选取的元的阶 r 的概率为 1/2,不整除的概率也为 1/2.

定理 D.13 设 $N=p_1^{\alpha_1}\cdots p_m^{\alpha_m}$ 是正奇合数的素因子分解,令 x 从 Z_N^* 中随机选取,而 r 为 x 模 N 的阶,则

$$p(r \text{ 为偶数且 } x^{r/2}\neq -1 \pmod N)\geqslant 1-\frac{1}{2^m} \tag{D.32}$$

证明 我们证明

$$p(r \text{ 为奇数或 } x^{r/2}=-1 \pmod N)\leqslant \frac{1}{2^m} \tag{D.33}$$

由中国剩余定理，从 Z_N^* 中随机均匀地选取 x，等价于从 $Z_{p_j^{\alpha_j}}^*$ 中独立均匀地选取 x_j，并要求 $x \equiv x_j \pmod{p_j^{\alpha_j}}$ 对每个 j 成立. 令 r_j 为 x_j 模 $p_j^{\alpha_j}$ 的阶，2^{d_j} 为整除 r_j 的 2 的最高次幂，而 2^d 是整除 r 的 2 的最高次幂. 我们将证明为使 r 为奇数或 $x^{r/2} \equiv -1 \pmod{N}$，$d_j$ 必须对所有的 j 取同样的值. 于是命题可从引理 D.12 推出的概率至多为 $\frac{1}{2^m}$ 得到.

我们考虑的第一种情况是 r 为奇数的情形. 易知 $r_j \mid r$ 对每个 j 成立，于是 r_j 是奇数，故对所有 $j=1,\cdots,k, d_j=0$. 第二种情况也是最后一种情况，即当 r 为偶数且 $x^{r/2} \equiv -1 \pmod{N}$，那么 $x^{r/2} \equiv 1 \pmod{N}$，因此 $x^{r/2} \equiv -1 \pmod{p_j^{\alpha_j}}$，故 $r_j \nmid (r/2)$. 因为 $r_j \mid r$，必有 $d_j = d$ 对所有 j 成立.

定理 D.11 和 D.13 一起可给出一个算法，能以高的概率返回任意合数 N 的一个非平凡因子. 除用到的求阶子程序外，算法的其他所有步骤都可在经典计算机上有效地执行. 通过反复使用该算法，我们可以得到 N 的完整素因子分解. 该算法总结如下.

(1) 若 N 是偶数，返回因子 2；

(2) 用练习 5.17 的算法确定是否对整数 $a \geqslant 1$ 和 $b \geqslant 2$ 成立 $N = a^b$，如果是则返回因子 a；

(3) 随机地从 1 到 $N-1$ 中选择 x，如果 $\gcd(x,N) > 1$，则返回因子 $\gcd(x,N)$；

(4) 用求阶子程序找出 x 模 N 的阶 r；

(5) 如果 r 是偶数且 $x^{r/2} \neq -1 \pmod{N}$，那么计算 $\gcd(x^{r/2}-1, N)$ 和 $\gcd(x^{r/2}+1, N)$，并测试哪一个是非平凡因子，返回该因子，否则，算法失败.

算法第 1 步和第 2 步要么返回一个因子，要么 N 是一个有多于一个的素因子的奇数. 这些步骤分别需要 $O(1)$ 和 $O(L^3)$ 次运算. 第 3 步要么返回一个因子，要么随机产生一个 Z_N^* 中的元 x. 第 4 步调用求阶子程序，计算 x 模 N 的阶 r. 第 5 步完成算法，因为定理 D.13 以 1/2 概率保证 r 是偶数且 $x^{r/2} \neq -1 \pmod{N}$，于是定理 D.11 保证要么 $\gcd(x^{r/2}-1, N)$，要么 $\gcd(x^{r/2}+1, N)$ 是 N 的一个非平凡因子.

练习 D.17(求阶向求因子的归约) 我们已经看到有效的求阶算法，可以使我们有效求因子. 证明有效求因子算法，可以让我们有效地求出与 N 互质的任意 x 模 N 的阶.

D.4 连分式

实数的连续统与整数之间有许多重要的联系，其中之一是连分式(continued fraction)的漂亮理论. 本节我们对连分式的一些基本理论进行阐述，这些理论在第 5 章中详细介绍的求阶和求因子快速量子算法中用到.

作为连分式的例子，考虑表达式

$$s \equiv \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cdots}}} \tag{D.34}$$

定义的数 s. 不严格地讲，注意 $s=1/(2+s)$，容易看出 $s=\sqrt{2}-1$. 连分式方法的思想是采用如(D.34)那样的表达式，单用整数来描述实数. 有限单连分式定义为一组正整数 $a_0,\cdots,a_N$

$$[a_0,\cdots,a_N] \equiv a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{+\cdots+\cfrac{1}{a_N}}}} \tag{D.35}$$

该连分式的第 n 个($0\leqslant n\leqslant N$)渐近连分式定义为$[a_0,\cdots,a_n]$.

定理 D.14 设 x 是大于等于 1 的有理数，那么 x 具有连分式表达，$x=[a_0,\cdots,a_N]$，它可由连分式算法求出.

证明 连分式算法最好用例子来掌握. 设我们试图对 31/13 分解连分式，第一步是把 31/13 分成整数和分数部分

$$\frac{31}{13}=2+\frac{5}{13} \tag{D.36}$$

接着把分数部分翻转，得到

$$\frac{31}{13}=2+\cfrac{1}{\cfrac{13}{5}} \tag{D.37}$$

这样的分拆与翻转步骤应用到 13/5，给出

$$\frac{31}{13}=2+\cfrac{1}{2+\cfrac{3}{5}}=2+\cfrac{1}{2+\cfrac{1}{\cfrac{5}{3}}} \tag{D.38}$$

接下来对 5/3 进行分拆与翻转

$$\frac{31}{13}=2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{2}{3}}}=2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{\cfrac{3}{2}}}} \tag{D.39}$$

连分式分解终止，因为 3/2=1+1/2 可以写成带有分子 1 而无需再翻转，从而得到 31/13 的最终连分式表示

$$\frac{31}{13}=2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2}}}} \tag{D.40}$$

显然对任意的有理数经过有限次分拆与翻转连分式算法都会终止，因为出现的分子(例子中是 31,3,2,1)是严格递减的. 终止有多快？我们很快会回到这个问题.

上述定理对 $x\geqslant 1$ 断言；然而，实际上可以放松 a_0 是正数的要求，允许它是任意整数，这使 $x\geqslant 1$ 的要求变为只是表面上的. 特别地，如果 x 在量子算法使用的 0 到 1 的范围内，那么连分式展开具有 $a_0=0$.

连分式算法，为得到给定有理数的连分式展开提供了清晰的算法. 惟一可能的歧义在于最后阶段，因为可能有两种方式分拆整数，或者是 $a_n=a_n$，或者是 $a_n=(a_n-1)+1/1$，导致两种连分式展开. 这种歧义性实际上是有用的，因为它允许我们不失一般性，假定一个给定有理数的连分式展开具有期望的奇数或偶数长度的渐近连分式.

练习 D.18 求 $x=19/17$ 和 $x=77/65$ 的连分式展开.

定理 D.15 令 $a_0,\cdots,a_N$ 为一正数序列，那么

$$[a_0,\cdots,a_n]=\frac{p_n}{q_n} \tag{D.41}$$

其中 p_n 和 q_n 是递归定义的实数：$p_0\equiv a_0$，$q_0\equiv 1$，$p_1\equiv 1+a_0a_1$，$q_1\equiv a_1$，并且对 $2\leqslant n\leqslant N$，有

$$p_n\equiv a_np_{n-1}+p_{n-2} \tag{D.42}$$

$$q_n\equiv a_nq_{n-1}+q_{n-2} \tag{D.43}$$

在 a_j 为正整数时，p_j 和 q_j 也是正整数.

证明 对 n 进行归纳. 对 $n=0,n=1,2$ 的情况容易直接验证. 由定义，对 $n\geqslant 3$，有

$$[a_0,\cdots,a_n]=[a_0,\cdots,a_{n-2},a_{n-1}+1/a_n] \tag{D.44}$$

应用归纳假设，令 $\tilde{p}_j/\tilde{q}_j$ 是与右边的连分式关联的渐近连分式序列

$$[a_0,\cdots,a_{n-2},a_{n-1}+1/a_n]=\frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}} \tag{D.45}$$

显然 $\tilde{p}_{n-3}=p_{n-3}$，$\tilde{p}_{n-2}=p_{n-2}$ 并且 $\tilde{q}_{n-3}=q_{n-3}$，$\tilde{q}_{n-2}=q_{n-2}$，因此

$$\frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}}=\frac{(a_{n-1}+1/a_n)p_{n-2}+p_{n-3}}{(a_{n-1}+1/a_n)q_{n-2}+q_{n-3}} \tag{D.46}$$

$$=\frac{p_{n-1}+p_{n-2}/a_n}{q_{n-1}+q_{n-2}/a_n} \tag{D.47}$$

右边分子分母同乘以 a_n，可得

$$\frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}}=\frac{p_n}{q_n} \tag{D.48}$$

结合式(D.48)，式(D.45)和式(D.44)可知

$$[a_0,\cdots,a_n]=\frac{p_n}{q_n} \tag{D.49}$$

如所欲证.

练习 D.19 证明对 $n\geqslant 1$ 成立 $q_n p_{n-1}-p_n q_{n-1}=(-1)^n$. 利用这个事实证明 $\gcd(p_n,q_n)=1$(提示:对 n 进行归纳).

对有理数 $x=p/q>1$,为获得连分式展开需要多少个 a_n 值?其中 p 和 q 互质. 设 $a_0,\cdots,a_N$ 为正整数,从 p_n 和 q_n 的定义可知 p_n 和 q_n 为递增序列,因此 $p_n=a_n p_{n-1}+p_{n-2}\geqslant 2p_{n-2}$,并且类似地 $q_n\geqslant 2q_{n-2}$,从而 $p_n,q_n\geqslant 2^{\lfloor n/2\rfloor}$. 因此 $2^{\lfloor n/2\rfloor}\leqslant q\leqslant p$,故 $N=O(\log(p))$. 于是如果 $x=p/q$ 是有理数,p 和 q 是 L 比特整数,那么 x 的连分式展开可以用 $O(L^3)$ 次运算得到——$O(L)$ 次分拆与翻转步骤,每个步骤用 $O(L^2)$ 个初等算术门.

定理 D.16 令 x 是有理数,且设 p/q 是有理的,使得

$$\left|\frac{p}{q}-x\right|\leqslant\frac{1}{2q^2} \tag{D.50}$$

那么 p/q 是 x 的一个渐近连分式.

证明 令 $p/q=[a_0,\cdots,a_n]$ 为 p/q 的连分式展开,并按照定理 D.15 方式定义 p_j 和 q_j,使得 $p_n/q_n=p/q$. 由式

$$x\equiv\frac{p_n}{q_n}+\frac{\delta}{2q_n^2} \tag{D.51}$$

定义 δ,因此 $|\delta|<1$. 定义 λ 为

$$\lambda\equiv 2\left(\frac{q_n p_{n-1}-p_n q_{n-1}}{\delta}\right)-\frac{q_{n-1}}{q_n} \tag{D.52}$$

如此定义 λ 的原因是,经过简单的代数运算,可知它满足

$$x=\frac{\lambda p_n+p_{n-1}}{\lambda q_n+q_{n-1}} \tag{D.53}$$

并且有 $x=[a_0,\cdots,a_n,\lambda]$. 选择 n 为偶数,从练习 D.19 可知

$$\lambda=\frac{2}{\delta}-\frac{q_{n-1}}{q_n} \tag{D.54}$$

由 q_n 的递增性可知

$$\lambda=\frac{2}{\delta}-\frac{q_{n-1}}{q_n}>2-1>1 \tag{D.55}$$

因此 λ 是大于 1 的有理数,并且具有有限单连分式 $\lambda=[b_0,\cdots,b_m]$. 于是 $x=[a_0,\cdots,a_n,b_0,\cdots,b_m]$ 是 x 的有限单连分式,而 p/q 为其渐近连分式.

问题 D.1(素数估计) 令 $\pi(n)$ 为小于 n 的素数数目. 很难证明的结果素数定理(prime number theorem)断言,$\lim_{n\to\infty}\pi(n)\log(n)/n=1$,从而 $\pi(n)\approx n/\log(n)$. 本问题给出素数分布的一个相当不错的下界估计,作为素数定理的很粗糙的版本.

(1) 证明 $n\leqslant\log\binom{2n}{n}$.

(2) 证明

$$\log\binom{2n}{n} \leqslant \sum_{p<2n} \left\lfloor \frac{\log(2n)}{\log p} \right\rfloor \log p \tag{D.56}$$

其中求和是对所有小于等于 $2n$ 的素数取的.

(3) 利用前两个结果证明

$$\pi(2n) \geqslant \frac{n}{\log(2n)} \tag{D.57}$$

历史和进一步阅读的材料

有许多关于数论的优秀著作,我们采用了 Koblitz 的书[Kob94]中的不少内容.该书同时包括关于数论、算法和密码学的许多导引材料.类似的综合性组合构成 Cormen、Leiserson 和 Rivest 的文献[CLR90]更面向算法的表述的一小部分,可在该书第 33 章找到.我们关于连分式的讨论基于 Hardy 和 Wright 关于数论的经典教材[HW79]的第 10 章.问题 4.1 取自 Papadimitriou 的文献[Pap94].

APPENDIX E

附 录 E

公钥密码术与 RSA 密码系统

密码术是使双方能够秘密通信的技术. 例如，希望在互联网上购物的顾客，要求只有他们在购买商品的公司能够访问被传送的信用卡号. 更危险的情形是在战时，每个参战方都要求有保密通信的手段. 为实现保密，人们采用密码协议或密码系统. 有效的密码系统让通信方很容易地通信，但第三方很难偷听到对话的内容.

公钥密码系统是特别重要的一类密码系统，图 E.1 给出它的示意图. Alice 设立一个信箱，任何人都可以把信投入，而发信给她，但只有她可以从中取信. 为此信箱有两个门. 一个是顶部被锁住的活门. 任何可以打开活门的人都可以把信放进信箱，不过，从活门到盒子的斜道是单向的，他们无法把信掏出. Alice 免费提供给大家活门的钥匙——称为公钥——因此她绝对可以收到任何人的邮件. 信箱的正面是第二个门，可以取出已经在盒子里的邮件. Alice 拥有该门惟一的钥匙，这称为她自己的私钥. 这种设计——包含两个密钥，一个秘密而另一个公开——使世界上的任何人都可以和 Alice 进行保密通信.



图 E.1 用通俗的说法说明公钥密码系统的关键思想. 许多国家的邮局实质上采用同样的方案.

公钥密码系统按照类似的原则运行. 设 Alice 希望用公钥密码系统接收消息，她必须首先生成两个密钥，一个公开的，记作 P，另一个秘密的记作 S. 这些密钥的准确性质取决于具体的秘密系统，某些密码系统使用简单的对象，如数字作为密钥，而另外一些使用远为复杂的数学对象，如椭圆曲线作为密钥. 一旦 Alice 生成了密钥，她就公布公开密钥，以便让别人都能获得这个密钥.

现在设 Bob 希望给 Alice 送一条秘密消息. 他首先获得 Alice 的公钥 P，然后把他希望发给 Alice 的消息，用 Alice 的公钥加密. 如何进行加密变换的细节，依赖于使用的密码系统的细节. 关键在于为了保证保密性，加密阶段需要很快还原，即使利用先前用于加密的公钥! 这正像邮件的活门 —你无法取回你所投入的，即使你有活门的钥匙. 因为公钥和被加密消息是窃听者惟一可利用的信息，窃听者不太可能恢复消息. 然而 Alice 有窃听者没有的额外信息，私钥 S. 私钥决定第二个变换，这一次是在被加密的消息上. 这个变换称为解密，逆转了加密过程，使 Alice 可以恢复原来的消息.

在理想情况下，这就是公钥密码术的工作过程. 不幸的是，直到本书写作时为止，还不知道是否存在任何这样的安全方案，来实施公钥密码术. 确实存在普遍相信是安全的一些方案，并被广泛用于网络商业等应用场合，但普遍相信并不等于安全性的证明. 这些方案被认为是安全的理由是，人们已经花了很大的力气来寻找破解它们的方法(却没有成功!)，算是一种耐久性的证明. RSA 密码系统是这些公钥系统中应用最广的一类. RSA 得名于发明者 Rivest、Shamir 和 Adleman 名字的首字母. 如将要说明的，RSA 密码系统的安全性基于求因子问题在经典计算机上看起来的困难. 了解 RSA 需要一点数论的背景，已在附录 D 中给出，特别是 D.1 和 D.2 节.

设为使用 RSA 密码系统，Alice 希望建立公钥和私钥. 她采用如下过程.

(1) 选择两个大素数 p 和 q；

(2) 计算乘积 $n=pq$；

(3) 随机选择一个小奇数 e，与 $\varphi(n)=(p-1)(q-1)$ 互质；

(4) 计算 e 模 $\varphi(n)$ 的乘法逆 d；

(5) RSA 公开密钥就是数对 $P=(e,n)$，私钥就是数对 $S=(d,n)$.

设第二方 Bob 希望用公钥 (e,n) 加密消息 M，并发给 Alice. 我们假设消息 M 仅为 $\lfloor \log n \rfloor$ 比特，因为长消息可以通过，把 M 拆成至多 $\lfloor \log n \rfloor$ 比特的块，分别加密. 加密过程是对单块计算

$$E(M) = M^e \pmod{n} \tag{E.1}$$

Bob 向 Alice 发送的 $E(M)$ 是消息 M 的加密版本. Alice 可以简单地通过用她的私钥 $S=(d,n)$，把加密后的消息提高到 d 次幂

$$E(M) \to D(E(M)) = E(M)^d \pmod{n} \tag{E.2}$$

来很快地解密该消息. 为成功解密，我们需要 $D(E(M))=M \pmod{n}$. 为证明这一

点，注意根据构造 $ed=1(\mathrm{mod}\ \varphi(n))$，因此对某个整数 k 有 $ed=1+k\varphi(n)$. 证明考虑两种不同情况. 第一种情况，M 与 n 互质. 由 Euler 形式的 Fermat 小定理的推广，定理 D.9，可知 $M^{k\varphi(n)}=1(\mathrm{mod}\ n)$，于是

$$D(E(M)) = E(M)^d(\mathrm{mod}\ n) \tag{E.3}$$

$$= M^{ed}(\mathrm{mod}\ n) \tag{E.4}$$

$$= M^{1+k\varphi(n)}(\mathrm{mod}\ n) \tag{E.5}$$

$$= M \cdot M^{k\varphi(n)}(\mathrm{mod}\ n) \tag{E.6}$$

$$= M(\mathrm{mod}\ n) \tag{E.7}$$

这就证明了当 M 与 n 互质时，可以成功解密. 下面设 M 不与 n 互质，于是 p 和 q 至少有一个整除 M. 为确定起见，假设只有 p 整除 M，而 q 不能整除 M，其他情况的证明只需要稍作修改. 因为 p 整除 M，我们有 $M=0(\mathrm{mod}\ p)$，故 $M^{ed}=0=M(\mathrm{mod}\ p)$. 因为 q 不能整除 M，根据 Fermat 小定理，我们有 $M^{q-1}=1(\mathrm{mod}\ q)$，于是 $M^{\varphi(n)}=1(\mathrm{mod}\ q)$，因为 $\varphi(n)=(p-1)(q-1)$. 利用 $ed=1+k\varphi(n)$，可知 $M^{ed}=M(\mathrm{mod}\ q)$. 由中国剩余定理必有 $M^{ed}=M(\mathrm{mod}\ n)$，故当 M 不与 n 互质时，也可成功解密.

练习 E.1 写出应用 RSA 的例子相当冗长，最好是读者亲自实践. 用 $p=3$ 和 $q=11$ 每次加密一个字母，来对单词"*QUANTUM*"(或至少是前几个字母)进行加密. 适当选择 e 和 d 的值，英语的每个字母用 5 个比特表示.

RSA 实现的有效性如何？在实现时需要考虑两个问题. 第一是密码系统公钥和私钥的产生问题. 如果这不能很快进行，那么 RSA 对很多情况并不好用. 主要的瓶颈是素数 p 和 q 的产生. 解决办法是随机产生期望长度的数，然后应用素性检验的手续确定该数是否确为素数. 像 Miller-Rabin 测试那样的快速素性检验法，可以用大概 $O(L^3)$ 次运算，来判定一个数是否为素数，其中 L 是密钥的期望长度. 如果该数被发现为合数，我们就简单地重复上述过程，直到找到一个素数. 素数定理(参见问题 D.1)，蕴含任何给定的数为素数的概率大约为 $1/\log(2^L)=1/L$，因此经过 $O(L)$ 次尝试，以很高的概率可以得到一个素数. 密钥生成的总开销为 $O(L^4)$ 次运算.

实现 RSA 的第二个问题是加密解密变换的有效性问题. 这些过程由模幂运算完成，可用 $O(L^3)$ 次运算有效执行——参见盒子 5.2. 因此 RSA 的所有操作都可以在经典计算机上迅速进行，并且在实践中一台中等计算能力的计算机，可以轻易对付数千比特长度的密钥.

如何破解 RSA？我们描述两种可能的破解方法，一种是基于求阶，另一种基于求因子. 假设 Eve 收到加密的消息 $M^e(\mathrm{mod}\ n)$，并且知道用于加密该消息的公钥 (e,n). 假设她可以找出加密消息的阶，即可以找出使得 $(M^e)^r=1(\mathrm{mod}\ n)$ 的最小正整数 r(不失一般性，我们假设这样的阶是存在的，即 M^e 与 n 互质. 若不是这

样，那么 $M^r \pmod n$ 与 n 有公因子，可以用 Euclid 算法找出，使我们能够用如下所述的第二种方法破解 RSA). 于是练习 D.16 蕴含 r 整除 $\varphi(n)$. 因为 e 与 $\varphi(n)$ 互质，它必然也与 r 互质，因此具有模 r 的乘法逆. 令 d' 是这样的乘法逆，即 $ed'=1+kr$ 对某个整数 k 成立. 于是 Eve 可以通过把被加密的消息提升到 d' 次幂

$$(M^e)^{d'} \pmod n = M^{1+kr} \pmod n \tag{E.8}$$

$$= M \cdot M^{kr} \pmod n \tag{E.9}$$

$$= M \pmod n \tag{E.10}$$

来恢复原始消息 M. 有趣的是 Eve 实际上对私钥 (d,n) 一无所知，她只知道 (d',n). 当然 d' 与 d 有密切的联系，因为 d' 是 e 模 r 的逆，而 d 是 e 模 $\varphi(n)$ 的逆并且 r 整除 $\varphi(n)$. 然而，此例表明，为破解 RSA 不一定非要确定私钥的准确值. 当然，这个方法只有在 Eve 能够有效求阶时奏效. 但在经典计算机上目前尚不知道有这样的方法. 不过在量子计算机上，求阶可以有效进行，如 5.3.1 节描述的，因此 RSA 可以被破解.

练习 E.2 证明 d 也是 e 模 r 的逆，因此 $d=d' \pmod r$.

破解 RSA 的第二种方法可以完全确定私钥. 假设 Eve 可以分解 $n=pq$，找出 p 和 q，并且因此可以有效计算 $\varphi(n)=(p-1)(q-1)$. 那么 Eve 就很容易计算 d，即 e 模 $\varphi(n)$ 的逆，于是完全确定出私钥 (d,n). 因此如果分解大数很容易，那么很容易破解 RSA.

RSA 预设的安全性，基于这些进攻依赖求阶和求因子，这样的被相信(但不知道)在经典计算机上不可解的问题. 不幸的是，甚至当这些问题是困难的情况下，还是不能肯定 RSA 是安全的. 存在这些问题确实是难解的，但仍有其他破解 RSA 方法的可能性. 尽管有这些警告，破解 RSA 的 20 多年的努力均告失败，普遍相信 RSA 对经典计算机上的攻击是安全的.

问题 E.1 写一个计算机程序，用 RSA 算法进行解密和加密. 求一对 20 比特的素数，并用它们来加密 40 比特的消息.

历史和进一步阅读的材料

公钥密码系统是 Diffe 和 Hellman 在 1976 年[DH76]，以及 Merkle 在大约同时独立地发明的，Merkle 的工作直到 1978 年才发表[Mer78]. RSA 密码系统由 Rivest、Shamir 和 Adleman 在稍后发明[RSA78]. 1997 年人们了解到这些思想——公钥密码术，Diffie Hellman 和 RSA 密码系统——实际上是 20 世纪 60 年代末到 70 年代初，由英国情报局 GCHQ 发明的. 该工作的说明可在"http://www.cesg.gov.uk/

about/nsecret"找到. Koblitz 的优秀著作[Kob94]描述了 Miller-Rabin 和 Solovay-Strassen 等的素性测试法,该书是关于数论和密码术的,包含关于公钥密码术的更多材料. 这些素性测试方法是,最早显示随机化算法,比确定性算法更有效的算法中的两个. Solovay-Strassen 算法来源于 Solovay 和 Strassen 发表的[SS76],而 Miller-Rabin 测试则归功于 Miller[Mil76]和 Rabin[Rab80].

参考文献

[AB097] D. Aharonov and M. Ben-Or. Fault tolerant computation with constant error. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing*, pages 176--188, 1997.

[AB099] D. Aharonov and M. Ben-Or. Fault tolerant quantum computation with constant error rate. *SIAM J. Comp.*, page to appear, 1999. *arXive e-print quant-ph* 9906129[1]

[ABOIN96] D. Aharonov, M. Ben-Or, R. Impagliazzo, and N. Nisan. Limitations of noisy reversible computation. *arXive e-print quant-ph* /9611028, 1996.

[ADH97] L. Adleman, J. Demarrais, and M. A. Huang. Quantum computability. *SIAM J. Comp.*, 26(5):1524 - 1540, 1997.

[Adl94] L. M. Adleman. Molecular computation of solutions to combinatorial problems. *Science*, 266:1021, 1994.

[Adl98] L. M. Adleman. Computing with DNA. *Sci. Am.*, 279:54--61, Aug. 1998.

[AE75] L. Allen and J. H. Eberly. *Optical Resonance and Two-level Atoms*. Dover, New York, 1975.

[Aha99a] D. Aharonov. *Noisy Quantum Computation*. Ph. D. thesis, The Hebrew University, Jerusalem, 1999.

[Aha99b] D. Aharonov. Quantum computation. In D. Stauffer, editor, *Annual Reviews of Computational Physics VI*. World Scientific, Singapore, 1999.

[AKN98] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. *STOC 1997*, 1998. *arXive e-print quant ph/9806029*.

[AL70] H. Araki and E. H. Lieb. Entropy inequalities. *Comm. Math. Phys.*, 18:160 - 170, 1970.

[AL97] D. S. Abrams and S. Lloyd. Simulation of many-body Fermi systems on a quantum computer. *Phys. Rev. Lett.*, 79(13):2586 - 2589, 1997. *arXive e-print quant-ph/9703054*.

[1] 带有"arXive e-print quant ph/xxxxxxx"的文献可以在互联网址 http://www.arXiv.org 找到.

[AL99] A. Ashikhmin and S. Lytsin. Upper bounds on the size of quantum codes. *IEEE Trans. Inf. Theory*, 45(4): 1206 – 1215, 1999.

[Alb83] P. M. Alberti. A note on the transition-probability over c-* algebras. *Lett. In Math. Phys.*, 7(1): 25 – 32, 1983.

[Amb00] A. Ambainis. Quantum lower bounds by quantum arguments. *arXive e-print quant-ph/*O002066, 2000.

[And79] T. Ando. Concavity of certain maps on positive definite matrices and applications to Hadamard products. *Linear Algebra Appl.*, 26: 203 – 241, 1979.

[Ash97] A. Ashikhmin. Remarks on bounds for quantum codes, *arXive e-print quant-ph/*9705037, 1997.

[Bar78] E. Barton. A reversible computer using conservative logic. Unpublished MIT 6. 895 term paper, 1978.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175 – 179, IEEE, New York, 1984. Bangalore, India, December 1984.

[BBB+92] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *J. Cryptology*, 5:3 – 28, 1992.

[BBB+98] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor. Security of quantum key distribution against all collective attacks, *arXive e-print quant-ph/*9801022, 1998.

[BBBV97] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5): 1510 – 1523, 1997. *arXive e-print quant-ph/*9701001.

[BBBW82] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. Quantum cryptography, or unforgeable subway tokens. In D. Chaum, R. L. Rivest, and A. T. Sherman, editors, *Advances in Cryptology: Proceedings of Crypto* 82, pages 267 – 275, Plenum Press, New York, 1982.

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and EPR channels. *Phys. Rev. Lett.*, 70: 1895 – 1899, 1993.

[BBC+95] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H.

Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52: 3457 — 3467, 1995. *arXive e-print quant-ph*/9503016.

[BBC+98] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS'98)*, pages 352 — 361, IEEE, Los Alamitos, California, November 1998. *arXive e-print quant-ph*/9802049.

[BBCM95] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Trans. Inf. Theory*, 41: 1915 — 1923, .995.

[BBE92] C. H. Bennett, G. Brassard, and A. K. Ekert. Quantum cryptography. *Sci. Am.*, 267 (4): 50, Oct. 1992.

[BBHT98] M. Boyer, G. Brassard, P. Hoyer, and A. Tapp. Tight bounds on quantum searching. *Fortsch. Phys. Prog. Phys.*, 46(4--5): 493—505, 1998.

[BBM+98] D. Boschi, S. Branca, F. D. Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolski Rosen channels. *Phys. Rev. Lett.*, 80: 1121 — 1125, 1998. *arXive e-print quant-ph*/9710013.

[BBP+96] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76: 722, 1996. *arXive e-print quant-ph*/9511027.

[BBPS96] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53 (4): 2046—2052, 1996. *arXive e-print quant-ph*/9511030.

[BBR88] C. H. Bennett, G. Brassard, and J. M. Robert. Privacy amplification by public discussion. *SIAM J. Comp.*, 17: 210--229, 1988.

[BCDP96] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill. Efficient networks for quantum factoring. *Phys. Rev. A*, 54(2): 1034, 1996. *arXive e-print quant-ph*/9602016.

[BCF+96] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher. Noncommuting mixed states cannot be broadcast. *Phys. Rev. Lett.*, 76 (15): 2828 — 2821, 1996. *arXive e-print quant-ph*/9511010.

[BCJ+99] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. Separability of very noisy mixed states and implications for NMR quantum computing. *Phys. Rev. Lett.*, 83(5): 1054—1057, 1999.

[BCJD99] G. K. Brennen, C. M. Caves, P. S. Jessen, and I. H. Deutsch. Quantum logic gates in optical lattices. *Physical Review Letters*, 82: 1060—1063, 1999.

[BD00] C. H. Bennett and D. P. DiVincenzo. Quantum information and computation. *Nature*, 404:247—255, 2000.

[BDG88a] J. L. Balcázar, J. Diaz, and J. Gabarró. *Structural Complexity*, Volume I. Springer-Verlag, Berlin, 1988.

[BDG88b] J. L. Balcázar, J. Diaz, and J. Gabarró. *Structural Complexity*, Volume II Springer-Verlag, Berlin, 1988.

[BDK92] R. G. Brewer, R. G. DeVoe, and R. Kallenbach. Planar ion microtraps. *Phys. Rev. A*, 46 (11):R6781—6784, 1992.

[BDS97] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin. Capacities of quantum erasure channels. *Phys. Rev. Lett.*, 78(16): 3217—3220, 1997. *arXive e-print quant-ph/9701015.*

[BDSW96] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed state entanglement and quantum error correction. *Phys. Rev. A*, 54: 3824, 1996. *arXive e-print quant-ph/9604024.*

[Bel64] J. S. Bell. On the Einstein-Podolsy-Rosen paradox. *Physics*, 1: 195—200, 1964. Reprinted in J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, Cambridge University Press, Cambridge, 1987.

[Ben73] C. H. Bennett. Logical reversibility of computation. *IBM J. Res. Dev.*, 17(6):525—532, 1973.

[Ben80] P. Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *J. Stat. Phys.*, 22 (5):563—591, 1980.

[Ben82a] C. H. Bennett. The thermodynamics of computation—A review. *Int. J. Theor. Phys.* 21, 905—940, 1982.

[Ben87] C. H. Bennett. Demons, engines and the second law. *Sci. Am.*, 295(5):108, 1987.

[Ben89] C. H. Bennett. Time-space tradeoffs for reversible computation. *SIAM J. Comput.*, 18: 766—776, 1989.

[Ben92] C. H. Bennett. Quantum cryptography using any two non-

orthogonal states. *Phys. Rev. Lett.*, 68(21): 3121—3124, 1992.

[Bet84] T. Beth. *Methoden der Schnelle Fouriertransformation*. Teubner Leipzig, 1984.

[BFGL98] S. L. Braunstein, C. A. Fuchs, D. Gottesman, and H. Lo. A quantum analog of Huffman coding. *arXive e-print quant-ph*/9805080, 1998.

[BFJS96] H. Barnum, C. A. Fuchs, R. Jozsa, and B. Schumacher. General fidelity limit for quantum channels. *Phys. Rev. A*, 54:4707, 1996. *arXive e-print quant-ph* /9603014.

[Bha97] R. Bhatia. *Matrix Analysis*. Springer-Verlag, New York, 1997.

[BHT98] G. Brassard, P. Hoyer, and A. Tapp. Quantum counting, *arXive e-print quant ph* 9805082, 1998.

[BK92] V. B. Braginsky and F. Y. Khalili. *Quantum Measurement*. Cambridge University Press, Cambridge, 1992.

[BK98a] S. L. Braunstein and H. J. Kimble. Teleportation of continuous quantum variables. *Phys. Rev. Lett.*, 80: 869—872, 1998.

[BK98b] S. B. Bravyi and A. Y. Kitaev. Quantum codes on a lattice with boundary, *arXive e-print quant-ph*/9811052, 1998.

[BK99] S. L. Braunstein and H. J. Kimble. Dense coding for continuous variables, *arXive e-print quant-ph*/9910010, 1999.

[BKLW99] D. Bacon, J. Kempe, D. A. Lidar, and K. B. Whaley. Universal fault tolerant computation on decoherence-free subspaces, *arXive e-print quant-ph* /9909058, 1999.

[BKN98] H. Barnum, E. Knill, and M. A. Nielsen. On quantum fidelities and channel capacities. *arXive e-print quant-ph*/9809010, 1998.

[BL95] D. Boneh and R. J. Lipton. Quantum cryptoanalysis of hidden linear functions (extended abstract). In Don Coppersmith, editor, *Lecture notes in computer science — Advances in Cryptology — CRYPTO'95*, pages 124—137, Springer Verlag, Berlin, 1995.

[BMP+99] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan. On universal and fault-tolerant quantum computing. *arXive e print quant-ph*/9906054, 1999.

[BNS98] H. Barnum, M. A. Nielsen, and B. W. Schumacher. Information transmission through a noisy quantum channel. *Phys. Rev. A*, 57:4153, 1998.

[Boh51] D. Bohm. *Quantum Theory*. Prentice-Hall, Englewood Cliffs, New Jersey, 1951.

[BP93] S. M. Barnett and S. J. D. Phoenix. Information-theoretic limits to quantum cryptography. *Phys. Rev. A*, 48(1): R5－R8, 1993.

[BPM+97] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390 (6660):575－579, 1997.

[BR98] D. S. Bethune and W. P. Risk. An autocompensating quantum key distribution system using polarization splitting of light. In *IQEC '98 Digest of Post deadline Papers*, pages QPD12－2, Optical Society of America, Washington, DC, 1998.

[BR00] D. S. Bethune and W. P. Risk. An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light. *J. Quantum Electronics*, 36 (3): 100, 2000.

[Bra93] G. Brassard. A bibliography of quantum cryptography. *Université de Montréal preprint*, pages 1－10, 3 December 1993. A preliminary version of this appeared in *Sigact News*, vol. 24 (3), 1993, pages 16－20.

[Bra98] S. L. Braunstein. Error correction for continuous quantum variables. *Phys. Rev. Lett.*, 80:4084－4087, 1998. *arXive e-print quant-ph*/9711049.

[BS94] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In T. Helleseth, editor, *Lecture Notes in Computer Science; Advances in Cryptology - EUROCRYPT'93*, Volume 765, pages 410423, Springer-Verlag, New York, 1994.

[BS98] C. H. Bennett and P. W. Shor. Quantum information theory, *itit*, 44 (6): 2724 － 2742, 1998.

[BST98] H. Barnum, J. A. Smolin, and B. Terhal. Quantum capacity is properly defined without encodings. *Phys. Rev. A*, 58 (5):3496－3501, 1998.

[BT97] B. M. Boghosian and W. Taylor. Simulating quantum mechanics on a quantum computer, *arXive e-print quant-ph*/9701019, 1997.

[BV97] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26 (5): 1411－1473, 1997. *arXive e-print quant-ph*/9701001.

[BW92] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69 (20):2881－2884, 1992.

[CAK98] N. J. Cerf, C. Adami, and P. Kwiat. Optical simulation of

quantum logic. *Phys. Rev. A*, 57:R1477, 1998.

[Cay99] C. M. Caves. Quantum error correction and reversible operations. *Journal of Superconductivity*, 12(6):707—718, 1999.

[CD96] R. Cleve and D. P. DiVincenzo. Schumacher's quantum data compression as a quantum computation. *Phys. Rev. A*, 54: 2636. 1996. *arXive e-print quant ph*/9603009.

[CEMM98] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *Proc. R. Soc. London A*, 454 (1969):339 - 354, 1998.

[CFH97] D. G. Cory, A. F. Fahmy, and T. F. Havel. Ensemble quantum computing by NMR spectroscopy. *Proc. Nat. Acad. Sci. USA*, 94:1634 — 1639. 1997.

[CGK98] I. L. Chuang, N. Gershenfeld, and M. Kubinec. Experimental implementation of fast quantum searching. *Phys. Rev. Lett.*, 18(15):3408 - 3411. 1998.

[CGKL98] I. L. Chuang, N. Gershenfeld, M. G. Kubinec, and D. W. Leung. Bulk quantum computation with nuclear-magnetic-resonance: theory and experiment. *Proc. R Soc. London A*, 454 (1969): 447 — 467. 1998.

[Che68] P. R. Chernoff. Note on product formulas for operator semigroups. *J. Functional Analysis*, 2:238—242. 1968.

[Cho75] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra and Its Applications*, 10: 285 — 290. 1975.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 49:1804 — 1807, 1969.

[Chu36] A. Church. An unsolvable problem of elementary number theory. *Am. J. Math.* (*reprinted in* [*Dav*65]). 58:345. 1936.

[CK81] I. Csiszár and J. Korner. Information Theory: Coding Theorems for Discrete Memoryless Systems. *Academic Press*, New York. 1981.

[CL83] A. O. Caldeira and A. J. Leggett. Quantum tunnelling in a dissipative system. *Ann. Phys.*, 149(2): 374 — 456, 1983.

[Cla89] M. Clausen. Fast generalized Fourier transforms. *Theor. Comput. Sci.*, 67: 55 — 63, 1989.

[Cle99] R. Cleve. The query complexity of order-finding. *arXive e-print quant-ph*/9911124, 1999.

[CLR90] T. H. Cormen, C. E. Leiser-

son, and R. L. Rivest. *Introduction to Algorithms*. MIT Press, Cambridge, Mass., 1990.

[CM97] C. Cachin and U. M. Maurer. Linking information reconciliation and privacy amplification. *J. Cryptology*, 10:97—110, 1997.

[CM00] I. L. Chuang and D. Modha. Reversible arithmetic coding for quantum data compression. *IEEE Trans. Inf. Theory*, 46(3): 1104, May 2000.

[CMP+98] D. G. Cory, W. Mass, M. Price, E. Knill, R. Lafiamme, W. H. Zurek, T. F. Havel, and S. S. Somaroo. Experimental quantum error correction, *arXive e-print quant-ph*/9802018, 1998.

[CN97] I. L. Chuang and M. A. Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *J. Mod. Opt.*, 44(11—12):2455—2467, 1997. *arXive e-print quant-ph*/9610001.

[Con72] J. H. Conway. Unpredictable iterations. In *Proceedings of the Number Theory Conference*, pages 49—52, Boulder, Colorado, 1972.

[Con86] J. H. Conway. Fractran: a simple universal programming language. In T. M. Cover and B. Gopinath, editors, *Open Problems in Communication and Computation*, pages 4—26, Springer-Verlag, New York, 1986.

[Coo71] S. A. Cook. The complexity of theorem-proving procedures. In *Proc. 3rd Ann. ACM Symp. on Theory of Computing*, pages 151—158, Association for Computing Machinery, New York, 1971.

[Cop94] D. Coppersmith. An approximate Fourier transform useful in quantum factoring. *IBM Research Report RC* 19642, 1994.

[CPZ96] J. I. Cirac, T. Pellizzari, and P. Zoller. Enforcing coherent evolution in dissipative quantum dynamics. *Science*, 273: 1207, 1996.

[CRSS97] A. R. Calderbank, E. M. Rains P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78:405—408, 1997.

[CRSS98] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory*, 44(4): 1369—1387, 1998.

[CS96] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54: 1098, 1996. *arXive e-print quant-ph*/9512032.

[CST89] R. A. Campos, B. E. A. Saleh, and M. C. Tiech. Quantum mechanical lossless beamsplitters: SU(2) symmetry and photon statistics. *Phys. Rev. A*, 40:1371, 1989.

[CT91] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley and Sons, New York, 1991.

[CTDL77a] C. Cohen Tannoudji, B. Diu, and F. Laloe. *Quantum Mechanics, Vol. I*. John Wiley and Sons, New York, 1977.

[CTDL77b] C. Cohen Tannoudji, B. Diu, and F. Laloë. *Quantum Mechanics, Vol. II*. John Wiley and Sons, New York, 1977.

[CVZ+98] I. L. Chuang, L. M. K. Vandersypen, X. L. Zhou, D. W. Leung, and S. Lloyd. Experimental realization of a quantum algorithm. *Nature*, 393(6681):143—146, 1998.

[CW95] H. F. Chau and F. Wilczek. Simple realization of the Fredkin gate using a series of two body operators. *Phys. Rev. Lett.*, 75(4):748—750, 1995. *arXive e-print quant-ph*/9503005.

[CY95] I. L. Chuang and Y. Yamamoto. Simple quantum computer. *Phys. Rev. A*, 52:3489—3496, 1995. *arXive e print quant-ph*/9505011.

[CZ95] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, 71:4091, 1995.

[Dav65] M. D. Davis. *The Undecidable*. Raven Press, Hewlett, New York, 1965.

[Day76] E. B. Davies. *Quantum Theory of Open Systems*. Academic Press, London, 1976.

[DBE95] D. Deutsch, A. Barenco, and A. Ekert. Universality in quantum computation. *Proc. R. Soc. London A*, 449(1937):669—677, 1995.

[Deu83] D. Deutsch. Uncertainty in quantum measurements. *Phys. Rev. Lett.*, 50(9):631—633, 1983.

[Deu85] D. Deutsch. Quantum theory, the Church-Turing Principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400:97, 198..

[Deu89] D. Deutsch. Quantum computational networks. *Pro. R. Soc. London A*, 425:73, 1989.

[DG98] L.-M. Duan and G.-C. Guo. Probabilistic cloning and identification of linearly independent quantum states. *Phys. Rev. Lett.*, 80:4999—5002, 1998. *arXive e-print quant-ph*/9804064.

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory*, IT-22(6):644—654, 1976.

[DH96] C. Dtirr and P. Hoyer. A quantum algorithm for finding the minimum, *arXive e-print quant-ph*/9607014, 1996.

[Die82] D. Dieks. Communication by EPR devices. *Phys. Lett. A*, 92(6):271—272, 1982.

[DiV95a] D. P. DiVincenzo. Quantum computation. *Science*, 270: 255, 1995. *arXive e-print quant-ph*/9503016

[DiV95b] D. P. DiVincenzo. Two-bit gates are universal for quantum computation. *Phys. Rev. A*, 51(2):1015—1022, 1995.

[DiV98] D. P. DiVincenzo. Quantum gates and circuits. *Proc. R. Soc. London A*, 454: 261—276, 1998.

[DJ92] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proc. R. Soc. London A*, 439:553, 1992.

[DL98] W. Diffie and S. Landau. *Privacy on the Line: the Politics of Wiretapping and Encryption*. MIT Press, Cambridge Massachusetts, 1998.

[DMB+93] L. Davidovich, A. Maali, M. Brune, J. M. Raimond, and S. Haroche. *Phys. Rev. Lett.*, 71:2360, 1993.

[DR90] P. Diaconis and D. Rockmore. Efficient computation of the Fourier transform on finite groups. *J. Amet. Math. Soc.*, 3(2):297—332, 1990.

[DRBH87] L. Davidovich, J. M. Raimond, M. Brune, and S. Haroche. *Phys. Rev. A*, 36: 3771, 1987.

[DRBH95] P. Domokos, J. M. Raimond, M. Brune, and S. Haroche. Simple cavity-QED, two-bit universal quantum logic gate: The principle and expected performances. *Phys. Rev. Lett.*, 52:3554, 1995.

[DS96] D. P. DiVincenzo and P. W. Shor. Fault-tolerant error correction with efficient quantum codes. *Phys. Rev. Lett.*, 77: 3260, 1996.

[DSS98] D. P. DiVincenzo, P. W. Shor, and J. Smolin. Quantum-channel capacities of very noisy channels. *Phys. Rev. A*, 57 (2):830—839, 1998.

[Ear42] S. Earnshaw. On the nature of the molecular forces which regulate the constitution of the luminiferous ether. *Trans. Camb. Phil. Soc.*, 7: 97—112, 1842.

[EBW87] R. R. Ernst, G. Bodenhausen, and A. Wokaun. *Principles of Nuclear Magnetic Resonance in One and Two Dimensions*. Oxford University Press, Oxford, 1987.

[EH99] M. Ettinger and P. Hoyer. On quantum algorithms for noncommutative hidden subgroups. In *Symposium on Theoretical Aspects in Computer*

Science. University of Trier, 1999. *arXive e-print quant-ph*/9807029.

[EHK99] M. Ettinger, P. Hoyer, and E. Knill. Hidden subgroup states are almost orthogonal. *arXive e-print quant-ph*/9901034, 1999.

[EHPP94] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres. Eavesdropping on quantum-cryptographical systems. *Phys. Rev. A*, 50(2):1047—1056, 1994.

[EJ96] A. Ekert and R. Jozsa. Quantum computation and Shor's factoring algorithm. *Rev. Mod. Phys.*, 68:1, 1996.

[EJ98] A. Ekert and R. Jozsa. Quantum algorithms: Entanglement enhanced information processing. *Proc. R. Soc. London A*, 356(1743):1769—1782, Aug. 1998. *arXive e-print quant-ph*/9803072.

[Eke91] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661—663, 1991.

[EM96] A. Ekert and C. Macchiavllo. Error correction in quantum communication. *Phys. Rev. Lett.*, 77:2585, 1996. *arXive e-print quant-ph*/9602022.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777—780, 1935.

[Eps73] H. Epstein. *Commun. Math. Phys.*, 31:317—325, 1973.

[Fan73] M. Fannes. A continuity property of the entropy density for spin lattice systems. *Commun. Math. Phys.*, 31:291—294, 1973.

[FC94] C. A. Fuchs and C. M. Caves. Ensemble-dependent bounds for accessible information in quantum mechanics. *Phys. Rev. Lett.*, 73(23):3047—3050, 1994.

[Fel68a] W. Feller. *An Introduction to Probability Theory and its Applications*, Volume 1. Wiley, New York, 1968.

[Fel68b] W. Feller. *An Introduction to Probability Theory and its Applications*, Volume 2. Wiley, New York, 1968.

[Fey82] R. P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467, 1982.

[FG98] E. Farhi and S. Gutmann. An analog analogue of a digital quantum computation. *Phys. Rev. A*, 57(4):2403—2406, 1998. *arXive e-print quant-ph*/9612026.

[FLS65a] R. P. Feynman, R. B. Leighton, and M. Sands. Volume Ⅲ of *The Feynman Lectures on Physics*. Addison-Wesley, Reading, Mass., 1965.

[FLS65b] R. P. Feynman, R. B. Leighton, and M. Sands. Volume I of *The Feynman Lectures on Physics*. Addison-Wesley, Reading, Mass., 1965.

[FM98] M. H. Freedman and D. A. Meyer. Projective plane and planar quantum codes. *arXive e-print quant-ph*/9810055, 1998.

[FS92] A. Fässler and E. Stiefel. *Group Theoretical Methods and Their Applications*. Birkhaüser, Boston, 1992.

[FSB+98] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik. Unconditional quantum teleportation. *Science*, 282: 706—709, 1998.

[FT82] E. Fredkin and T. Toffoli. Conservative logic. *Int. J. Theor. Phys.*, 21 (3/4): 219—253, 1982.

[Fuc96] C. A. Fuchs. *Distinguishability and Accessible Information in Quantum Theory*. Ph. D. thesis, The University of New Mexico, Albuquerque, NM, 1996. *arXive e-print quant-ph*/9601020.

[Fuc97] C. A. Fuchs. Nonorthogonal quantum states maximize classical information capacity. *Phys. Rev. Lett.*, 79 (6): 1162—1165, 1997.

[Gar91] C. W. Gardiner. *Quantum Noise*. Springer-Verlag, Berlin, 1991.

[GC97] N. Gershenfeld and I. L. Chuang. Bulk spin resonance quantum computation. *Science*, 275: 350, 1997.

[GC99] D. Gottesman and I. L. Chuang. Quantum teleportation is a universal computational primitive. *Nature*, 402: 390 — 392, 1999. *arXive e-print quant-ph*/9908010.

[GJ79] M. R. Garey and D. S. Johnson. *Computers and Intractibility*. W. H. Freeman and Company, New York, 1979.

[GN96] R. B. Griffiths and C.-S. Niu. Semiclassical Fourier transform for quantum computation. *Phys. Rev. Lett.*, 76 (17): 3228 — 3231, 1996. *arXive e-print quant-ph*/9511007.

[Gor64] J. P. Gordon. Noise at optical frequencies: information theory. In P. A. Miles, editor, *Quantum Electronics and Coherent Light*, Proceedings of the International School of Physics 'Enrico Fermi' XXXI. Academic Press, New York, 1964.

[Got96] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, 54: 1862, 1996.

[Got97] D. Gottesman. Stabilizer Codes and *Quantum Error Correction*.

Ph. D. thesis, California Institute of Technology, Pasadena, CA, 1997.

[Got98a] D. Gottesman. Fault-tolerant quantum computation with higher dimensional systems. *arXive e-print quant ph* 9802007, 1998.

[Got98b] D. Gottesman. Theory of fault-tolerant quantum computation. *Phys. Rev. A*, 57(1): 127 — 137, 1998. *arXive e print quant ph* /9702029.

[GP10] D. Gottesman and J. Preskill. The Hitchiker's guide to the threshold theorem *Eternally in preparation*, 1: 1 — 9120, 2010.

[Gro96] L. Grover. In *Proc. 28th Annual ACM Symposium on the Theory of Computation*, pages 212--219, ACM Press, New York, 1996.

[Gro97] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79(2): 325, 1997. *arXive e-print quant ph* /9706033.

[Gru99] J. Gruska. *Quantum Computing*. McGraw-Hill, London, 1999.

[GS92] G. R. Grimmett and D. R. Stirzaker. *Probability and Random Processes*. Clarendon Press, Oxford, 1992.

[HAD+95] R. J. Hughes, D. M. Aide, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer. Quantum cryptography. *Contemp. Phys.*, 36(3): 149 — 163, 1995. *arXive e-print quant ph* /9504032.

[Hal58] P. R. Halmos. *Finite-dimensional Vector Spaces*. Van Nostrand, Princeton, N. J., 1958.

[Ham89] M. Hammermesh. *Group Theory and its Application to Physical Problems*. Dover, New York, 1989.

[HGP96] J. L. Hennessey, D. Goldberg, and D. A. Patterson. Computer Architecture: *A Quantitative Approach*. Academic Press, New York, 1996.

[HHH96] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223(1 — 2): 1 — 8, 1996

[HHH98] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: is there a 'bound' entanglement in nature? *Phys. Rev. Lett.*, 80(24): 5239 — 5242, 1998.

[HHH99a] M. Horodecki, P. Horodecki, and R. Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Phys. Rev. A*, 60(3): 1888 — 1898, 1999.

[HHH99b] M. Horodecki, P. Horodecki,

and R. Horodecki. Limits for. Entanglement measures, *arXive e-print quant-ph/* 9908065, 1999.

[HHH99c] P. Horodecki, M. Horodecki, and R. Horodecki. Bound entanglement can be activated. *Phys. Rev. Lett.*, 82(5): 1056—1059, 1999.

[HJ85] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge University Press, Cambridge, 1985.

[HJ91] R. A. Horn and C. R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, Cambridge, 1991.

[HJS+96] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters. Classical information capacity of a quantum channel. *Phys. Rev. A*, 54:1869,1996.

[HJW93] L. P. Hughston, R. Jozsa, and W. K. Wootters. A complete classification of quantum ensembles having a given density matrix. *Phys. Lett. A*, 183: 14—18, 1993.

[HK69] K.-E. Hellwig and K. Kraus. Pure operations and measurements. *Commun. Math. Phys.*, 11:214—220, 1969.

[HK70] K.-E. Hellwig and K. Kraus. Operations and measurements. Ⅱ. *Commun. Math. Phys.*, 16:142—147, 1970.

[Hof79] D. R. Hofstadter. *Gödel, Escher, Bach: an Eternal Golden Braid*. Basic Books, New York, 1979.

[Hol73] A. S. Holevo. Statistical problems in quantum physics. In Gisiro Maruyama and Jurii V. Prokhorov, editors, *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, pages 104—119, Springer-Verlag, Berlin, 1973. Lecture Notes in Mathematics, vol. 330.

[Hol79] A. S. Holevo. Capacity of a quantum communications channel. *Problems of Inf. Transm.*, 5(4): 247—253, 1979.

[Hol98] A. S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Trans. Inf. Theory*, 44(1): 269—273, 1998.

[Hor97] M. Horodecki. Limits for compression of quantum information carried by ensembles of mixed states. *Phys. Rev. A*, 57:3364—3369, 1997.

[HSM+98] A. G. Huibers, M. Switkes, C. M. Marcus, K. Campman, and A. C. Gossard. Dephasing in open quantum dots. *Phys. Rev. Lett.*, 82:200, 1998.

[HW60] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers, Fourth Edition*. Oxford University Press, London, 1960.

[IAB+99] A. Imamoglu, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss, M. Sherwin, and A. Small. Quantum information processing using quantum dot spins and cavity qed. *Phys. Rev. Lett.*, 83(20):4204—4207, 1999.

[IY94] A. Imamoglu and Y. Yamamoto. Turnstile device for heralded single photons: Coulomb blockade of electron and hole tunneling in quantum confined p-i-n heterojunctions. *Phys. Rev. Lett.*, 72(2):210—213, 1994.

[Jam98] D. James. The theory of beating of the quantum ground state of trappedions. *arXive e-print quant-ph* 9804048, 1998.

[Jay57] E. T. Jaynes. Information theory and statistical mechanics, ii. *Phys. Rev.*, 108(2): 171—190, 1957.

[JM98] J. A. Jones and M. Mosca. Implementation of a quantum algorithm to solve Deutsch's problem on a nuclear magnetic resonance quantum computer. *arXive e print quant-ph* 9801027, 1998.

[JMH98] J. A. Jones, M. Mosca, and R. H. Hansen. Implementation of a quantum search algorithm on a nuclear magnetic resonance quantum computer. *Nature*, 393(6683):344, 1998. *arXive e-print quant-ph* 9805069.

[Jon94] K. R. W. Jones. Fundamental limits upon the measurement of state vectors. *Phys. Rev. A*, 50:3682—3699, 1994.

[Joz94] R. Jozsa. Fidelity for mixed quantum states. *J. Mod. Opt.*, 41:2315—2323, 1994.

[Joz97] R. Jozsa. Quantum algorithms and the Fourier transform. *arXive e print quant-ph*/9707033, 1997.

[JP99] D. Jonathan and M. B. Plenio. Entanglement-assisted local manipulation of pure states. *Phys. Rev. Lett.*, 83:3566—3569, 1999.

[JS94] R. Jozsa and B. Schumacher. A new proof of the quantum noiseless coding theorem. *J. Mod. Opt.*, 41:2343—2349, 1994.

[Kah96] D. Kahn. *Codebreakers: the Story of Secret Writing*. Scribner, New York. 1996.

[Kan98] B. Kane. A silicon-based nuclear spin quantum computer. *Nature*, 393: 133—137, 1998.

[Kar72] R. M. Karp. Reducibility among combinatorial problems. In *Complexity of Computer Computations*, pages 85—103, Plenum Press, New York, 1972.

[KCL98] E. Knill, I. Chuang, and R. Laflamme. Effective pure states for bulk quantum com-

putation. *Phys. Rev. A*, 57 (5): 3348 — 3363, 1998. *arXive e-print quant-ph/*9706053.

[Kit95] A. Y. Kitaev. Quantum measurements and the Abelian stabilizer problem, *arXive e-print quant-ph*/9511026, 1995.

[Kit97a] A. Y. Kitaev. Fault-tolerant quantum computation by anyons, *arXive e-print quant-ph*/9707021, 1997.

[Kit97b] A. Y. Kitaev. Quantum computations: algorithms and error correction. *Russ. Math. Surv.*, 52(6): 1191 — 1249, 1997.

[Kit97c] A. Y. Kitaev. Quantum error correction with imperfect gates. In A. S. Holevo O. Hirota and C. M. Caves, editors, *Quantum Communication, Computing, and Measurement*, pages 181 — 188, Plenum Press, New York, 1997.

[KL51] S. Kullback and R. A. Leibler. On information and sufficiency. *Ann. Math. Stat.*, 22: 79—86, 1951.

[KL97] E. Knill and R. Laflamme. A theory of quantum error-correcting codes. *Phys. Rev. A*, 55:900, 1997. *arXive e-print quant-ph*/9604034.

[KL99] E. Knill and R. Laflamme. Quantum computation and quadratically signed weight enumerators, *arXive e-print quant-ph*/9909094, 1999.

[Kle31] O. Klein. *Z. Phys.*, 72: 767—775, 1931.

[KLV99] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise, *arXive e-print quant-ph*/9908066, 1999.

[KLZ98a] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation. *Science*, 279(5349): 342 — 345, 1998. *arXive e-print quant-ph/*9702058.

[KLZ98b] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation: error models and thresholds. *Proc. R. Soc. London A*, 454(1969): 365 — 384, 1998. *arXive e-print quant-ph*/9702058.

[KMSW99] P. G. Kwiat, J. R. Mitchell, P. D. D. Schwindt, and A. G. White. Grover's search algorithm: An optical approach, *arXive e-print quant-ph/*9905086, 1999.

[Kni95] E. Knill. Approximating quantum circuits, *arXive e-print quant-ph*/9508006, 1995.

[Knu97] D. E. Knuth. *Fundamental Algorithms 3rd Edition*, Volume 1 of *The Art of Computer Programming*. Addison-Wesley, Reading, Massachusetts, 1997.

[Knu98a] D. E. Knuth. *Seminumerical*

Algorithms 3rd Edition, Volume 2 of *The Art of Computer Programming*. Addison-Wesley, Reading, Massacnusetts, 1998.

[Knu98b] D. E. Kruth. *Sorting and Searching 2nd Edition*, Volume 3 of *The Art of Computer Programming*. Addison-Wesley, Reading, Massachusetts. 1998.

[Kob94] N. Koblitz. *A Course in Number Theory and Cryptography*. Springer-Verlag, New York, 1994.

[KR99] C. King and M. B. Ruskai. Minimal entropy of states emerging from noisy quantum channels. *arXive e print quant-ph*/9911079, 1999.

[Kra83] K. Kraus. *States, Effects, and Operations: Fundamental Notions of Quantum Theory*. *Lecture Notes in Physics*, Vol. 190. Springer-Verlag, Berlin, 1983.

[Kra87] K. Kraus. Complementary observables and uncertainty relations. *Phys. Rev. D*, 35 (10): 3070—3075, 1987.

[KSC+94] P. G. Kwiat, A. M. Steinberg, R. Y. Chiao, P. H. Eberhard, and M. D. Petroff. Absolute efficiency and time-response measurement of single-photon detectors. *Appl. Opt.*, 33 (10): 1844—1853, 1994.

[KU91] M. Kitagawa and M. Ueda. Nonlinear-interferometric generation of number-phase correlated Fermion states. *Phys. Rev. Lett*, 67 (14): 1852, 1991.

[Lan27] L. Landau. Das dampfungsproblem in der wellenmechanik. *Z. Phys.*, 45: 430—441, 1927.

[Lan61] R. Landauer. Irreversibility and heat generation of the computing process. *IBM J. Res. Dev.*, 5: 183, 1961.

[LB99] S. Lloyd and S. Braunstein. Quantum computation over continuous variables. *Phys. Rev. Lett.*, 82: 1784—1787, 1999. *arXive e print quant-ph*/9810082.

[LBW99] D. A. Lidar, D. A. Bacon, and K. B. Whaley. Concatenating decoherence free subspaces with quantum error correcting codes. *Phys. Rev. Lett.*, 82 (22): 4556—4559, 1999.

[LC99] H. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283: 2050—2056, 1999. *arXive e-print quant-ph*/9803006.

[LCW98] D. A. Lidar, I. L. Chuang, ard K. B. Whaley. Decoherence-free subspaces for quantum computation. *Phys. Rev. Lett.*, 81 (12): 2594 - 2597, 1998.

[LD98] D. Loss and D. P. DiVincenzo.

Quantum computation with quantum dots. *Phys. Rev. A*, 57:120—126, 1998.

[Lec63] Y. Lecerf. Machines de Turing réversibles. *Comptes Rendus*. 257:2597—2600, 1963.

[Leo97] U. Leonhardt. *Measuring the Quantum State of Light*. Cambridge University Press, New York, 1997.

[Lev73] L. Levin. Universal sorting problems. *Probl. Peredaci Inf.*, 9: 115 — 116, 1973. Original in Russian. English translation in *Probl. Inf. Transm. USSR* 9:265—266, (1973).

[Lie73] E. H. Lieb. Convex trace functions and the Wigner-Yanase-Dyson conjecture. *Ad. Math.*, 11:267—288, 1973.

[Lie75] E. H. Lieb. *Bull. AMS*, 81: 1—13, 1975.

[Lin75] G. Lindblad. Completely positive maps and entropy inequalities. *Commun. Math. Phys.*, 40:147—151, 1975.

[Lin76] G. Lindblad. On the generators of quantum dynamical semigroups. *Commun. Math. Phys.*, 48:199, 1976.

[Lin91] G. Lindblad. Quantum entropy and quantum measurements. In C. Bendjaballah, O. Hirota, and S. Reynaud, editors, *Quantum Aspects of Optical Communications*, Lecture Notes in Physics, vol. 378, pages 71—80, Springer-Verlag, Berlin, 1991.

[Lip95] R. Lipton. DNA solution of hard computational problems. *Science*, 268: 542 — 525, 1995.

[LKF99] N. Linden, E. Kupce, and R. Freeman. NMR quantum logic gates for homonu-clear spin systems, *arXive e-print quant-ph*/9907003, 1999.

[LL93] A. K. Lenstra and H. W. Lenstra Jr., editors. *The Development of the Number Field Sieve*. Springer-Verlag, New York, 1993.

[Llo93] S. Lloyd. A potentially realizable quantum computer. *Science*, 261:1569, 1993.

[Llo94] S. Lloyd. Necessary and sufficient conditions for quantum computation. *J. Mod. Opt.*, 41(12):2503, 1994.

[Llo95] S. Lloyd. Almost any quantum logic gate is universal. *Phys. Rev. Lett.*, 75(2):346, 1995.

[Llo96] S. Lloyd. Universal quantum simulators. *Science*, 273: 1073, 1996.

[Llo97] S. Lloyd. The capacity of the noisy quantum channel. *Phys. Rev.*, 4, 56:1613, 1997.

[LLS75] R. E. Ladner, N. A. Lynch, and A. L. Selman. A comparison of polynomial-time reducibilities. *Theor. Comp. Sci.*, 1:103—124, 1975.

[LMPZ96] R. Lafiamme, C. Miquel, J.-

P. Paz, and W. H. Zurek. Perfect quantum error correction code. *Phys. Rev. Lett.*, 77: 198, 1996. *arXive e-print quant-ph* 9602019.

[LNCY97] D. W. Leung, M. A. Nielsen, I. L. Chuang, and Y. Yamamoto. Approximate quantum error correction can lead to better codes. *Phys. Rev. A*, 56: 2567–2573, 1997. *arXive e-print quant-ph*/9704002.

[Lo99] H. Lo. A simple proof of the unconditional security of quantum key distribution. *arXive e-print quant-ph* 9904091, 1999.

[Lom87] J. S. Lomont. *Applications of Finite Groups*. Dover, New York, 1987.

[Lou73] W. H. Louisell. *Quantum Statistical Properties of Radiation*. Wiley, New York, 1973.

[LP97] H.-K. Lo and S. Popescu. Concentrating local entanglement by local actions beyond mean values, *arXive e-print quant-ph*/9707038, 1997.

[LP99] N. Linden and S. Popescu. Good dynamics versus bad kinematics. Is entanglement needed for quantum computation? *arXive e-print quant-ph*/9906008, 1939.

[LR68] O. E. Lanford and D. Robinson. Mean entropy of states in quantum-statistical mechanics. *J. Math. Phys.*, 9(7): 1120–1125, 1968.

[LR73a] E. H. Lieb and M. B. Ruskai. A fundamental property of quantum-mechanical entropy. *Phys. Rev. Lett.*, 30(10): 434–436, 1973.

[LR73b] E. H. Lieb and M. B. Ruskai. Proof of the strong subadditivity of quantum mechanical entropy. *J. Math. Phys.*, 14: 1938–1941, 1973.

[LR90] H. Left and R. Rex. *Maxwell's Demon: Entropy, Information, Computing*. Princeton University Press, Princeton, NJ, 1990.

[LS93] L. J. Landau and R. F. Streater. On Birkhoff theorem for doubly stochastic completely positive maps of matrix algebras. *Linear Algebra Appl.*, 193: 107–127, 1993.

[LS98] S. Lloyd and J. E. Slotine. Analog quantum error correction. *Phys. Rev. Lett.*, 80: 4088–4091, 1998.

[LSP98] H.-K. Lo, T. Spiller, and S. Popescu. Quantum information and computation. *World Scientific*, Singapore, 1998.

[LTV98] M. Li, J. Tromp, and P. Vitanyi. Reversible simulation of irreversible computation by pebble games. *Physica D*, 120: 168–176, 1998.

[LV96] M. Li and P. Vitanyi. Reversibility and adiabatic computa-

tion: trading time and space for energy. *Proc. R. Soc. London A*, 452:76.

[LVZ+99] D. W. Leung, L. M. K. Vandersypen, X. Zhou, M. Sherwood, C. Yannoni, M. Kubinec, and I. L. Chuang. Experimental realization of a two-bit phase damping quantum code. *Phys. Rev. A*, 60: 1924, 1999.

[Man80] Y. Manin. *Computable and Uncomputable (in Russian)*. Sovetskoye Radio, Moscow, 1980.

[Man99] Y. I. Manin. Classical computing, quantum computing, and Shor's factoring algorithm, *arXive e-print quant-ph/9903008*, 1999.

[Mau93] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory*, 39:733—742, 1993.

[Max71] J. C. Maxwell. *Theory of Heat*. Longmans, Green, and Co., London, 1871.

[May98] D. Mayers. Unconditional security in quantum cryptography, *arXive e-print quant-ph/9802025*, 1998.

[ME99] M. Mosca and A. Ekert. The hidden subgroup problem and eigenvalue estimation on a quantum computer, *arXive e-print quant-ph/9903071*, 1999.

[Mer78] R. Merkle. Secure communications over insecure channels. *Comm. of the ACM*, 21: 294—299, 1978.

[Mil76] G. L. Miller. Riemann's hypothesis and tests for primality. *J. Comput. Syst. Sci.*, 3 (3):300—317, 1976.

[Mil89a] G. J. Milburn. Quantum optical Fredkin gate. *Phys. Rev. Lett.*, 62(18):2124, 1989.

[Mil89b] D. A. B. Miller. Optics for low energy communications inside digital processors: quantum detectors, sources, and modulators as efficient impedance converters. *Opt. Lett.*, 14: 146, 1989.

[Mil96] G. J. Milburn. A quantum mechanical Maxwell's demon. Unpublished, 1996.

[Mil97] G. J. Milburn. Scr6dinger's Machines: *the Quantum Technology Reshaping Everyday Life*. W. H. Freeman, New York, 1997.

[Mil98] G. J. Milburn. *The Feynman Processor: Quantum Entanglement and the Computing Revolution*. Perseus Books, Reading, Mass., 1998.

[Min67] M. L. Minsky. *Computation: finite and infinite machines*. Prentice-Hall, Englewood Cliffs, N. J., 1967.

[MM92] M. Marcus and H. Minc. *A Survey of Matrix Theory and Matrix InequaliTies*. Dover,

New York, 1992.

[MMK+95] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland. Demonstration of a fundamental quantum logic gate. *Phys. Rev. Lett.*, 75: 4714, 1995.

[MO79] A. W. Marshall and I. Olkin. Inequalities: *Theory of Majorization and its Applications*. Academic Press, New York, 1979.

[MOL+99] J. E. Mooij, T. P. Orlando, L. Levitov, L. Tian, C. H. van der Waal, and S. Lloyd. Josephson persistent-current qubit. *Science*, 285: 1036 – 1039, 1999.

[Mor98] T. Mor. No-cloning of orthogonal states in composite systems. *Phys. Rev. Lett.*, 80: 3137—3140, 1998.

[Mos98] M. Mosca. Quantum searching, counting and amplitude amplification by eigenvector analysis. In R. Freivalds, editor, *Proceedings of International Workshop on Randomized Algorithms*, pages 90—100, 1998.

[Mos99] M. Mosca. *Quantum Computer Algorithms*. Ph. D. thesis, University of Oxford, 1999.

[MR95] R. Motwani and P. Raghavan. *Randomized Algorithms*. Cambridge University Press, Cambridge, 1995.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-correcting Codes*. North-Holland, Amsterdam, 1977.

[MU88] H. Maassen and J. H. B. Uffink. Generalized entropic uncertainty relations. *Phys. Rev. Lett.*, 60 (12): 1103 1106, 1988.

[MvOV96] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[MWKZ96] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger. Dense coding in experimental quantum communication. *Phys. Rev. Lett.*, 76 (25): 4656—4659, 1996.

[MZG96] A. Muller, H. Zbinden, and N. Gisin. Quantum cryptography over 23 km in installed under-lake telecom fibre. *Europhys. Lett.*, 33: 334 — 339, 1996.

[NC97] M. A. Nielsen and C. M. Caves. Reversible quantum operations and their application to teleportation. *Phys. Rev.*, 4, 55(4): 2547—2556, 1997.

[NCSB98] M. A. Nielsen, C. M. Caves, B. Schumacher, and H. Barnum. Information-theoretic approach to quantum error correction and reversible measurement. *Proc. R. Soc. London A*, 454(1969): 277—304, 1998.

[Nie98] M. A. Nielsen. *Quantum In-*

formation Theory. Ph. D. thesis, University of New Mexico, 1998.

[Nie99a] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett.*, 83(2):436—439, 1999.

[Nie99b] M. A. Nielsen. Probability distributions consistent with a mixed state, *arXive e-print quant-ph*/9909020, 1999.

[NKL98] M. A. Nielsen, E. Knill, and R. Laflamme. Complete quantum teleportation using nuclear magnetic resonance. *Nature*, 396(6706):52—55, 1998.

[NPT99] Y. Nakamura, Y. A. Pashkin, and J. S. Tsai. Coherent control of macroscopic quantum states in a single-cooper-pair box. *Natur*, 398:786 — 788, 1999.

[OP93] M. Ohya and D. Petz. *Quantum Entropy and Its Use*. Springer-Verlag, Berlin, 1993.

[Pai82] A. Pals. Subtle is the Lord: *The Science and the Life of Albert Einstein*. Oxford University Press, Oxford, 1982.

[Pai86] A. Pals. *Inward Bound: Of Matter and Forces in the Physical World*. Oxford University Press, Oxford, 1986.

[Pai91] A. Pals. *Niels Bohr's Times: In Physics, Philosophy, and Polity*. Oxford University Press, Oxford, 1991.

[Pap94] C. M. Papadimitriou. *Computational Complexity*. Addison-Wesley, Reading, Massachusetts, 1994.

[Pat92] R. Paturi. On the degree of polynomials that approximate symmetric Boolean functions (preliminary version). *Proc. 24th Ann. ACM Syrup. on Theory of Computing (STOC'92)*, pages 468—474, 1992.

[PCZ97] J. F. Poyatos, J. I. Cirac, and P. Zoller. Complete characterization of a quantum process: the two-bit quantum gate. *Phys. Rev. Lett.*, 78(2):390—393, 1997.

[PD99] P. M. Platzman and M. I. Dykman. Quantum computing with electrons floating on liquid helium. *Science*, 284: 1967, 1999.

[Pen89] R. Penrose. *The Emperor's New Mind*. Oxford University Press, Oxford, 1989.

[Per52] S. Perils. *Theory of Matrices. Addison-Wesley, Reading, Mass.*, 1952.

[Per88] A. Peres. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 128:19, 1988.

[Per93] A. Peres. *Quantum Theory: Concepts and Methods. Kluwer Academic*, Dordrecht, 1993.

[Per95] A. Peres. Higher order schmidt decompositions. *Phys. Lett. A*, 202:16—17, 1995.

[Pet86] D. Petz. Quasientropies for finite quantum systems. *Rep. Math. Phys.*, 23(1): 57–65, 1986.

[Phy92] Physics Today Editor. Quantum cryptography defies eavesdropping. *Physics Today*, page 21, November 1992.

[PK96] M. B. Plenio and P. L. Knight. Realistic lower bounds for the factorization time of large numbers on a quantum computer. *Phys. Rev. A*, 53: 2986–2990, 1996.

[PK98] M. B. Plenio and P. L. Knight. The quantum-jump approach to dissipative dynamics in quantum optics. *Rev. Mod. Phys.*, 70(1): 101–144, 1998.

[Pop75] R. P. Poplavskii. Thermodynamical models of information processing (in Russian). *Usp. Fiz. Nauk*, 115(3): 465–501, 1975.

[PRB98] M. Pueschel, M. Roetteler, and T. Beth. Fast quantum Fourier transforms for a class of non-abelian groups, *arXive e-print quant-ph* 9807064, 1998.

[Pre97] J. Preskill. Fault-tolerant quantum computation, *arXive e print quant-ph* 9712048, 1997.

[Pre98a] J. Preskill. Fault-tolerant quantum computation. In H.-K. Lo, T. Spiller, and S. Popescu, editors, *Quantum information and computation*. World Scientific, Singapore, 1998.

[Pre98b] J. Preskill. *Physics 229: Advanced Mathematical Methods of Physics—Quantum Computation and Information*. California Institute of Technology, 1998. *URL: http://www.theory.caltech.edu/people/preskill/ph229/*

[Pre98c] J. Preskill. Reliable quantum computers. *Proc. R. Soc. London A*, 454(1969): 385–410, 1998.

[Rab80] M. O. Rabin. Probabilistic algorithm for testing primality. *J. Number Theory*, 12: 128–138, 1980.

[Rah99] H. Z. Rahim. Richard Feynman and Bill Gates: an imaginary encounter. 1999. *URL: http://www.trnsoft.com/features/lrfbg.Htm*

[Rai98] E. M. Rains. Quantum weight enumerators. *IEEE Trans. Inf. Theory*, 44(4): 1388–1394, 1998.

[Rai99a] E. M. Rains. Monotonicity of the quantum linear programming bound. *IEEE Trans. Inf. Theory*, 45(7): 2489–2492, 1999.

[Rai99b] E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inf. Theory*, 45(6): 1827–1832, 1999.

[Rai99c] E. M. Rains. Quantum shadow enumerators. *IEEE Trans. Inf. Theory*, 45(7): 2361—2366, 1999.

[RB98] M. Roetteler and T. Beth. Polynomialtime solution to the hidden subgroup problem for a class of nonabelian groups. *arXive e-print quant-ph/9812070*, 1998.

[Res81] A. Ressler. *The Design of a Conservative Logic Computer and A Graphical Editor Simulator*. Master's thesis, Massachusetts Institute of Technology, 1981.

[RHSS97] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane. Nonadditive quantum code. *Phys. Rev. Lett*, 79(5): 953—954, 1997.

[Roy96] A. Royer. Reduced dynamics with initial correlations, and time-dependent environment and Hamiltonians. *Phys. Rev. Lett.*, 77(16): 3272—3275, 1996.

[RR67] D. W. Robinson and D. Ruelle. *Commun. Math. Phys.*, 5: 288, 1967.

[RSA78] R. L. Rivest, A. Shamir, and L. M. Adleman. A method of obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2): 120—126, 1978.

[Rus94] M. B. Ruskai. Beyond strong subadditivity: improved bounds on the contraction of generalized relative entropy. *Rev. Math. Phys.*, 6(5A): 1147—1161, 1994.

[RWvD84] S. Ramo, J. R. Whinnery, and T. van Duzer. *Fields and waves in communication electronics*. Wiley, New York, 1984.

[RZBB94] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73(1): 58431, 1994.

[Sak95] J. J. Sakurai. *Modern Quantum Mechanics*. Addison-Wesley, Reading, Mass., 1995.

[SC99] R. Schack and C. M. Caves. Classical model for bulk-ensemble NMR quantum computation. *Phys. Rev. A*, 60(6): 4354—4362, 1999.

[Sch06] E. Schmidt. Zur theorie der linearen und nichtlinearen integralgleighungen. *Math. Annalen.*, 63:433—476, 1906.

[Sch36] E. Schrödinger. Probability relations between separated systems. *Proc. Cambridge Philos. Soc.*, 32: 446—452, 1936.

[Sch95] B. Schumacher. Quantum coding. *Phys. Rev. A*, 51:2738—2747, 1995.

[Sch96a] B. Schneier. *Applied Cryptography*. John Wiley and Sons, New York, 1996.

[Sch96b] B. W. Schumacher. Sending entanglement through noisy quantum channels. *Phys. Rev. A*, 54:2614, 1996.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27: 379—423, 6234356, 1948.

[Sho94] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings, 35th Annual Symposium on Foundations of Computer Science*, IEEE Press, Los Alamitos, CA, 1994.

[Sho95] P. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:2493, 1995.

[Sho96] P. W. Shor. Fault-tolerant quantum computation. In *Proceedings, 37th Annual Symposium on Fundamentals of Computer Science*, pages 56—65, IEEE Press, Los Alamitos, CA, 1996.

[Sho97] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM. J. Comp.*, 26 (5): 1484 — 1509, 1997.

[Sim79] B. Simon. *Trace Ideals and Their Applications*. Cambridge University Press Cambridge, 1979.

[Sim94] D. Simon. On the power of quantum computation. In *Proceedings, 35th Annual Symposium on Foundations of Computer Science*, pages 116 — 123. IEEE Press, Los Alamitos, CA, 1994.

[Sim97] D. R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26 (5): 1474 — 1483, 1997.

[SL97] P. W. Shor and R. Laflamme. Quantum analog of the MacWilliams identities for classical coding theory. *Phys. Rev. Lett.*, 78 (8): 1600 — 1602, 1997.

[SL98] D. Shasha and C. Lazere. *Out of Their Minds: The Lives and Discoveries 15 Great Computer Scientists*. Springe-Verlag, New York, 1998.

[Sle74] D. Slepian, editor. *Keys Papers in the Development of Information Theory IEEE Press*, New York, 1974.

[Sli96] C. P. Slichter. *Principles of Magnet Resonance*. *Springer*. Berlin, 1996.

[SN96] B. W. Schumacher and M. A. Nielse. Quantum data processing and error correction. *Phys. Rev. A*, 54 (4): 2629, 1996. *arXive e-print quant-ph*/9604022.

[SP00] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *arXive e-print*

quant-ph 003001, 2000.

[SS76] R. Solovay and V. Strassen. A fast MonteCarlo test for primality. *SIAM J. Comput.*, 6: 84－85, 1976.

[SS96] P. W. Shor and J. A. Smolin. Quantum error-correcting codes need not completely reveal the error syndrome, *arXive e-print quant-ph*/9604006, 1996.

[SS99] A. T. Sornborger and E. D. Stewart. Higher order methods for simulations on quantum computers. *Phys. Rev. A*, 60(3): 1956－1965, 1999. *arXive e-print quant-ph*/9903055.

[ST91] B. E. A. Saleh and M. C. Teich. *Fundamentals of Photonics*. Wiley, NY, 1991.

[Ste96a] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77: 793, 1996.

[Ste96b] A. M. Steane. Multiple particle interference and quantum error correction. *Proc. R. Soc. London A*, 452: 2551－2576, 1996.

[Ste97] A. Steane. The ion-trap quantum information processor. *Appl. Phys. B-Lasers and Optics*, 64(6): 623－642, 1997.

[Ste99] A. M. Steane. Efficient fault-tolerant quantum computing. *Nature*, 399: 124－126, May 1999.

[STH+99] S. Somaroo, C. H. Tseng, T. F. Havel, R. Laflamme, and D. G. Cory. Quantum simulations on a quantum computer. *Phys. Rev. Lett.*, 82: 5381－5384, 1999.

[Str76] G. Strang. *Linear Algebra and Its Applications*. Academic Press, New York, 1976.

[SV99] L. J. Schulman and U. Vazirani. Molecular scale heat engines and scalable quantum computation. *Proc. 31st Ann. ACM Symp. on Theory of Computing (STOC'99)*, pages 322－329, 1999.

[SW49] C. E. Shannon and W. Weaver. *The Mathematical Theory of Communication*. University of Illinois Press, Urbana, 1949.

[SW93] N. J. A. Sloane and A. D. Wyner, editors. *Claude Elwood Shannon: Collected Papers*. IEEE Press, New York, 1993.

[SW97] B. Schumacher and M. D. Westmoreland. Sending classical information vianoisy quantum channels. *Phys. Rev. A*, 56(1): 131－138, 1997.

[SW98] B. Schumacher and M. D. Westmoreland. Quantum privacy and quantum coherence. *Phys. Rev. Lett.*, 80(25): 5695－5697, 1998.

[SWW96] B. W. Schumacher, M. Westmoreland, and W. K. Wootters. Limitation on the amount

of accessible information in a quantum channel. *Phys. Rev. Lett.*, 76:3453, 1996.

[Szi29] L. Szilard. Uber die entropieverminderung in einen thermodynamischen system bei eingriffen intelligenter wesen. *Z. Phys.*, 53:840—856, 1929.

[TD98] B. M. Terhal and D. P. DiVincenzo. The problem of equilibration and the computation of correlation functions on a quantum computer, *arXive e-print quant ph*/9810063, 1998.

[THL+95] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble. Measurement of conditional phase shifts for quantum logic. *Phys. Rev. Lett.*, 75:4710, 1995.

[Tro59] H. F. Trotter. On the product of semigroups of operators. *Proc. Am. Math. Soc.*, 10: 545—551, 1959.

[Tsi80] B. S. Tsirelson. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.*, 4:93, 1980.

[Tur36] A. M. Turing. On computable numbers, with an application to the Entschei-dungsproblem. *Proc. Lond. Math. Soc. 2 (reprinted in [Dav65])*, 42:230, 1936.

[Tur97] Q. A. Turchette. *Quantum optics with single atoms and single photons.* Ph. D. thesis, California Institute of Technology, Pasadena, California, 1997.

[Uhl70] A. Uhlmann. On the Shannon entropy and related functionals on convex sets. *Rep. Math. Phys.*, 1(2):147—159, 1970.

[Uhl71] A. Uhlmann. Sätze über dichtematrizen. *Wiss. Z. Karl-Marx-Univ. Leipzig*, 20: 633—637, 1971.

[Uhl72] A. Uhlmann. Endlich-dimensionale dichtematrizen Ⅰ. *Wiss. Z. Karl-Marx-Univ. Leipzig*, 21:421—152, 1972.

[Uhl73] A. Uhlmann. Endlich-dimensionale dichtematrizen Ⅱ. *Wiss. Z. Karl-Marx Univ. Leipzig*, 22:139—177, 1973.

[Uhl76] A. Uhlmann. The 'transition probability' in the state space of a *-algebra. *Rep. Math. Phys.*, 9:273—279, 1976.

[Uhl77] A. Uhlmann. Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory. *Commun. Math. Phys.*, 54:21—32, 1977.

[Ume62] H. Umegaki. *Kodai Math. Sem. Rep.*, 14:59—85, 1962.

[Vai94] L. Vaidman. Teteportation of quantum states. *Phys. Rev. A*, 49(2):1473—1476, 1994.

[van98a] W. van Dam. Quantum oracle interrogation: getting all information for half the price. In *Proceedings of the 39th FOCS*, 1998. *arXive e-print quant-ph*/9805006.

[van98b] S. J. van Enk. No-cloning and superluminal signaling, *arXive e-print quant-ph*/9803030, 1998.

[Ved99] V. Vedral. Landauer's erasure, error correction and entanglement, *arXive e-print quant-ph*/9903049, 1999.

[Vid98] G. Vidal. Entanglement monotones. *arXive e-print quant-ph*/9807077, 1998.

[Vid99] G. Vidal. Entanglement of pure states for a single copy. *Phys. Rev. Lett.*, 83 (5): 1046—1049, 1999.

[von27] J. von Neumann. *Göttinger Nachrichten*, page 245, 1927.

[von56] J. von Neumann. Probabilistic logics and the synthesis of reliable organisms from unreliable components. In *Automata Studies*, pages 329 — 378, Princeton University Press, Princeton, NJ, 1956.

[von66] J. yon Neumann. Fourth University of Illinois lecture. In A. W. Burks, editor, *Theory of Self-Reproducing Automata*, page 66, University of Illinois Press, Urbana, 1966.

[VP98] V. Vedral and M. B. Plenio. Entanglement measures. *Phys. Rev. A*, 57(3): 1619 — 1633, 1998.

[VR89] K. Vogel and H. Risken, Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase. *Phys. Rev. A*, 40(12): 7113 7120, 1989.

[VYSC99] L. M. K. Vandersypen, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. Realization of effective pure states for bulk quantum computation. *Phys. Rev. Lett.*, 83: 3085 — 3088, 1999.

[VYW+99] R. Vrijen, E. Yablonovitch, K. Wang, H. W. Jiang, A. Balandin, V. Roychowdhury, T. Mor, and D. DiVincenzo. Electron spin resonance transistors for quantum computing in silicon-germanium heterostructures, *arXive e-print quant-ph*/9905096, 1999.

[CWar97] W. Warren. The usefulness of NMR quantum computing. *Science*, 277 (5332): 1688, 1997.

[Wat99] J. Watrous. PSPACE has around quantum interactive proof systems, *arXive e-print cs*/9901015, 1999.

[WC67] S. Winograd and J. D. Cowan. *Reliable Computation in the Presence of Noise*. MIT Press, Cambridge, MA, 1967.

[Weh78] A. Wehrt. General properties of entropy. *Rev. Mod. Phys.*, 50:221, 1978.

[Wel88] D. J. A. Welsh. *Codes and Cryptography*. Oxford University Press, New York, 1988.

[Wie] S. Wiesner. Unpublished

manuscript circa 1969, appeared as [Wie83].

[Wie83] S. Wiesner. Conjugate coding. *SIGACT News*, 15:77, 1983.

[Wie96] S. Wiesner. Simulations of manybody quantum systems by a quantum computer. *arXive e-print quant-ph*/9603028, 1996.

[Wil91] D. Williams. *Probability with Martingales*. Cambridge University Press, Cambridge, 1991.

[Win98] E. Winfree. *Algorithmic Self-Assembly of DNA*. Ph. D. thesis, California Institute of Technology, Pasadena, California, 1998.

[WMI+98] D. J. Wineland, C. Monroe, W. M. Itano, D. Leibfried, B. E. King, and D. M. Meekhof. Experimental issues incoherent quantum-state manipulation of trapped atomic ions. *J. Res. Natl. Inst. Stand. Tech.*, 103: 259, 1998.

[WS98] M. D. Westmoreland and B. Schumacher. Quantum entanglement and the non-existence of superluminal signals, *arXive e-print quant-ph*/9801014, 1998.

[WY63] E. P. Wigner and M. M. Yanase. *Proc. Natl. Acad. Sci. (U. S. A.)*, 19: 910—918, 1963.

[WY90] K. Watanabe and Y. Yamamoto. Limits on tradeoffs between third-order optical nonlinearity, absorption loss, and pulse duration in self-induced transparency and real excitation. *Phys. Rev. A*, 42 (3): 1699—1702, 1990.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299: 802—803, 1982.

[Yao93] A. C. Yao. Quantum circuit complexity. *Proc. of the 34th Ann. IEEE Symp. on Foundations of Computer Science*, pages 352—361, 1993.

[YK95] S. Youms and T. Knight. Non dissipative rail drivers for adiabatic circuits. In *Proceedings, Sixteenth Conference on Advanced Research in VLSI* 1995, pages 404—414, IEEE Computer Society Press, Los Alamitos, CA, 1995.

[YKI88] Y. Yamamoto, M. Kitagawa, and K. Igeta. In *Proc. 3rd Asia-Pacific Phys. Conf.*, World Scientific, Singapore, 1988.

[YO93] H. P. Yuen and M. Ozawa. Ultimate information carrying limit of quantum systems. *Physical Review Letters*, 70: 363—366, 1993.

[YY99] F. Yamaguchi and Y. Yamamoto. Crystal lattice quantum computer. *Appl. Phys. A*, pages 1—8, 1999.

[Zal98] C. Zalka. Simulating quantum systems on a quantum

computer. *Proc. R. Soc. Lon-don A*, 454(1969):313—322, 1998.

[Zal98] C. Zalka. Grover's quantum searching algorithm is optimal. *Physical Review A*, 60: 2746—2751, 1999.

[Zan99] P. Zanardi. Stabilizing quantum information. *arXive e-print quant-ph*/9910016, 1999.

[ZG97] P. Zoller and C. W. Gardiner. Quantum noise in quantum optics: the stochastic Schrödinger equation. In S. Reynaud, E. Giacobino, and J. Zinn-Justin, editors, *Quantum Fluctuations: Les Houches Summer School LXIII*, Elsevier, Amsterdam, 1997.

[ZHSL99] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. Volume of the set of separable states. *Phys. Rev. A*, 58(2):883—892, 1999.

[ZL96] W. H. Zurek and R. Laflamme. Quantum logical operations on encoded qubits. *Phys. Rev. Lett.*, 77(22): 4683—4686, 1996.

[ZLC00] X. Zhou, D. W. Leung, and I. L. Chuang. Quantum logic gate constructions with one-bit "teleportation". *arXive e-print quant-ph/O* 002039, 2000.

[ZR98] P. Zanardi and M. Rasetti. Noiseless quantum codes. *Phys. Rev. Lett.*, 79(17): 3306—3309, 1998.

[Zur89] W. H. Zurek. Thermodynamic cost of computation, algorithmic complexity and the information metric. *Nature*, 341: 119, 1989.

[Zur91] W. H. Zurek. Decoherence and the transition from quantum to classical. *Phys. Today*, October 1991.