Quantum Information Made Easy

通俗量子信息学

何广平 著

科学出版社

内 容 简 介

本书用通俗易懂的语言，介绍量子信息学中的量子算法和量子密码术这两大研究方向的发展历史、重要成果以及最新进展。详细讲解了Deutsch算法、Shor算法、量子纠错码、量子密钥分配、量子秘密分享、量子比特承诺等内容。尤其注重对研究思路的引导，以使读者在通过本书了解到相关知识的同时，能够逐步掌握一定的科研能力。

本书适于对量子力学概念有初步认识的物理或计算机专业的大学本科学生、或对量子信息学感兴趣的科研人员用作教材或参考书。

图书在版编目(CIP)数据

通俗量子信息学 = Quantum Information Made Easy / 何广平著. —北京：科学出版社，2012

ISBN 978-7-03-034504-2

Ⅰ. ①通… Ⅱ. ①何… Ⅲ. ①量子力学 Ⅳ. ①O413.1

中国版本图书馆 CIP 数据核字（2012）第 109983 号

责任编辑：裴 育 唐保军 / 责任校对：朱光兰

责任印制：张 倩 / 封面设计：耕者设计工作室

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

中国科学院印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2012 年 6 月第 一 版 开本：B5（720×1000）

2012 年 6 月第一次印刷 印张：11 3/4

字数：228 000

定价：45.00

（如有印装质量问题，我社负责调换）

前　言

我一向觉得写书不如写科研论文，想不到发现自己也在写书了。

不过写书也有写书的乐趣。与论文相比，书里面可以更多地分享自己处理问题的思路，而不是故作客观地仅仅罗列冰冷的技术性细节和结论。而思路，对于有意真正掌握相关科研技能、不满足于机械地接受既有发展成果的读者来说，才是最重要的。

为此，本书在选材上不求面面俱到，而是在量子信息学中的量子算法和量子密码术这两大领域，选取 Deutsch 算法、Shor 算法、量子纠错码、量子密钥分配、量子秘密分享、量子比特承诺等意义重大从而值得学习、同时又特征明显从而易于学习的内容。此外也在最后一章提及信息论与基本理论的一些尚未成熟、但富有生命力的前沿进展，以便读者对今后的研究方向有所把握。

在写法上，我们则力图在通俗和专业之间取得平衡。本书仍然希望定位于专业读物而不是科普作品，故而不刻意放弃必要和严谨的数学描述。但若是可有可无的数学抽象形式和专业术语则能免则免。力求以浅白的语言，使读者能在具有尽可能少的前期知识基础上接触到这一学科的神髓。总的原则就是一切以引导启发思路为最终目的。

出于这种考虑，对于某些问题，当国际上惯用的、或见于原始文献的表达方式由于注重形式的精简而显得艰深晦涩的时候，我们改为采用从自身经验来看最可能有利于系统地学习理解的描述。例如对 Shor 算法、量子纠错码等问题中涉及的变换操作，本书并没有照搬现有文献的普遍写法，而是按照我们自己的思路重新进行构造，并且还补充了很多在其它文献中鲜见的细节。

也正因为如此，本书中的一些观点难免受到作者个人的见解所影响。例如在发展量子计算机的原因以及量子比特承诺问题上，作者有着与目前该领域内的权威意见相左的立场。斟酌再三，本人不敢轻掩个人之见而盲从主流之说，故而决定直陈自己相信正确的看法。但为免误导，有争议之处都明确地列出各方的观点，望读者注意自行评判。

量子信息是个正在发展的学科，很多当今的结论可能在以后看来其实尚未成熟。不过，我不想以“由于笔者水平有限，因此难免会有错误之处”作为托辞。本书所涉及的结论，都至少是本人在现阶段认为是逻辑上正确的。这就是说，只要当前

（截止到2011年底）的量子力学本身是正确的，则按现有逻辑方法推理，它必然导致本书所给出的量子信息学结论。当然，这样说丝毫不意味着本人对“我们所在的世界为什么必须是量子的”这一问题有什么成见。但它已超出了本书的范围——至少前六章对此完全不做讨论。

借此机会，谨向长期以来对作者的科研工作不倦教导和大力支持的导师李华钟教授（中山大学）致敬。同时，还感谢汪子丹教授（香港大学）、朱诗亮教授（华南师范大学）的指导和合作，陈娟老师（中山大学）在日常工作中的协助，以及王帮海博士（广东工业大学）对本书初稿提出的建议。

本书系国家自然科学基金、广东省自然科学基金资助项目研究成果。

何广平

2012年1月于广州中山大学

目　录

为什么要量子？

量子算法强在哪里？

能抵挡量子算法吗？

还有哪些量子密码术？

与基本理论有关吗?

第1章 绪 论

§1.1 什么是量子信息学

量子信息学是涉及量子力学和信息科学的一门边缘学科。它的开端可以追溯到二十世纪七十年代初甚至更早，但是在八、九十年代才真正得到广泛重视，现在仍处在迅速发展中。因此它的研究内容一直在不断扩充，以后也很可能会有进一步更新。目前，这一领域主要包含以下三个方向：

- 量子算法和量子计算机：

该方向以1985年提出的Deutsch算法[1]为开端。九十年代关于大数因子分解的Shor算法[2]和关于快速搜索的Grover算法[3]的提出，使传统的经典密码术顿时在理论上显得危机重重，让人们看到了量子算法的强大潜力，量子信息学因而一下子成为人们关注的前沿课题。现在人们一方面在理论上不断尝试提出新的量子算法，另一方面在实验上力图制造出能够运行量子算法的装置，即量子计算机。

- 量子密码术：

要抵御强大的量子算法，必须用量子技术武装密码术。因此量子密码术与量子算法形成了量子信息学问题中的一对矛与盾。1970年Stephen Wiesner提出了“量子货币（quantum money）”的概念[4]，可视为最早的量子密码术。但直到1984年Charles Bennett和Gilles Brassard提出了简称为BB84的量子密钥分配（quantum key distribution）协议[5]，量子密码术的实用性和重要性才真正得到广泛承认并开始高速发展。随后人们相继研究了量子隐形传态（quantum teleportation）、量子秘密分享（quantum secret sharing）、量子比特承诺（quantum bit commitment）等众多量子密码术协议，相应的实验技术也取得很大突破，甚至超越了量子计算机的发展水平。目前进行量子密钥分配的实验装置已实现商品化。

- 相关的信息理论问题：

这一方向主要关注经典信息学理论观念在量子层面的对应和延伸，如信息熵、信道容量等经典概念的量子形式，以及量子纠缠度的度量等量子领域独有的新内容。它是量子信息学中发展比较迟的一个分支，至今尚未完全成熟。有些问题甚至离形成统一的定论似乎还比较遥远。比如关于如何定量描述量子纠缠态的纠缠度，目前

就有熵、concurrence、negativity 以及其它众多的度量方法，各有各的长短，新的度量方法也不断被提出来，但至今仍没有哪一种能在任何场合都优于其它描述。

本书仅介绍上述前两个研究方向的内容。鉴于第三个方向的发展现状，并考虑到其内容较深、在应用上目前也不如其它两个方向那么直接，因此在本书中暂且略去。但必须注意，它对于全面、透彻地掌握量子信息学是不可或缺的一个组成部分。它与前面两个方向之间的关系就好比武侠小说中武术的内功与外功的关系。所以希望读者在熟习本书涉及的内容之后，自行阅读该方向的文献资料（例如 Nielsen 和 Chuang[6] 及张永德[7] 的著作中的相关部分）予以充实。

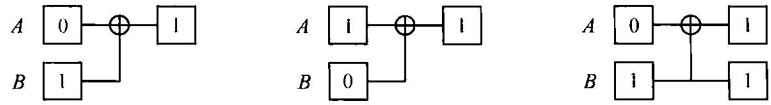
§1.2 发展量子计算机的原因

相对于量子计算机，我们目前身边熟悉的传统计算机可称为经典计算机。在经典计算机技术突飞猛进的今天，为什么要发展量子计算机？在给出正确答案之前，我们先要澄清两种常见的误解。

一种最容易产生的误解，就是以为随着经典计算机不断微型化，器件的大小将进入量子效应不可忽略的微观尺度，从而需要新的理论。其实，这一问题确实存在，但却是属于当前“介观电路”的研究范畴。介观电路理论关注的是在有量子效应的情况下，如何修改经典电路理论、设计新型电路元件、描述电路性能参数等问题，这个层面的计算机运行的仍然是传统的算法。即在被实现的算法上没有利用到量子力学带来的新计算能力。所以它与我们要研究的量子计算机是完全不同的概念。

另一种理解流传甚广，但却值得斟酌。它认为发展量子计算机是解决经典计算机散热问题的需要。这始于 1961 年 IBM 的 Rolf Landauer 研究计算机发热问题时得出的 Landauer 定律[8]：任何对信息的不可逆逻辑操作，例如清除一个比特或合并两条计算路径，都一定会伴随着运算器件或环境的相应的熵增。举例来说，考虑图 1.1 所示的关于两个存储单元 A 和 B 的“逻辑和”运算 $\oplus$，即当 A 和 B 的内容相同时 $A \oplus B = 0$，当 A 和 B 的内容不同时 $A \oplus B = 1$。图 1.1（a）表示我们在存储单元 A 中存入 0，在存储单元 B 中存入 1，然后把运算结果存在 A 中，同时把单元 B 的内容舍弃或清零。图 1.1（b）则表示我们在存储单元 A 中存入 1，在存储单元 B 中存入 0，然后把运算结果存在 A 中并把单元 B 的内容舍弃或清零。显然，这两种情形下存储单元 A 和 B 的最终状态完全相同，都是单元 A 的内容为 1，单元 B 的内容被舍弃或清零。因而我们不可能从 A 和 B 的最终状态逆向推算出它们的初始内容是图 1.1（a）还是图 1.1（b）的情形。所以，这样的运算是不可逆的。而根据热力学第二定律，对环境放热的过程一般都是不可逆过程。因此 Landauer 定律被普遍解读为：计算机发热的原因来自于计算过程的不可逆性。用惯手提电脑的人可

能都会深有感受，就是如果电脑散热不好，CPU 温度显著上升就会导致运算速度下降。因此如果能减少计算机本身的发热，对计算机进一步微型化将大有裨益。而把图 1.1（a）和（b）的不可逆计算改成可逆形式并不难。如图 1.1（c）所示，只要我们在完成计算并把结果存在 A 里面以后，不把单元 B 的内容舍弃而是让它仍保持着初始的内容，则从 A 和 B 的最终状态随时可以反推出它们的初始内容。从这种意义上说，运算就被改写成了可逆的形式。1973 年，IBM 的 Charles Bennett 进一步证明了任何经典计算都可以改写成可逆计算的形式[9]。而量子力学中的幺正变换都是可逆的。于是不少人据此得出结论，只要用量子计算机运行可逆计算，就可以避免发热问题。出于 Landauer 和 Bennett 本身的影响力，加上这一观点出现在一些量子信息方面的早期著作中并在网络上被一些主流网站（如百度百科关于“量子计算机”的词条）广泛引用转载，令很多人以为这是推动量子计算机研究的重要动力之一。



(a)不可逆形式1　　(b) 不可逆形式2　　(c)可逆形式

图 1.1　经典“逻辑和”运算

但笔者认为，上述观点中的逻辑值得推敲。且不说 Landauer 定律本身已有人提出过质疑（参见 Wikipedia 关于“Landauer's principle”词条中的引文），即使 Landauer 定律是正确的，它也并不意味着量子计算机在发热问题上有必然优于经典计算机之处。一方面，从实际实验的角度看，目前已经有人成功进行了 7 个量子比特的量子算法演示（更有报道声称已经制出了 28 个量子比特的量子计算机，但受到一定的质疑，参见 http：//quantalk. org/view. php? id = 41&thread = 1），不过整套设备就像经典计算机问世之初那样，涉及庞大复杂的一大堆装置。其能耗自然不在话下。而根据能量守恒定律不难想象得到，消耗的能量最后大部分都转换成了热的形式。那么为什么实现了量子算法仍然产生出了大量的热量？再者，在图 1.1 所示的经典算法中，运算不可逆的来源似乎来自对单元 B 的内容舍弃或清零。众所周知，如果我们在经典计算机完成计算后拔掉电源，那么暂存器里面的内容自然就丢失了。反而如果我们希望保留这些结果，就需要对计算机维持供给能源。但在上面的推理中，如果保留单元 B 的内容，则运算是可逆的，因而应该是可以降低能耗的，为什么现在保持存储内容反过来需要消耗更多的能量？到这里，可能有些细心的读者已经会注意到问题的所在。也许有人会觉得，这些例子与之前所说的发热不是一回事：上面量子算法实验里消耗的能量主要用于维持设备运作而不是计算过程本身；而经典

计算机维持内存内容需要耗能，则是为了避免表示“1”和“0”的不同电压值在断电后自发落到相近的值上。没错！无论是量子还是经典计算机，耗能及散热的大部分正是用在了为实现计算而需要的相关操作上，比如给总线施加脉冲信号、使得CPU对输入做出反应、对存储单元进行读出和写入操作、进行相应的计算。相对而言，计算过程本身对应的耗能散热只是其中比较小的一部分。而且除非算完不提取结果，不然算过和没算是完全不同的两个状态，一旦算完并读出结果，就不再是可逆的了。再有就是如果能通过绝热等方式保证存储单元与外界环境完全隔绝，那么保持单元内容不变确实是不需要耗能的，然而实际情况是我们永远不可能达到这种理想状态。环境与存储单元的纠缠会导致单元内容自发向着“0”和“1”状态的界限越来越模糊的方向演化，如要避免这种出错，则需要输入能量做功来维持。所以我们的看法是，Landauer定律本身的表述并没有问题，问题是它抓住的只是计算机发热现象中的次要矛盾。不可逆计算过程只是发热的众多原因之一，而远不是唯一的原因。发热现象的主要矛盾是为了实现计算所需要进行的操作的不可逆性，而不是运算本身是否可逆。所以Landauer定律并不能导出“用可逆计算代替不可逆计算就可避免计算机发热”这样的结论，更不能由此作为发展量子计算机的理由。特别是，既然已经证明了所有经典计算都可以改写成相应的可逆计算，如果只要计算可逆就可以避免发热，那么从逻辑上说我们岂不是只需要用经典计算机进行经典的可逆计算就可以达到目的了？何苦还那么艰难地去研究量子计算机？不过，必须指出这些质疑只是笔者个人的见解。前面的观点目前仍然被相当多的人所认同。请读者自行作出自己的评判。

那么，如果说上面两种关于发展量子计算机的原因都是误解，真正原因又是什么呢？实际上，Richard Feynman很早就指出[10]，只有量子的计算机才能真正地模拟量子系统。虽然把这简单的一句话算作量子计算机研究的开端未免牵强，但它已经反映出了量子计算有解决经典计算机无法胜任的任务的可能。1985年的Deutsch算法确实证明了量子算法对特定的问题可以超越经典算法，因此量子计算机才真正有了发展的必要性。量子计算机之所以能如此强大，关键在于量子层面有着本质上完全不同于经典力学的现象和规律。在下一章中，我们将具体说明如何利用量子力学的新特性，构造出优于经典算法的量子算法，从而彻底解释为什么要发展量子计算机。但在此之前，我们需要先弄清楚量子力学有何可供利用的新特性。为此，在§1.3中我们先对量子力学理论的重点做一个简要的概述。

§1.3 量子理论概述

本节将扼要概括量子力学对本书所涉及的量子信息学问题有直接作用的要点，

并对本书常用的公式符号形式做出说明。我们尽力使这一节提供的知识能让不具备量子力学基础的读者在不需要借助其它参考书的情况下都仍能读懂本书的全部内容。但尝试以如此简短的篇幅取代对量子力学的全面学习显然是不切实际的。因此读者在遇到本书阐述不够详尽的量子力学细节问题时，最好还是通过其它的完整量子力学教材补充相关知识。而对量子力学已经有透彻理解的读者，仍建议阅读§1.3.1的最后一段和§1.3.2的第一点（量子比特）和最后一点（广义测量），以便了解我们在量子信息学中对量子力学有哪些独特的关注点。

§1.3.1 量子力学基本假设

尽管关于量子力学的内容目前基本没有太大分歧，但在其基本假设的文字表述形式上存在一些略有不同的形式。比如有把下面第一、二条或第三、四条假设合并为一条的，顺序也会有区别，甚至也有不列出第五条的。我们这里大致遵循周世勋所编写的教材[11]中的划分方式，但顺序略有不同。

- 第一假设：物理体系的状态被一个波函数（ψ）完全描述。

为了保证ψ具有物理上可解释的意义（比如坐标表象中的$|\psi|^2$通常被理解为体系在空间某处能够被测量到的几率，故ψ被称为几率幅），它必须是连续、有限、单值、归一的。

从运动学（即描述物体如何运动）的角度来看，这个假设表明了量子力学与经典牛顿力学的最大分歧。在经典力学中，描述一个体系的最基本的量是它的空间坐标$\boldsymbol{r}$。一旦知道了$\boldsymbol{r}$对时间t的依赖关系，那么分别对$\boldsymbol{r}$求关于时间t的一阶、二阶导数就可得到体系的速度、加速度。体系的动量、动能以及其它所有的运动学参数原则上都可以进一步求出来。但在量子力学中，$\boldsymbol{r}$的理论地位退化成了仅仅是众多物理观测量中的一个。ψ才是具有物理客观实在性的最基本的运动学参量。如果知道了ψ，就可以推算出测量$\boldsymbol{r}$时会以何种几率得到何种结果。但知道$\boldsymbol{r}$却不能完全推出关于ψ的全部信息。同时，ψ也是完全的描述，即它在原则上足以对体系的所有运动学可观测量做出预言。而包括$\boldsymbol{r}$在内的这些可观测量的取值只有在对体系进行了相应的测量后才成为物理事实。至于未进行测量前讨论体系的位置$\boldsymbol{r}$是什么，在量子力学的主流理解看来在物理上是没有意义的。这正是量子力学与传统观念背离最明显的地方。像爱因斯坦这样的人物也始终不愿接受这一点。然而至今为止的所有相关物理实验却一次又一次地证实量子力学确实是正确的。

然而，必须注意几率幅ψ却是物理上不能被直接测出的，能够测出的只是几率$|\psi|^2$。那么，ψ是由什么决定的呢？下面这条假设做出了回答。

• 第二假设：波函数 ψ 满足薛定谔（Schrödinger）方程（非相对论近似下）：

$$\mathrm{i}\hbar\frac{\partial}{\partial t}\psi = \hat{H}\psi \tag{1.1}$$

式中 i 是虚单位，$\hbar \equiv h/2\pi$，$h \sim 6.63 \times 10^{-34}$ 焦/秒是普朗克（Planck）常数，$\hat{H}$ 叫做这个系统的哈密顿量（Hamiltonian）。

值得特别注意的是薛定谔方程是一条线性方程。即如果已知 ψ_1、ψ_2 都是满足该方程的解，那么它们的任意线性叠加 $\psi \equiv c_1\psi_1 + c_2\psi_2$ 仍然是方程的解（当然，为了同时满足第一假设中关于 ψ 的归一化要求，叠加系数 c_1、c_2 仍需遵从一定的条件）。因此，量子力学允许体系处在两种甚至更多种状态的线性叠加上。该结果也常被称为态叠加原理。这里我们看到，它并不是一个独立的新的基本原理，而是量子力学第二假设的必然结果。它是我们今后在量子计算和量子密码术中都必须用到的一个非常重要的部分。如果一个量子算法或量子密码术没有用到态叠加原理，那么它就极有可能不是真正量子的，而是存在等价的经典形式，不具备量子效应带来的优越性。

这条假设表明了量子力学与经典力学在动力学（即解释物体为何运动）上的不同。经典力学关于动力学的基本假设是牛顿第二定律 $F = ma$，而加速度 a 来源于 $\boldsymbol{r}$，因此 F 就是决定 $\boldsymbol{r}$ 的最基本的动力学参量。但在量子力学的层面 $\boldsymbol{r}$ 不再是最基本的运动学参量，因此 F 也不再是基本量了。在动力学角度完全决定 ψ 的基本量现在变成了 $\hat{H}$。那么 $\hat{H}$ 又是怎样得来呢？

• 第三假设：每一个力学量都对应于一个厄米（Hermite）算符。

这里力学量又被称为可观测量或守恒量，就是可以通过一个物理上能够实现的过程得到测量结果的量。如果按照海森堡对量子力学的表示形式把一个量用矩阵 M 来代表，那么这条假设的意思就是说只有当 M 是厄米矩阵（即 $M = M^+$，这里“+”表示厄米共轭，就是把 M 的每个矩阵元都取复共轭，再把整个矩阵转置）时，相应的量才是物理上可以测量的。

$\boldsymbol{r}$ 就是这样的一个力学量，它对应的数学形式就是 $\boldsymbol{r}$ 本身。其它常见的力学量的数学形式还有动量 $\hat{p} = -\mathrm{i}\hbar\nabla$，和上面的哈密顿量 $\hat{H} = \hat{p}^2/2m + V$ 等。有了与一个力学量 F 相应的算符 $\hat{F}$，就意味着可以通过计算 $\int_{-\infty}^{\infty}\psi^*\hat{F}\psi\mathrm{d}\boldsymbol{r}$ 求得在对由 ψ 描述的系统测量 F 时，预期能够得到的平均值。其中哈密顿量的预期测量平均值就对应于系统的能量。

• 第四假设：若力学量 F 的正交完备本征函数系是 $\{\phi_n\}$（即集合 $\{\phi_n\}$ 包含了所有满足 $\hat{F}\phi_n = \lambda_n\phi_n$（$\lambda_n$ 为常数）的函数 ϕ_n，且对于不同的 n，各 ϕ_n 互相正交），ψ 可以表成 $\psi = \sum_n c_n\phi_n$，则在态 ψ 中测 F 得到第 n 个结果的几率是 $|c_n|^2$。

这个假设也叫做测量公设。它表明如果ψ本来不处在F的一个本征态ϕ_n上、而是多个本征态的叠加，那么对它进行F的测量前，不能确定地对能得到哪一个测量结果做出预言，只能预言得到每一个结果的几率。这被称作量子测量的不确定性(quantum uncertainty)。更重要的是，一旦进行测量，这个量子态就会受到干扰，从而损失掉关于叠加系数c_n的信息。因此如果ψ由一方制备，而测量由另一方进行，那么就会造成双方的信息不对称，产生出一定的秘密信息。以后我们会看到，这在量子密码术中将会起到至关重要的作用。而ψ可以不处在F的本征态上，正是这个现象的关键。它意味着在量子的世界，各种可观测量可以有着不同的本征函数系。换句话说，量子力学允许存在相互不对易的可观测量。由于测量时会对量子态产生干扰从而丢失原来的信息，在对一个量子系统先后测量互不对易的几个可观测量时，先测哪个量、后测哪个量，其顺序会影响到测量结果的平均值。这就是著名的海森堡不确定原理（uncertainty principle，旧译测不准原理）。因此，测量公设、量子测量的不确定性、测不准原理实际上是同一个基本假设的不同表述形式。是否用到了关于相互不对易的可观测量的测量，是一个密码协议是否充分利用了量子力学的关键，往往会直接决定该协议是否具有量子密码术那种超越经典密码术的安全性。

- 第五假设：即全同性原理：系统内任意两个全同粒子交换，不会改变系统的状态。

它的意思是，如果一个多粒子组成的量子体系的总体波函数由$\psi(\boldsymbol{r}_1,\boldsymbol{r}_2,\boldsymbol{r}_3,\cdots)$描述，其中$\boldsymbol{r}_1,\boldsymbol{r}_2,\boldsymbol{r}_3,\cdots$标识着不同的粒子，那么交换其中任意两个粒子（比如由$\boldsymbol{r}_1$和$\boldsymbol{r}_2$标识的两个），体系的几率分布$|\psi|^2$保持不变。因此几率幅最多只能改变一个符号，即：

$$\psi(\boldsymbol{r}_1,\boldsymbol{r}_2,\boldsymbol{r}_3,\cdots) = \pm\psi(\boldsymbol{r}_2,\boldsymbol{r}_1,\boldsymbol{r}_3,\cdots) \tag{1.2}$$

式中如果取“+”号，那么这种粒子被称为玻色（Bose）子，包括光子、处于基态的氦原子等自旋为$\hbar$的整数倍的粒子。如果取“-”号，则被称为费米（Fermi）子，包括电子、质子、中子等自旋为$\hbar/2$的奇数倍的粒子。这其实意味着在量子层面，粒子是不可以被明确地标识的。我们不可能看得出一个电子与另一个电子“长”得有什么不同，而不像经典物理世界中，我们可以在乒乓球上写上号码来区别它们。因此这一假设也称为全同粒子的不可分辨性。

上述五条假设一起构成了量子力学的完整公理体系，彼此互相联系，缺一不可。因此我们不能说哪条假设不重要。但从应用角度，有着明显的直接作用且同时又会被忽略的往往是第二和第四假设。因此学习量子算法和量子密码术的思路关键，就是要特别注意把握这两条假设是如何把量子力学的特性转化为优越性的。第五假设在大部分时间我们似乎不会直接涉及，但在§7.2.1结尾我们会再一次提到它。

§1.3.2 常用符号和公式

• 量子比特：

量子力学第二假设在信息学中的应用，直接的效果首先就是量子比特（qubit）概念的出现。在经典的世界里，一个比特（bit）简单地说就是可以用一位二进制数表示的信息。因此它只有两个取值，可以记为“0”或“1”。经典比特的一个最浅显特征就是0和1这两种状态是正交的，即0就是0，1就是1，写在纸上（或记录在其它“经典”材料上）的0不可能被看做是1，1也不可能被看做是0。然而在量子的层面，量子力学第二假设中的薛定谔方程是线性的，导致了态叠加原理的出现。因此如果用 ψ_0 表示与经典的0相对应的量子系统的状态，ψ_1 表示与1相对应的量子状态，那么它们的任意线性叠加 $\psi = \alpha\psi_0 + \beta\psi_1$ 仍然是物理上允许存在的解，只要叠加系数 α 和 β 满足归一化条件 $|\alpha|^2 + |\beta|^2 = 1$。也就是说，一个量子比特原则上可以有无穷多个允许取值。所以，与以经典比特为处理单位的经典计算机不同，量子计算机如果以量子比特为处理单位，那么一个存储单元就可以存储无穷多个值。这是导致量子计算机超越经典计算机的一个首要条件。

• 狄拉克符号与矩阵形式：

今后我们通常使用狄拉克（Dirac）符号来表示态和变换。比如，状态 ψ_0 和 ψ_1 分别写为右矢 $|0\rangle$ 和 $|1\rangle$，而它们的线性叠加态 $\psi = \alpha\psi_0 + \beta\psi_1$ 则写为 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$。但是，这种写法虽然简洁，在遇到具体计算时采用海森堡形式（即矩阵形式）会更为准确。以qubit（即物理上的二能级系统）为例，按照一般习惯，$|0\rangle$ 和 $|1\rangle$ 的矩阵形式表为2阶向量

$$|0\rangle \to \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle \to \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.3}$$

则

$$|\psi\rangle \to \alpha\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{1.4}$$

而态 ψ 的复共轭 ψ^* 则用左矢表示，矩阵形式为

$$\langle\psi| \to [\alpha^* \quad \beta^*] \tag{1.5}$$

左矢 $\langle\psi|$ 与右矢 $|\phi\rangle$ 的乘积叫做它们的内积，通常简记为 $\langle\psi|\phi\rangle$，即省略中间的一条竖线。

• 直积：

如果系统不是qubit而是具有更多的能级，则需要用更高阶的向量来表示。但由于多能级系统在数学上等价于多个二能级系统的复合（比如一个四能级系统显然可

以看做是两个二能级系统构成的总体），因此最终总可以通过多个 qubit 的直积形式来描述。具体地说，2 × 2 矩阵的直积定义为如下运算：设有两个矩阵

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}, \quad B = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} \tag{1.6}$$

则它们的直积是

$$A \otimes B \equiv \begin{bmatrix} A_{11}B & A_{12}B \\ A_{21}B & A_{22}B \end{bmatrix} = \begin{bmatrix} A_{11}B_{11} & A_{11}B_{12} & A_{12}B_{11} & A_{12}B_{12} \\ A_{11}B_{21} & A_{11}B_{22} & A_{12}B_{21} & A_{12}B_{22} \\ A_{21}B_{11} & A_{21}B_{12} & A_{22}B_{11} & A_{22}B_{12} \\ A_{21}B_{21} & A_{21}B_{22} & A_{22}B_{21} & A_{22}B_{22} \end{bmatrix} \tag{1.7}$$

更高阶的矩阵或向量的直积可依此类推。所以，一个四能级系统的一个态 $\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$ 可以表为 $\begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix}$。因此下面我们一般只研究 qubit 的情形。

在使用狄拉克符号表示多个系统共同组成的量子态时，为了简便，在不引起混淆的前提下经常会省掉直积符号 ⊗，比如 $|\psi\rangle \otimes |\phi\rangle$ 可以简记为 $|\psi\rangle|\phi\rangle$ 或 $|\psi\phi\rangle$。

• 变换算符：

设变换操作 T 把态 ψ 变为 $\psi' = T\psi$，狄拉克符号记为 $|\psi'\rangle = T|\psi\rangle$，则矩阵形式为（仍以 qubit 为例）

$$\begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = \begin{bmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{1.8}$$

若变换 T 存在逆变换 T^{-1}，即 $\psi = T^{-1}\psi'$，则狄拉克符号记为 $|\psi\rangle = T^{-1}|\psi'\rangle$，矩阵形式为（注意这里 T^{-1} 是指 T 的逆矩阵而不是倒数）

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} (T^{-1})_{11} & (T^{-1})_{12} \\ (T^{-1})_{21} & (T^{-1})_{22} \end{bmatrix} \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} \tag{1.9}$$

最普通的变换当然是恒等变换（identity transformation），通常记为 I 或 E，其作用的结果是 $I\psi = \psi$ 即保持态 ψ 不变，相应的矩阵是单位矩阵 $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$。

而物理上可以实现的可逆变换必须是幺正变换（unitary transformation），即满足 $T^{+}T = I$（注意与厄米算符 $T^{+} = T$ 相区别）。这是因为波函数必须满足归一化条件，故有

$$1 = \langle \psi' | \psi' \rangle = (T|\psi\rangle)^{+}(T|\psi\rangle) = \langle \psi | T^{+}T | \psi \rangle \tag{1.10}$$

• 投影测量：

满足 $P^2 = P$ 的算符叫做投影算符。它是最常见的一种测量。例如把一个态投影到 $|0\rangle$ 态或 $|1\rangle$ 态上的投影算符分别是

$$\begin{aligned} P_0 &\equiv |0\rangle\langle 0| = \begin{bmatrix} 1 \\ 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \\ P_1 &\equiv |1\rangle\langle 1| = \begin{bmatrix} 0 \\ 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned} \tag{1.11}$$

当一个投影算符（例如 P_0）作用在一个量子系统上发现投影成功（即与该投影算符相应的物理装置有表示“测到”的反应），那么该量子系统无论初始状态如何，这时就变到了与该投影算符相应的量子态上（例如 $|0\rangle$）。这一过程通常叫做坍缩（collapse）。值得指出的是，目前有些量子诠释（quantum interpretation）理论认为不存在坍缩过程，当一个初始状态 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ 在 P_0 作用下投影成功时，与 $\beta|1\rangle$ 有关的信息并没有丢失，而是以一定方式保存在了测量者所没有感知到的某处。但是，由于这些诠释理论与认为有坍缩过程的诠释理论在处理具体的物理实验时都给出相同的结果，因此本书中我们暂且搁置坍缩是否真实物理过程这一争议，为简便起见，一律把测量之后发生的过程用坍缩这个名词来称呼。

注意到 $P_0 + P_1 = I$ 和 $P_0P_1 = 0$，像这样求和等于单位矩阵的一组互相正交的测量，我们称之为一组完备测量（complete measurement）。其特点是如果施加其中一个测量，结果发现投影不成功，则相当于把系统向剩下的其它测量算符所对应的 Hilbert 空间作投影成功。例如如果试图把一个 qubit 用 P_0 投影到 $|0\rangle$ 态，但发现不成功，则其结果等价于用 P_1 把这个 qubit 成功地投影到了 $|1\rangle$ 态上。对于更高阶的量子系统，互相正交的投影算符（即 $P_iP_j = \delta_{ij}P_i$）会不止两个。设 $\{P_1, P_2, P_3, \cdots, P_n\}$ 构成了一组完备测量，则当用 P_1 投影不成功时，系统就坍缩到了 $\{P_2, P_3, \cdots, P_n\}$ 所对应的 Hilbert 空间，即相当于用算符 $P_2 + P_3 + \cdots + P_n$ 投影成功。我们以后在讲到量子封印时（例如 §5.4.5 的式（5.10））会更具体地涉及这种投影。

一组完备测量里的各个投影算符的本征态合在一起，就构成一组测量基，比如与 P_0 和 P_1 对应的测量基记为 $\{|0\rangle, |1\rangle\}$。

• 运算规则：

如前所述，遇到算符和态之间进行运算时，以矩阵形式来表示、并按照矩阵运算的规则进行处理是最准确的。但习惯之后，从狄拉克符号形式也往往可以直接运算。比如，由矩阵形式不难验证

$$\langle 0|0\rangle = \langle 1|1\rangle = 1, \langle 0|1\rangle = \langle 1|0\rangle = 0 \tag{1.12}$$

所以

$$P_0|0\rangle = (|0\rangle\langle 0|)|0\rangle = |0\rangle(\langle 0|0\rangle) = |0\rangle,$$
$$P_1|0\rangle = (|1\rangle\langle 1|)|0\rangle = |1\rangle(\langle 1|0\rangle) = 0 \tag{1.13}$$

它表示 $|0\rangle$ 态有100%的几率能被投影到 $|0\rangle$ 态上，而被投影到 $|1\rangle$ 态上的几率为零。同样可得

$$P_0|1\rangle = 0, \quad P_1|1\rangle = |1\rangle \tag{1.14}$$

对于态 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$，有

$$P_0|\psi\rangle = |0\rangle\langle 0|\psi\rangle = (|0\rangle\langle 0|)(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle\langle 0|0\rangle + \beta|0\rangle\langle 0|1\rangle = \alpha|0\rangle,$$
$$P_1|\psi\rangle = |1\rangle\langle 1|\psi\rangle = (|1\rangle\langle 1|)(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle\langle 1|0\rangle + \beta|1\rangle\langle 1|1\rangle = \beta|1\rangle \tag{1.15}$$

这意味着如果试图把 $|\psi\rangle$ 投影到 $|0\rangle$ 上，则投影成功的几率幅是 α。而一旦投影成功，则 $|\psi\rangle$ 在测量之后坍缩到了 $|0\rangle$ 态上；如果投影不成功，则 $|\psi\rangle$ 坍缩到了 $(|\psi\rangle - \alpha|0\rangle) \sim |1\rangle$ 态上。类似地，$|\psi\rangle$ 成功投影到 $|1\rangle$ 上的几率幅是 β，一旦投影成功，则 $|\psi\rangle$ 坍缩到了 $|1\rangle$ 态上，否则 $|\psi\rangle$ 坍缩到了 $|0\rangle$ 态上。

● 广义测量：

近来量子信息方面的文献上越来越多地出现一种简称为 POVM（意即 positive operator valued measure）测量的概念。它不必须满足 $P^2 = P$ 因此不一定是投影算符，故被称为广义测量。其严谨的数学定义比较抽象，故这里不做提及。有兴趣的读者可参阅 Nielsen 和 Chuang 的著作[6]的 §2.2.6。而其物理含义则并不复杂。它是指当我们想知道一个量子系统 A 是不是处在某个特定的状态时，不是直接测量这个系统本身，而是先引入一个用于存储操作结果的附加量子系统 B，然后对整个复合系统 $A \otimes B$ 进行幺正变换，使得对系统 A 的各种测量结果以相互正交的态的形式被转存到了系统 B 里。如果我们想要取出结果，则只需在最后对系统 B 再作一个完整的投影测量即可。在这种情形下，施加在系统 A 上的那部分操作就叫做 POVM。由此可见，对任何系统进行的 POVM 都等价于对一个更大的系统作幺正变换、然后再对其中附加的系统进行投影测量。因此我们实际上只需研究幺正变换和投影测量，就足以处理所有的测量和操作。

下面通过一个具体例子来看一个系统上的测量是如何转化为一个更大的系统上的幺正变换的。设系统 A 处在状态 $|\psi\rangle_A = \alpha|0\rangle_A + \beta|1\rangle_A$ 上。如果直接用投影测量，则可以直接把投影算符 $P_{0A} \equiv |0\rangle_A\langle 0|$ 或 $P_{1A} \equiv |1\rangle_A\langle 1|$ 作用在 $|\psi\rangle_A$ 上。现引入一个附加系统 B，并把其初始状态制备成 $|\psi\rangle_B = |0\rangle_B$。然后用一个作用于整个复合系统 $A \otimes B$ 上的量子操作 T_{AB} 实现下列功能：如果用 P_{0A} 作用在 $|\psi\rangle_A$ 上能够投