HZ BOOKS
华章IT

人人可懂的量子计算

QUANTUM COMPUTING FOR EVERYONE

CHRIS BERNHARDT

【美】克里斯·伯恩哈特 著

邱道文 周旭 等译

机械工业出版社
China Machine Press

QUANTUM COMPUTING FOR EVERYONE

人人可懂的量子计算

CHRIS BERNHARDT

【美】克里斯·伯恩哈特 著

邱道文 周旭 萧利刚
林一诺 朱祎康 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

人人可懂的量子计算 /（美）克里斯·伯恩哈特（Chris Bernhardt）著；邱道文等译 . —北京：机械工业出版社，2020.2
书名原文：Quantum Computing for Everyone

ISBN 978-7-111-64668-6

I. 人… II. ①克… ②邱… III. 量子计算机 IV. TP385

中国版本图书馆 CIP 数据核字（2020）第 023835 号

本书版权登记号：图字 01-2019-5653

人人可懂的量子计算

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：唐晓琳
责任校对：李秋荣
印　　刷：北京诚信伟业印刷有限公司
版　　次：2020 年 3 月第 1 版第 1 次印刷
开　　本：147mm × 210mm 1/32
印　　张：7.875
书　　号：ISBN 978-7-111-64668-6
定　　价：59.00 元

客服电话：（010）88361066 88379833 68326294
投稿热线：（010）88379604
华章网站：www.hzbook.com
读者信箱：hzit@hzbook.com

•• 译者序 ••

诺贝尔奖获得者 Feynman 于 20 世纪 80 年代初指出使用经典计算机难以有效模拟量子系统的演化，从而提出量子计算机的想法——遵循量子力学规律调控量子信息单元进行计算。1985 年，牛津大学的 Deutsch 建立了量子计算机的数学模型——量子图灵机，并提出量子 Church-Turing 命题：量子图灵机可以有效模拟现实中的任何计算模型。因此，量子计算不仅是新的计算模式，更是人类对计算更深刻的认识。

理论上已经证明量子计算至少不比经典计算弱。第一个量子算法是 Deutsch 提出的。之后 Deutsch 和 Jozsa 于 1992 年提出了比经典算法有指数优势的量子算法解决 D-J 问题，其后 Simon 提出了比经典算法有指数优势的量子算法——Simon 算法。特别是，受 Simon 算法思想的启发，Shor 于 1994 年提出了大数分解的多项式时间量子算法，而目前所知道的经典算法分解大数都是指数时间的。1996 年 Grover 发现了与经典算法相比具有平方加速的量子搜索算法。可以说，Deutsch、Jozsa 和 Simon 首先给出了量子算法的基本设计过程，Shor 和 Grover 分别发现了量子算

法设计的两个基本方法：量子相位估计和振幅放大方法。2009 年，Harrow、Hassidim 和 Lloyd 提出了具有指数加速的 HHL 量子算法求解线性方程组。量子计算的硬件设计也在不断发展，特别是最近谷歌设计的 53 个比特的量子芯片——Sycamore，进一步显示了量子计算的优势。这或许也是发展通用量子计算机给人类带来实际应用的曙光。

21 世纪的今天，世界各国都意识到研究量子计算的重要性和可行性，从而纷纷发布各自的量子计算科技战略，争取实现有实际应用价值的“量子优势”。世界各高校也在大力发展量子计算学科。如今，量子计算已经成为大众应该了解和学习的知识之一。本书是 Chris Bernhardt 教授撰写的 ***Quantum Computing For Everyone*** 的中译本。原著共有九章，分别介绍了自旋，高等代数，自旋与量子比特，量子纠缠，Bell 不等式，经典逻辑，门和电路，量子门和电路，量子算法以及量子计算的作用，一般理工科本科学生都能读懂。中译本继承了原著者的思想和内容，旨在向读者介绍量子计算的基本知识，希望读者通过阅读本书对量子计算有基本的了解。

量子计算在我国引起了广泛重视，越来越多的高校和科研院所正在开展量子计算的研究，在理论和硬件方面已经取得了不少的成果。同时，各界的专家学者也关注和学习量子计算。虽然通用量子计算机的研发远未成熟，而且理论上还需要大力发展新的量子算法和量子计算模型，但是我们已经看到了量子计算机的发展充满希望。本书以尽可能浅显的方式向一般读者介绍量子计算的基本知识，译者希望本书能引起更多读者对量子计算的兴趣，

吸引更多的人才投身于量子计算的研究之中。

邱道文

2019 年 11 月

于广州中山大学

•• 前　言 ••

本书的目的是介绍量子计算，使得任何一个熟悉高中数学知识和愿意投入一点时间的人都能理解。我们将会学习量子比特、量子纠缠、量子隐形传态和量子算法，以及其他量子相关的主题。我们的目标不是对这些概念给出一些不明确的想法，而是使它们清晰明了。

量子计算经常出现在新闻中：中国通过隐形传态将一个量子比特从地球传送到一颗卫星上；Shor 算法使我们目前的加密方法面临风险；量子密钥分发将使加密再次变得安全；Grover 算法将加速数据检索。但这一切究竟意味着什么？这一切是如何运作的？所有这些都将在本书中得到解释。

不使用数学能做到这一点吗？如果我们想真正了解发生了什么，那就需要使用数学。量子力学的基本思想往往与直觉相悖。试图用文字来描述这些是行不通的，因为我们在日常生活中对它们没有经验。更糟糕的是，文字描述常常给人留下这样的印象：我们貌似理解了一些东西，而实际上我们还没有理解。好消息是，我们并不需要引入太多的数学知识。作为一名数学家，我的职责

是尽可能地简化数学（坚持绝对的本质）并给出基本的例子来说明它的用法与含义。也就是说，这本书可能包含你以前从未见过的数学概念，而且和所有的数学知识一样，新的概念一开始可能看起来很奇怪。重要的是不要忽略这些例子，而且要仔细阅读计算的每一步。

量子计算是量子物理与计算机科学的完美融合，将20世纪物理学中一些最令人惊叹的观点融入一种全新的计算思维方式中。量子计算的基本单位是量子比特。我们将看到什么是量子比特以及测量量子比特时会发生什么。一个经典比特要么是0，要么是1。如果是0，我们测量它，得到0；如果是1，我们测量它，得到1。在这两种情况下，比特都保持不变。量子比特的情况则完全不同。一个量子比特可能是无限多个状态中的某一个——0和1的叠加态，但是当我们测量它时，和经典情况一样，我们只得到两个值中的一个——0或1。测量会改变量子比特，一个简单的数学模型可以精确地描述这一切。

量子比特还可能纠缠。当我们对其中一个进行测量时，会影响另一个的状态。这是我们在日常生活中没有经历过的，但我们的数学模型完美地描述了这种现象。

这三个概念——叠加、测量和纠缠——是量子力学的核心。一旦我们理解了这些概念，就能知道如何在计算中使用它们。这正体现了人类的聪明才智。

数学家通常认为：证明是美丽的，而且经常包含意想不到的见解。对于我们将要讨论的许多主题，我有完全相同的看法。贝尔定理、量子隐形传态和超密编码，这些都是珍宝。纠错线路和

Grover 算法更是相当惊人的。

读完本书，你应该理解了量子计算的基本概念，并会看到一些巧妙而漂亮的结构。同时，你还将认识到量子计算和经典计算并不是两个截然不同的学科。量子计算是计算的一种更基本的形式——任何经典计算机可以计算的都可以在量子计算机上计算。计算的基本单位是量子比特，而不是比特。从本质上讲，计算就是量子计算。

最后应该强调的是，本书是关于量子计算理论的介绍。它是关于软件的，而不是硬件的。虽然我们在某些地方简要地提到了硬件，偶尔也会讨论如何在物理上纠缠量子比特，但这些只是题外话。这本书讲的不是如何构建量子计算机，而是如何使用量子计算机。

以下是对这本书内容的简要描述。

第 1 章。经典计算的基本单位是比特。比特可以表示为处于两种可能状态之一的任何东西，标准例子是一个可以打开或关闭的电子开关。量子计算的基本单位是量子比特。这可以用电子的自旋或光子的偏振来表示，但自旋和偏振的性质对我们来说并不像开关打开或关闭那样熟悉。

我们先来看看自旋的基本性质。从奥托·斯特恩（Otto Stern）和瓦尔特·格拉赫（Walther Gerlach）的经典实验开始，他们在实验中研究了银原子的磁性。我们可以看到在不同方向上测量自旋会发生什么。测量会影响量子比特的状态。我们还会解释与测量相关的随机性。

该章的结论是，类似于自旋的实验可以用偏振滤光片和自然

光来完成。

第 2 章。量子计算基于线性代数。幸运的是，我们只需要一小部分概念。该章介绍我们需要的线性代数知识，并说明在后面的章节中如何使用这些知识。

我们将介绍向量、矩阵、如何计算向量的长度以及如何判断两个向量是否垂直。首先介绍向量的初等运算，然后介绍矩阵是如何同时进行这些运算的。

起初这些知识的作用并不明显，但确实有用。线性代数是量子计算的基础。由于本书其余部分使用了这里介绍的数学知识，因此需要仔细阅读。

第 3 章。该章介绍前两章是如何联系在一起的。线性代数给出了自旋或偏振的数学模型，这使我们能够定义量子比特，并准确地描述测量时会发生什么。

接下来书中举了几个在不同方向上测量量子比特的例子。最后介绍量子密码学，并描述 BB84 协议。

第 4 章。该章描述两个量子比特纠缠的含义。使用文字很难描述纠缠，与之相对，使用数学描述则很简单。张量积是一种新的数学思想，这是将单量子比特组合成多量子比特最简单的方法。

虽然纠缠的数学描述很直观，但我们在日常生活中并不会接触到。当测量一对纠缠量子比特中的某一个时，会影响另一个。阿尔伯特·爱因斯坦（Albert Einstenin）不喜欢这种现象，并称之为“幽灵般的超距作用”。我们会看几个例子。

该章最后指出，我们不能使用纠缠来实现超光速通信。

第 5 章。我们看看爱因斯坦对纠缠的担忧，以及隐变量理论

能否保持定域实在性。我们研究贝尔不等式的数学原理——这是一个显著的结果，它提供了一种实验方法来确定爱因斯坦的论点是否正确。虽然贝尔当时认为爱因斯坦的观点可能会被证明是正确的，但是爱因斯坦的观点是错误的。

阿图尔·埃克特（Artur Ekert）意识到，测试贝尔不等式的装置还可以用于生成密码学中使用的安全密钥，并同时测试是否存在窃听者。在该章的最后，我们描述了这种加密协议。

第 6 章。该章从计算的标准主题开始：比特、门和逻辑。然后简要地介绍可逆计算和爱德华·弗雷德金（Edward Fredkin）的想法。我们证明了 Fredkin 门和 Toffoli 门都是通用的——你可以仅使用 Fredkin 门（或 Toffoli 门）来构建一台完整的计算机。最后介绍 Fredkin 的台球计算机。尽管这并不是书中余下内容真正需要的，但它十足的独创性值得介绍。

这台计算机是由相互碰撞的球和很多墙组成的。它使人联想起粒子之间的相互作用。这激发了理查德·费曼（Richard Feynman）对量子计算的兴趣，费曼写了该领域最早的一些论文。

第 7 章。该章开始学习使用量子电路进行量子计算，并定义了量子门。我们将看到量子门如何作用于量子比特，并意识到我们一直在使用这种思想。我们只需要改变观点：不再认为正交矩阵作用于测量装置，而是作用于量子比特。我们还证明了一些有关超密编码、量子隐形传态、克隆和纠错的惊人结果。

第 8 章。这可能是最具挑战性的一章。我们会看到一些量子算法，并看到它们与经典算法相比计算的速度有多快。为了讨论算法的速度，我们需要引入复杂性理论中的思想。我们定义了查

询复杂性后，就开始学习三个量子算法，并证明它们的查询复杂性比经典算法的更低。

量子算法揭示了正在解决的问题的基本结构，它不仅仅是量子并行的思想——把输入放进所有可能状态的叠加中。该章介绍了最后一部分数学知识——矩阵的 Kronecker 积。实际上，这部分知识的困难源于我们正在以一种全新的方式进行计算，而我们并没有使用这些新思想来解决问题的经验。

第 9 章。最后一章着眼于量子计算将对生活带来的影响。我们首先简要描述两个重要的算法，一个是彼得·肖（Peter Shor）发明的，另一个是洛夫·格鲁弗（Lov Grover）发明的。

Shor 算法提供了一种将大数分解为质因数的方法。这似乎并不重要，但我们的互联网安全依赖于分解质因数是个难以解决的问题。能够分解大质数的乘积威胁到我们当前计算机之间的安全交易。可能还要等一段时间，我们才能拥有足够强大的量子计算机来分解目前正在使用的这些大数，但这一威胁是真实存在的，而且它已经迫使我们思考如何重新设计计算机之间的安全对话方式。

Grover 算法适用于特殊类型的数据检索。我们展示了它是如何在一个小样例中工作的，并说明了它是如何在一般情况下工作的。Grover 算法和 Shor 算法都很重要，不仅因为它们可以解决问题，还因为它们引入了新思想。这些基本思想正在被纳入新一代算法中。

学习算法之后，我们转个话题，简要地看一下如何使用量子计算来模拟量子过程。究其本质，化学就是量子力学。经典计算

化学的工作原理是利用量子力学方程，并用经典计算机进行模拟。这些模拟是近似的，忽略了细节。这种方法在很多情况下都很有效，但在某些情况下就行不通了。在这种情况下，你需要这些细节，而量子计算机应该能够提供。

该章还简要地介绍了实际机器的构建。这是一个快速发展的领域，第一批机器正在出售，“云”上甚至有一台人人都可以免费使用的机器。看来我们很快就会进入量子霸权时代。（我们会解释这意味着什么。）

本书的结论是，量子计算不是一种新型的计算，而是对计算本质的发现。

•• 致　　谢 ••

我非常感谢许多人对本书出版提供的帮助。Mart Coleman、Steve LeMay、Dan Ryan、Chris Staecker 和三位匿名审稿人非常仔细地阅读了各版原稿，他们的建议和修正使这本书得到了极大的改进。我还要感谢 Marie Lee 和她在 MIT 出版社的团队，感谢他们所有人的支持和努力，将一份粗略的提案变成了这本书。

•• 目　　录 ••