科学、科普和科幻的关系
——从《量子计算和量子信息》谈起

姬　扬

(中国科学院半导体研究所　100083)

量子信息和量子计算是21世纪最热门的一个研究领域，吸引了公众的很多注意，出版了科学论文和著作，科普文章和新闻，甚至还有很多科幻小说和类似于科幻的报道。这里我想借用2000年出版的一本著名的教科书《量子计算和量子信息》，谈谈科学、科普和科幻的关系。简单地说，科学文章的读者是科技工作者，讲究的是严谨负责，科普文章的读者是普通民众，需要吸引他们的注意力，这就必然要对一些细节进行取舍，不合适的舍弃就有可能使得科学变成了科幻，甚至是玄幻。

信息处理伴随着人类的整个历史，计算是最基本的信息处理手段之一。计算的历史很长，从手指到竹筹，从算盘到计算机，人们一直在寻求提高计算能力的方法。电子计算机的诞生还不到80年，但是计算机已经显著地改变了我们的研究和生活。

由于半导体科技的“摩尔定律”，计算机的计算能力一直在高速发展。1946年，第一台通用电子计算机ENIAC每秒钟可以进行5000次加减法；1954年，第一台晶体管化的计算机TRADIC每秒钟可以执行1百万次逻辑操作；1976年，Cray-1超级计算机的运算速度达到了2.5亿次；2018年，我国的“天河三号”超级计算机更是达到了每秒钟120亿亿次，处于世界领先的水平。人类的信息处理能力达到了空前的高度，在天气预报、材料设计、电磁仿真和生物医药等应用领域大显身手。

然而，随着“摩尔定律”的趋于终结，这种经典计算机的计算能力将达到极限，还有很多问题不能求解，例如，量子体系的演化问题，密码协议的破解问题，等等。因此，关于量子计算机的讨论也就越来越多，逐渐进入公众的视野了。

量子计算机以“量子比特”作为信息单元，利用量子力学规律调控“量子比特”来进行计算，由于“量子力学叠加性”，量子计算机的计算效率可能比经典计算机更高、处理问题的速度更快。20世纪80年代初期，贝尼奥夫(P. Benioff)和费恩曼(R. P. Feynman)先后独立地提出了量子计算的概念；1985年，D. Deutsch提出量子图灵机的概念；1994年，肖尔(P. Shor)提出了一种利用量子傅里叶变换的量子算法，可以高效率地进行大数的质数分解，用时比经典计算机少得多，从而破解信息安全领域常用的RSA公钥加密算法。1996年，格罗弗(Lov Grover)提出了量子搜索算法，可以平方根地加速无序数据库的搜索，不仅降低了AES等对称密码的安全性，而且可以加速求极值和人工智能等问题。这两个量子算法的提出是量子计算的突破，推动量子计算成为持续的国际研究前沿，吸引了众多的科学家关注量子计算这个新领域，认真考虑如何建造真正的量子计算机。正是在这个背景下，剑桥大学出版社在2000年出版了迈克尔A.尼尔森(Michael A. Nielsen)和艾萨克L.庄(Isaac L. Chuang)的《量子计算和量子信息》，系统地介绍了这个新兴领域的基本知识和主要成果，清华大学出版社在2003年出版了中译本，分为量子计算部分和量子信息部分的上下两册。

这是一本很好的教科书，体现在这么几个方面：是一本很有趣的书，虽然出版于大概20年前，但

是当前关于量子计算和量子信息的很多讨论，似乎并没有逃出这本书讨论的范围，被称为量子信息的“圣经”；它更多是从数学的角度来考虑量子计算和量子信息，写得很严谨，很像一本数学教材，还有很多练习题；它是这方面最早的教科书之一，出版3年就被译为中文，2010年还出版了10周年特别版；近20年来的很多研究论文和综述文章都引用了这本书，在最近出版的关于这个领域现状的报告《量子计算：现状和未来》里，第一页就引用了这本书。

这本书分为基本概念、量子计算和量子信息三个部分，共有十二章，以及五个特别数学化的附录。在每一章后面，都有“历史和进一步阅读的材料”，为感兴趣的读者指出了进一步学习的方向。

在《基本概念》这个部分里，第1章《引言和概述》介绍了量子计算和量子信息的历史和未来发展方向，既介绍了量子比特、量子计算、量子算法和量子信息及其实验处理，也是对全书内容的概括总结，我觉得是一篇非常好的科普文章。接下来的两章《量子力学引论》和《计算机科学简介》，是学习本书的基本知识基础。

在《量子计算》这个部分里，第4章《量子线路》讲述了量子计算的基本原理和单量子比特的运算，以及受控运算、测量和通用量子门，介绍了量子线路的基本模型以及量子计算的通用语言，最后介绍了量子计算如何应用于仿真实际的量子系统。第5章《量子傅里叶变换及其应用》介绍量子傅里叶变换及其在一些具体问题中的应用，包括求周期问题、离散对数问题、隐含子群问题，以及大名鼎鼎的Shor算法(用于大数的质数分解)。第6章《量子搜索算法》讲的是著名的Grover算法及其在数据库搜索、计数和NP完全问题加速中的应用，并且证明了这是适用于大多数非结构化问题的最优算法(达到了搜索速度的上限)。第七章《量子计算机：物理实现》是本书唯一与具体实验有关的一章，探讨了如何在现实中实现能够处理量子信息的机器，因为这样才有意义，“否则，该领域就只是引起数学上的好奇心而已”。首先介绍了具体实现必须考虑的各种折衷因素和指导性原则与，然后用5种不同的原型系统的例子来进行具体说明。当时还处于量子计算机的早期探索阶段，所以只有离子阱系统还是现在研究的热门，而超导量子比特仅仅在进一步阅读材料中提到。这一部分稍显落后，与现在的发展稍微脱节。对于专门从事相关研究的读者，需要阅读相关的综述来了解最新发展。

在《量子信息》部分一开始就指出，前面关于量子计算的讨论只涉及封闭量子系统的动力学过程，而现实世界中没有完全封闭的系统，肯定会与外部世界发生不希望有的交互作用(噪声，包括经典噪声和量子噪声)。为了建造有用的量子计算机，必须理解和控制这些噪声过程，《量子噪声和量子运算》、《量子信息的距离量度》和《量子纠错》这三章就是主要针对这个问题的。介绍了一些基本概念、编码方案和纠错原理，并得到了一个重要结论：当单个量子门的噪声低于某个常数阈值以后，就有可能有效地执行任意的大量子运算。第11章《熵与信息》综述了经典和量子信息理论熵的定义和基本性质，第12章《量子信息论》试图“用最纯粹的形式来描述量子信息论”，与前面3章一样，充满了大篇幅的数学论述，只是在最后一节，第12.6节《量子密码术》)才终于跟实验联系起来，讲述了量子密钥分发(QKD)协议及其实现。

在这本书出版后的将近20年里，量子计算和量子信息领域取得了很多重大进展，引起了民众的很多关注。量子信息是因为我国科学家在量子保密通讯方面取得了一些世界领先的成果，特别是“墨子号”卫星的成功发射和实验。而量子计算是因为加拿大量子计算公司宣称研发了全球第一款商用型量子计算机“D-Wave One”，随后美国IBM、微软和谷歌等企业投入巨资(最近华为、阿里巴巴也加入了这个行列)，希望能在短期内研制出量子计算机，而量子计算机的最大卖点就是有可能破译经典计算机无法破译的密码。最近几年，量子计算和量

子信息在我国都是很热门的话题，经常能在科学新闻和科普文章里看到。

在这种情况下，为什么要重提这本20年前的老书呢？部分原因是一些针对量子计算机的反对声音也变大了。特别是美国科学、工程和医学科学院(National Academies of Sciences, Engineering, and Medicine)去年发表的调查报告《量子计算：现状和未来》，明确地说在可预见的未来，基于通用量子门的量子计算机不可能破译RSA公钥密码(这一直是量子计算机的一个重大宣传亮点)。回过头来仔细再看这本书，就会发现这些问题早被就明确指出来了，以保证结论成立的强烈限制条件的形式出现，但是很多科学论文的导论对此都是一带而过，而绝大多数的科普文章更是好像忘却了限制条件的存在。为了实现量子傅里叶变换等量子操作或量子算法，必须能够对很多个量子比特进行保持相干性的、精确的量子操纵，这种操纵精度需要达到可以进行量子纠错的阈值，才有可能实现容错的量子计算。而量子纠错要求的错误阈值非常小，以目前IBM所公布的结果，需要大约1万个超导量子比特组合起来才能构造出Surface纠错码的一个逻辑量子比特，而目前只制备出不到100个超导比特。而且如何保证多个量子比特(而且个数真的很多)都能够做到这一点就更加困难了——如果不是完全不可能的话。现在关于量子比特个数的宣传很多，有几个、几十个乃至上千个的说法，但实际上他们谈论的都是“物理量子比特”，距离能够用在基于通用量子门的量子计算机上的“逻辑量子比特”(本书称为“数学量子比特”)的个数仍然是零(即使放宽些标准，也肯定是个位数)。

调查报告《量子计算：现状和未来》指出，在短时间内，具有完全纠错的量子计算机由于对资源要求巨大而很难实现，因此我们短期所能研制和使用的量子计算机是带有噪声的，即noisy intermediate-scale quantum(NISQ)的量子计算机。NISQ量子计算机有噪声，量子比特数在几百个或千个左右，还达不到容错量子计算机的能力，但是在一些问题上有可能解决现有经典计算机无法解决的难题。

现在看来，一些关于量子计算的宣传似乎已经超出了科普的范围，而是迈向了科幻、甚至玄幻。在这种情况下，再认真地看看这本20年前出版的量子计算教材，对照这些年里的调查、科普和宣传，必然能够让我们加深理解科学、科普和科幻之间的关系，提高我们的科学素质。

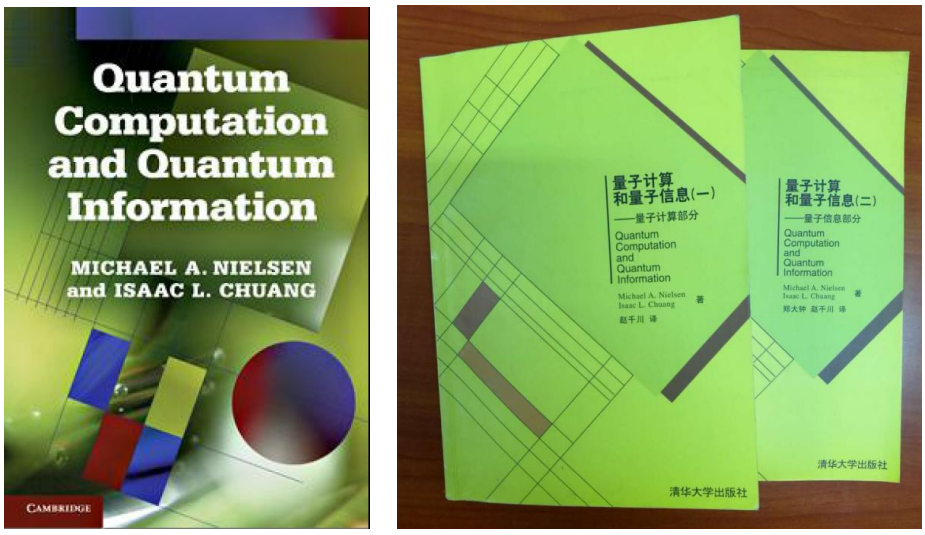

图1 《量子计算和量子信息》原著(2000年出版)及其中译本(2003年出版)

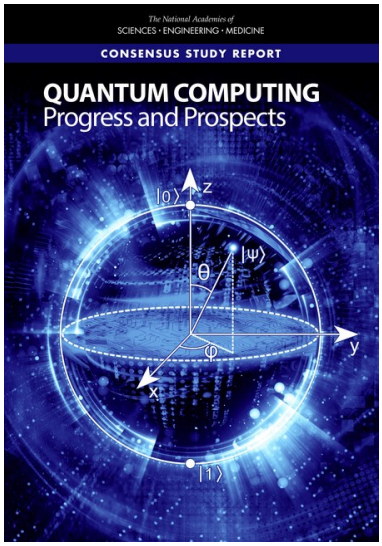

图2 《量子计算：现状和未来》(2019年出版)

参考文献

[1] Michael A. Nielsen, Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[2]《量子计算和量子信息(一)：量子计算部分》，Michael A. Nielsen, Isaac L. Chuang 著，赵千川 译，清华大学出版社，2003年；《量子计算和量子信息(二)：量子信息部分》，Michael A. Nielsen, Isaac L. Chuang 著，郑大钟 赵千川 译，清华大学出版社，2003年.

[3] National Academies of Sciences, Engineering, and Medicine. 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press.https://www.nap.edu/catalog/25196/quantum- computing- progress-and-prospects.

科苑快讯

海胆的牙齿可以自我打磨

海胆的刺，并非它多刺身体唯一锋利的部分。这种海洋生物5颗剃刀般的牙齿是自我磨削出来的——新的研究成果表明，科学家也许可以利用这一方法制造出几乎无需额外打磨的尖端工具。

海胆以嚼碎一切物体的能力闻名于世，它们利用自己的星状小嘴咬碎脆弱的海星、珊瑚礁，甚至岩石。科学家一直怀疑海星的瓷牙是自己磨削出来的，但是却无人能够说清它们是如何做到这点的。

为了找到答案，研究人员利用扫描电子显微术(scanning electron microscopy)拍摄粉红色海胆在一种由钻石制成的超硬材料上打磨牙齿的影像。

在精确分析了牙齿是怎样和在哪里磨削的3D影像后，还进行了多种机械测试——研究组发现，牙齿中的物质排列整齐，致使其只在一边磨削。这有助于它们保持各处的锋利边缘，他们在《物质》(*Matter*)杂志上做了报告。

在牙齿坚固的一面，有方解石纤维提供支撑壁。方解石物质在另一面形成易碎的斜板，在牙齿与海星、岩石摩擦时脱落，不断形成锋利的边缘。海胆的牙齿终生不断生长，所以这种磨损不会给牙齿带来太多损耗。

研究人员说，了解海胆的材料结构有助于科研人员和工程师制造出能够自己保持锋利的钻孔和切削工具。这不是海胆的星状小嘴首次为复杂工具的设计提供灵感——2016年，受到它们五颗牙齿的启发，工程师制造出一个爪状铲子，帮助太空探测设备采集沉积物样本。将这些新知识利用起来，未来的工程师可以从中获得更多的研究素材。

（高凌云编译自2019年9月18日www.sciencemag.org）