高等学校电子信息类“十三五”规划教材

西安电子科技大学研究生精品教材

量子信息学导论

Introduction to Quantum Information

许定国　编著

西安电子科技大学出版社
http://www.xduph.com

高等学校电子信息类“十三五”规划教材
本书获西安电子科技大学研究生精品教材项目资助

量子信息学导论

Introduction to Quantum Information

许定国　编著

西安电子科技大学出版社

内 容 简 介

量子信息学是近30多年发展起来的新型交叉学科，是量子力学与信息论、计算机科学、密码学、度量学等相结合的新兴研究领域。量子信息学主要涉及量子信息论、量子通信、量子计算、量子密码、量子模拟和量子度量等方面。

本书主要介绍量子信息学的基础理论、基本原理及其应用的主要成果。全书分为8章内容，第1章介绍量子信息学各主要领域的发展历史和现状以及量子信息学的性质、研究对象、内容、方法和意义，第2章介绍量子信息学的数学和物理基础，第3章介绍量子信息论的基本理论，第4章介绍量子密码术的方法和技术发展，第5章介绍量子通信及其量子通信网络的相关内容，第6章介绍量子算法和量子计算机的物理实现，第7章介绍现有的各种量子模拟方法，第8章介绍量子度量学及量子信息学在一些新领域的应用。

本书可以作为电子、信息、通信类各相关专业量子信息学课程的参考教材，也可供对量子信息学感兴趣的各类人员参考。

图书在版编目(CIP)数据

量子信息学导论/许定国编著. —西安：西安电子科技大学出版社，2015.11
高等学校电子信息类“十三五”规划教材

ISBN 978-7-5606-3805-8

Ⅰ. ① 量… Ⅱ. ① 许… Ⅲ. ① 量子力学—信息学 Ⅳ. ① O413.1

中国版本图书馆CIP数据核字(2015)第244549号

策划编辑 李惠萍
责任编辑 雷鸿俊
出版发行 西安电子科技大学出版社(西安市太白南路2号)
电 话 (029)88242885 88201467 邮 编 710071
网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com
经 销 新华书店
印刷单位 陕西华沐印刷科技有限责任公司
版 次 2015年11月第1版 2015年11月第1次印刷
开 本 787毫米×1092毫米 1/16 印张 17
字 数 399千字
印 数 1～3000册
定 价 30.00元
ISBN 978-7-5606-3805-8/O
XDUP 4097001-1

前　言

量子信息科学是量子力学与信息科学相结合而发展起来的一门新兴的前沿交叉学科。量子信息科学以微观粒子作为信息载体，进行操纵、存储和传输量子状态，利用量子现象实现经典信息科学所无法完成的功能。经过30多年的迅猛发展，量子信息科学无论在理论上还是在实验上都取得了重要突破，有些方面开始走向实际应用。如今，量子信息科学已经形成了量子计算、量子通信、量子密码、量子模拟、量子度量与量子信息论等主要研究领域，其研究内容十分丰富。

由于量子信息科学涉及量子力学、计算机科学、传统的通信科学、密码学和度量学，所用到的数学知识有概率论、数论、群论等，成为典型的多学科交叉科学。一些基本的物理问题到现在还不能给出明确的解释，譬如量子纠缠问题，虽然目前给人以困惑，但量子纠缠已经成为量子信息科学非常有用的资源，在量子通信、量子计算、量子度量等研究领域扮演着重要的角色。利用量子纠缠现象，人们已经实现了100多公里距离的量子态的隐形传送，实现了量子成像，更有中国的研究者创造出了量子照相机！量子信息城域网已经在世界多地建成并初步应用。虽然量子雷达实现的难度很大，但由于它在探测隐身目标方面的特殊功能，因此已成为世界各个技术与经济强国竞相开发的一个重要的技术研究领域。

量子信息科学从诞生到如今的30多年里迅猛发展，显示出十分广阔的科学和技术应用前景。随着量子信息科学的进一步发展，有望解决量子理论中的一些悬而未决的问题，促进量子理论的完善。量子信息科学在技术方面正在成为推动IT产业更新换代的动力。

作者从2007年起由于为本科高年级与研究生开设量子信息学讲座，开始了又一次艰难的学习历程，迫使作者认真学习了量子信息科学所涉及的大量的有关专业知识和文献资料，近几年又担任量子信息学课程的主讲教师，不断吸收整理国际量子信息科学最新研究进展成果，从中选取课程讲授材料，不断修改和更新讲稿，组织教学。本书就是在这些讲稿的基础上，经过几番补充修改形成的。书中有的内容直接引用了多位先驱者已经出版的著作中的内容，已在参考文献中列出，在此，谨向这些先驱者表示感谢并致敬。

本书内容共分8章。第1章为绪论，介绍了量子信息科学各主要研究领域

的发展历程，给出了过去30多年量子信息科学取得的主要研究成果。第2章为量子信息学的数学与物理基础，主要介绍了极式分解、奇异值分解、密度算符、量子纠缠等概念和理论。第3章为量子信息论基础，介绍了熵与量子信息的测度、香农编码定理和量子编码定理等，这些内容对于尚未涉足信息学的非通信专业的读者学习量子信息学是必要的。第4章为量子密码术，介绍量子密码的概念、量子密钥分配协议等内容。第5章为量子通信，介绍量子纠缠这一量子信息科学中极其重要的概念，以及量子纠缠态的性质、产生方法和测量原理及其在量子通信领域中的应用。第6章为量子计算基础，介绍量子比特概念、普适量子逻辑门工作原理、现有的几种量子算法，以及量子计算机物理实现的几种方案。第7章为量子模拟，介绍量子模拟器研究现状、量子模拟系统表示法、量子模拟的几个实例等。第8章为量子度量学，介绍光场压缩态、量子纠缠态这些量子领域特有的现象以及在量子测量中的应用，特别介绍了它们在量子成像、量子定位与量子雷达中的应用。

量子信息科学发展迅速，远没有定型，需要解决的问题很多，作者虽然尽心尽力想要在本书中给出量子信息科学的全貌，但由于作者的学识、水平有限，要达到理想境界确实是十分困难的。书中不妥、疏漏之处可能在所难免，敬请专家、同行指教。

最后，作者要特别指出，安毓英教授和杨志勇教授曾为“量子信息学”课程的设置以及教学大纲的制定和修订提出过许多良好的建议，多年来，他们的大力支持和鼓励，是作者坚持下来的动力；曾小东教授、刘继芳教授、王石语教授、邵晓鹏教授、王晓蕊教授、王学恩副教授、李军副教授、中国科学院西安光学精密机械研究所的张同意研究员、中国电科集团53所的吴养曹总工亦曾与作者就量子信息科学中的某些研究方面进行过多次有益的探讨和交流，使作者从这些活动中获益匪浅；西安电子科技大学物理与光电工程学院郭立新院长、李平舟副院长、杨光玮书记等领导以及金阳群、赵小燕、冯喆君、朱轩民、李兵斌、蒙文等老师给予作者很大的精神支持，研究生院领导也给以关心和支持，一些研究生帮忙校正了部分书稿，特别是孙怡莲女士帮忙输入了大部分书稿并在生活上给予作者很大关心；西安电子科技大学出版社的领导及李惠萍、雷鸿俊等编辑为本书的出版付出了艰辛的劳动。在此，作者特向相关单位及人员表示诚挚的感谢。

作　者

2015年6月

目　录

第1章 绪 论

量子信息学是量子力学、计算机科学、信息与通信工程学科相结合的一门交叉学科。量子信息领域的开拓者——美国IBM研究院的Bennett在2000年曾说："量子信息对经典信息的扩展与完善，就像复数对实数的扩展与完善一样。"量子信息学不仅将经典信息扩充延伸为量子信息，而且它直接利用量子态来表达信息、传输信息和储存信息。信息读出是通过对量子态的测量来实现的，信息处理过程就是对量子态实施幺正变换的过程，在整个过程中充分利用了量子态的叠加性、量子相干性、量子非局域性、量子纠缠性、量子不可克隆性等量子领域特有的性质。量子信息学的发展突破了许多经典信息技术的物理极限，从而实现电子信息技术无法做到的新的信息功能，如量子搜索、大数因式分解、量子保密通信、量子隐形传态、量子"鬼"成像等。量子信息领域几十年的研究业已表明，量子信息处理在提高运算速度、确保信息安全、增大信息容量和提高检测精度等方面具有潜在的巨大的应用价值，量子信息学的迅猛发展必将引起新的信息技术革命。量子信息学的内容主要包括量子计算、量子通信、量子密码、量子度量、量子模拟和量子信息物理基础等领域。本章以文献[1]为线索并参考相关资料对量子信息学各个主要领域的发展历史、研究对象、研究内容和研究现状全面进行描述，以使读者对量子信息学的全貌有一个整体的认识。

1.1 量子计算

1.1.1 量子计算的兴起

当今，电子计算机以其强大的信息处理功能深刻影响着人类社会的方方面面，它是经典图灵(Turing)机的物理实现，相对于正在发展中的量子计算机来说，它被称为传统计算机(或经典计算机、通用计算机)。它可以被描述为对输入信号序列按一定算法进行变换的机器，其算法由计算机的内部逻辑电路来实现。它有以下特点：

(1) 其输入态和输出态都是传统信号，若用量子力学的语言来描述，亦即：其输入态和输出态都是某一力学量的本征态，如输入二进制串行码0110110，用量子力学标记，就是$|0110110\rangle$，所有的输入态均相互正交。对于经典计算机不可能输入如下叠加态：$c_1|0110110\rangle+c_2|1101101\rangle$。

(2) 传统计算机内部的每一步变换都演化为正交态，而一般的量子变换没有这个性质，因此，传统计算机中的变换(或计算)只对应一类特殊集。

相应于经典计算机的以上两个限制，量子计算机分别作了推广。量子计算机的输入用一个具有有限能级的量子系统来描述，如二能级系统(称为量子比特(qubit))，量子计算机的变换(即量子计算)包括所有可能的幺正变换。因此量子计算机的特点为：① 量子计算机的输入态和输出态为一般的叠加态，其相互之间通常不正交；② 量子计算机中的变换为所

有可能的幺正变换。得出输出态之后，量子计算机对输出态进行一定的测量，给出计算结果。由此可见，量子计算对传统计算作了极大的扩充，传统计算是一类特殊的量子计算。量子计算最本质的特征为量子叠加性和量子相干性。量子计算机对每一个叠加分量实现的变换相当于一种经典计算，所有这些传统计算同时完成，并按一定的概率振幅叠加起来，给出量子计算机的输出结果。这种计算称为量子并行计算。

那么，能用经典计算机模拟量子力学系统吗？量子计算的概念又是如何提出的呢？

随着计算机科学的发展，史蒂芬·威斯纳在 1969 年最早提出“基于量子力学的计算设备”。而关于“基于量子力学的信息处理”的最早文章则是由亚历山大·豪勒夫(1973)、帕帕拉维斯基(1975)、罗马·印戈登(1976)和尤里·马尼(1980)发表的。史蒂芬·威斯纳的文章发表于 1983 年。20 世纪 80 年代一系列的研究使得量子计算机的理论变得丰富起来。人们研究量子计算机最初很重要的一个出发点是探索通用计算机的计算极限。1982 年，Richard Feynman 论证了用经典计算机模拟量子力学系统时，随着输入粒子数或自由度的增大计算机在时间和空间方面的资源消耗会呈现爆炸式的指数增加，即使一个完好的模拟所需的运算时间也变得相当可观，甚至是不切实际的天文数字。这对于任何经典计算机来说都不可能承受得起。可见，量子力学系统是无法在经典计算机上模拟的。

这一现象引起了 Feynman 的进一步思考，他推测，按照量子力学规律工作的计算机(量子计算机)有可能解决这样的困难，这就是最早的量子计算的思想。传统计算机靠控制集成电路来记录及运算信息，量子计算机则希望控制原子或小分子的状态，记录和运算信息。限于那个年代的实验技术，量子计算机在 20 世纪 80 年代多处于理论推导状态。

1985 年，David Deutsch 深入地研究了量子计算机是否比经典计算机更有效的问题，他定义了量子图灵机(见图 1.1)，描述了量子计算机的一般模型。量子图灵机的计算与经典图灵机计算的最大区别是：表征基本信息单元的比特是一个两能级的量子系统，它的状态由 Hilbert(希尔伯特)空间的基矢量叠加而成，不同于经典比特只能处于 0、1 两种可能，它不仅可以处于 0、1 两种状态，还可以处于 0 和 1 的任意叠加态；对信息的操控满足闭系统的量子力学演化规律，由薛定谔方程控制。这样一来，对 N 个量子比特的单次操纵，等效于同时对 2^N 个基矢量同时做了变换，这就是量子并行性。量子图灵机的运转带有天然的并行性，这是量子力学中的态叠加原理所赋予的。但是对于最后信息的读出过程，量子力学原理告诉我们只能读出这 2^N 种可能性中的一种，每种可能性出现的概率由演化后状态的基矢量前面的概率振幅决定。所以，原则上量子计算机是一种概率计算，人们通过对于最后随机输出结果的分析来求解问题的答案。这就证明，建立在量子力学原理基础上的量子算法对特定

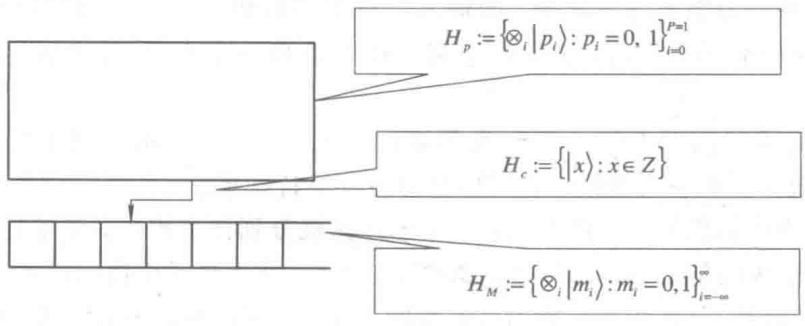


图 1.1 量子图灵机示意图

问题可以超越经典算法。这一证明反映出量子计算有解决经典计算机无法胜任的任务的可能。

开始人们并不能确信量子计算模式能够带来怎样的后果，转折性的事件发生在1994年，这一年贝尔实验室的专家Peter Shor发现了第一个具体的量子算法，它利用量子并行计算特性，在设想的量子计算机上用输入的多项式时间分解大数质因子，证明量子计算机能做出离散对数运算，理论上大大地降低了算法的计算复杂度，能应用于经典信息处理技术无法求解的NP(Non-Polynomial)难解问题，而且速度远胜传统计算机，因为量子计算机不像基于半导体的经典计算机只能记录0与1，它可以同时表示多种状态。如果把经典计算机比成单一乐器，那么量子计算机就像交响乐团，一次运算可以处理多种不同状况，因此，一个40比特的量子计算机，就能在很短时间内解开1024位的传统计算机花上数十年才能解决的问题。大数质因子的快速分解意味着广泛应用于现在通行于银行及网络等领域的RSA加密算法可以破解，会使得传统密码通信中的公钥体制RSA算法失去意义。

Shor算法的提出使量子计算和量子计算机的研究有了实际应用背景，因而也获得了新的推动力。接着在1996年，Grover又发现了未加整理的数据库搜索的量子迭代搜索算法。使用Grover算法，在量子计算机上可以实现对未加整理数据库$\sqrt{N}$量级加速搜索，能够快速地寻找到DES(Date Encryption Standard)加密算法的密钥，使得DES算法也不再具有安全性。Shor算法和Grover算法的共同点都是利用了量子力学中的态叠加原理。以量子算法为代表的量子计算由于具有高度的并行性、指数级存储容量和对经典的启发式算法的指数加速作用，因此它们在计算复杂度、收敛速度等方面明显超过了常规算法，所有这一切让人们看到量子计算的巨大潜力，使得传统的经典加密技术在理论上显得危机重重。量子计算需要在量子计算机上才能实现真正意义上的并行运算。因此，从1996年以后，量子计算机变成了热门的话题，除了理论之外，也有不少学者着力于利用各种量子系统来实现量子计算机，量子计算和量子计算机的理论与实验研究都呈现迅猛发展的势头。

尽管目前量子计算机还处于研制的初级阶段，但是，量子算法与量子计算机的研究已经从最初的仅是学术上的兴趣研究领域变成对计算机科学、密码技术、通信技术以及国家安全和商业都有潜在重大影响的领域，使得量子算法和量子计算机研究很快成为人们关注的焦点。人们一方面在理论上不断尝试提出新的量子算法，另一方面力图制造出能够运行量子算法的量子计算机。目前，量子计算研究大体有计算模式的研究、硬件研究、软件研究和算法研究四个方向。

1.1.2 量子计算的模式

量子计算模式研究大体上可分为标准量子计算模式、基于测量的量子计算模式、拓扑量子计算模式和绝热量子计算模式四类。

1. 标准量子计算模式

Deutsch在建立量子图灵机的理论模型之后，把建立一个普适量子计算机的任务转化为建立由量子逻辑门所构成的逻辑网络，并指出构成这种逻辑的普适部件应是Deutsch门。对照经典的逻辑电路，Deutsch门的角色就像是异或门，在经典电路模型中，所有的逻辑电路都可以由异或门构建。同样，对于量子逻辑电路，级联量子Deutsch门可以构建任意的量子逻辑电路。1995年，美国的Bennett等人进一步简化了Deutsch门的设计，获得

了更为简单的普适逻辑门集合：采用单量子比特的任意旋转和两量子比特的受控非门，就可以构建任意的量子逻辑电路。由此可见，标准量子计算模式的理论发展与经典计算机的理论发展非常相似。

量子计算也面临与经典计算类似的纠错问题，量子错误更甚于经典错误。因为量子错误本身可以看成一个不可控的量子操作，它会对量子态造成并行影响。多次连续量子错误的累积效果会造成量子相干性的退化(简称为退相干)或消失。克服量子退相干的主要手段是量子纠错码。最早的量子纠错码方法是由 Shor 在 1995 年提出的。目前，几乎所有的传统的纠错码都有了量子情况下的对应。

现今，人们对于成功的量子计算过程有这样一个总的物理图像：首先将要参与量子计算的所有比特在指数维度的 Hilbert 空间中制备出一个纯的量子态，然后，利用量子逻辑电路对这个量子态进行幺正变换，当运行完所有的逻辑变换后，对得到的末态进行量子测量，输出计算结果。进一步，通过对结果的分析、处理，获得待求解的数学问题的答案。在这个过程中，退相干会使量子态偏离理想的演化过程，同时系统与环境的纠缠使得系统状态偏离原来的纯态特征而只能用混合态来描述。如果退相干的程度不是很大，可以采用量子纠错码，可以以很大的概率将系统纠错扭转到原来的轨道上，如果错误的概率超出了量子纠错码所能承受的域值，那么量子纠错就会失效。当然，对于一些由特殊错误类型占统治地位的环境，可以发展主要纠正该错误类型的纠错码方法，所以，容错域值并不是一个绝对的数值，它依赖于错误的类型和使用的纠错码方法。因此，若知道了引起退相干原因的类型，就可以制订应对的量子纠错码的方法。

在有了量子计算过程的物理图像后，量子计算的物理实现问题就变得清晰起来。美国物理学家 Divincenzo 将量子计算的物理实现对物理系统的条件和人为操控能力划分为五条，即 Divincenzo 判据：

(1) 系统要有能很好地表征量子信息的基本单元——qubit，即一个两能级的 Hilbert 空间。

(2) 在计算开始时，要能够对系统进行有效的初态制备，将每一个 qubit 制备到 0 状态。

(3) 要有能力对系统的 qubit 实施普适量子逻辑门操作。具体来说，要能够对单个量子比特实施任意的单 qubit 的幺正变换，以及对任意两个量子比特实施受控非门操作。

(4) 要能够对量子计算机幺正演化的终态实施有效的量子测量。

(5) 系统要有长的相干时间，能够使得量子操作(包括纠错)和测量在相干时间内完成。这就是标准量子计算模式。

其他几种计算模式或是为了简化操作过程(如基于测量的量子计算模式)，或是出于克服环境退相干的考虑(如拓扑量子计算模式和绝热量子计算模式)，最终都需要满足 Divincenzo 判据这一标准量子计算。

2. 基于测量的量子计算模式

基于测量的量子计算模式最先为奥地利 Innsbruck 大学的 Raussendorf 和 Briegel 于 2000 年提出，当时被命名为单向量子计算机，其特点是：在计算的初始阶段，先制备出一个超大规模的称为图态的纠缠态，该纠缠态被命名为图态。这种图态相对来说很容易制备，只需要对初始化的 qubit 进行局域操作和紧邻的伊辛(Ising)相互作用即可。图态制备完毕后，相当于完成了初始化过程，接下来，量子计算机的所有逻辑门操作被证明只需要在图态上进行相应的局域测量和经典通信即可。局域操作和经典通信过程在很多物理体系

中是最简单的操控手段，而这种基于测量的量子计算模式将量子逻辑电路中两比特门的实现难度都退化到图态的制备上。如今已证明，很多多体纠缠态都能够承担实现基于测量模式的量子计算的任务。

3. 拓扑量子计算模式

拓扑量子计算模式方案最早由 Kitaev 于 1997 年提出，他构造了一个具有特殊拓扑量子性质的强关联系统，该系统低能激发的准粒子是一种非阿贝尔任意子，这些任意子可以编码 qubit 信息；同时，任意子的交换满足群论中的辫群规则，通过任意子之间的交换来完成逻辑门操作；最后通过对任意子进行干涉测量来读出计算结果。拓扑量子计算的最大特点是：在该系统中，表征量子信息的量子态是一种拓扑态，它基本上不受局域噪声的影响，具有很强的天然容错功能。

4. 绝热量子计算模式

该方案最早为美国 Goldstone 等人提出。该方案的核心思想是通过绝热演化特征来等效地实现幺正变换：如果将系统冷却到零温，则系统处于体系的基态(假定基态无简并)。此时如果绝热地改变系统哈密顿量的参数，则体系会绝热地跟随系统演化，如果系统不会出现基态和激发态的能级交叉并且绝热演化的条件始终成立，则系统量子态会一直处于系统的基态。但是，由于体系的哈密顿量已经改变，所以此基态非彼基态，演化后的基态同初始的基态之间相差一个幺正变换，因此，绝热过程有实现幺正演化的功效。该方案的优点在于：理想情况下，系统始终处于基态，不存在退相干的问题。它的缺点是：绝热条件依赖于基态与第一激发态之间的能隙。能隙越窄，所需的绝热演化的时间就越长。如果随问题的变大，绝热演化时间指数地变长，那么就失去了量子计算的意义。这个问题于 2004 年由以色列的 Aharonov 等人解决，他们证明了绝热量子计算与标准量子计算模型的等价性。

1.1.3 量子计算机的物理实现

国际上围绕量子计算机物理实现的研究已经进行了几十年，学术上取得了显著的进展。例如，目前操控有效量子比特数目最多的系统——离子阱(ion trap)系统，已经实现了 14 比特的纠缠态的制备。从世界范围内的研究趋势来看，人们对于实现量子计算物理系统的探索，从开始时的百花齐放，人们相继提出了离子阱系统、中性原子系统、线性光学系统以及固态物理系统等。虽然目前人们还不能确定地回答未来的量子计算机究竟会在哪种物理系统中实现，但研究的焦点渐渐移向容易实现器件化和产品化的固态物理系统，如超导约瑟夫森结系统、半导体量子点自旋系统、金刚石 NV 色心系统、集成光子学系统等。

1. 超导约瑟夫森结系统

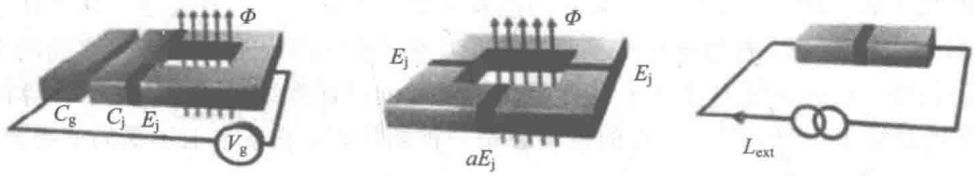
第一个基于超导量子比特的量子计算理论方案是在 1997 年由 Shnirman 等提出的。其核心元件是超导约瑟夫森结，这是一种“超导体—绝缘体—超导体”的三层结构，其中的绝缘层很薄，一般不超过 10 nm，这样的厚度可以使得两块超导体内的库柏对产生相互隧穿，从而使得两块超导体的波函数的相位差根据器件的外界电磁偏置产生确定的联系，这种约瑟夫森结隧穿效应是构建和调控超导量子比特的物理基础。

按照所调控的物理自由度不同，超导量子比特在目前分为超导电荷、超导磁通和超导相位比特三大类型。它们的物理构建和能级结构如图 1.2 所示。同传统的原子、光子之类

的天然量子体系相比较，超导量子比特系统具有以下特点：

(1) 超导量子比特的能级结构依赖于超导量子电路的具体设计和外加电磁信号的控制，可称其为人工原子；

(2) 基于现有的微电子制造工艺，约瑟夫森结量子电路具有良好的可扩展性，易于实现大规模量子比特的集成化，同时也易于实现同其他量子体系之间的耦合。



(a) 超导电荷　　(b) 超导磁通　　(c) 超导相位比特

图 1.2　超导电荷、超导磁通和超导相位比特

自 20 世纪 90 年代末以来，围绕上述三种类型的超导量子比特的实验研究广泛开展，日本、美国和欧洲的研究组相继实现了单个量子比特的表征、两量子比特的受控逻辑操作和三个量子比特的简单逻辑电路的实现。值得一提的是，2010 年中国南京大学的孙国柱和于扬以及美国堪萨斯大学的韩思远等人在一个超导比特和两个两能级体系相耦合的系统中，实现了三量子比特系统的相干调控。而世界上最早的超导相位量子比特的表征和操控，是于扬和其导师韩思远教授在堪萨斯大学完成的。

目前，除了升级量子比特的数目之外，超导量子计算的另外一大趋势是：构建超导量子比特同超导微波腔中的微波光子比特之间相互耦合的杂化量子系统。这个概念最早是由美国耶鲁大学的 Schoekopf 等人提出的：超导电荷量子比特被放置在由三个平行的超导平板构成的传输线腔中，通过耦合电容来实现电荷量子比特同传输线腔中的电磁模式之间的耦合。这里，传输线腔既可以作为操控器件来实现对单个量子比特的操作，又可以作为数据总线，实现远距离的两个量子比特之间的信息传递。2004 年，Schoekopf 小组实现了传输线腔和电荷量子比特之间的共振强耦合，实验中观察到了强度为 12 MHz 的真空 Rabi 劈裂，远远大于传输线腔和量子比特的退相干强度。2007 年，美国 NIST 和耶鲁大学的实验组从实验上实现了利用超导传输线腔耦合两个远程量子比特的实验。NIST 的小组实现了在共振强耦合区域内，两个超导相位量子比特通过传输线腔的耦合；而耶鲁大学的小组实现了两个电荷量子比特在大失谐区域内的耦合。2012 年，美国加州大学河边分校和圣芭芭拉分校的研究者们又提出了超导量子计算的 RezQu(振子—零态—量子比特)构建(见图 1.3)，其基本思想是：将每个量子比特分别同两个超导传输线腔耦合起来，其中的一个传输线腔作为存储器，另外一个传输线腔作为所有量子比特的数据总线。量子比特的能级是可以调节的，通过调节量子比特的能级，与不同类型的传输线腔模共振，从而实现量子信息在存储器—量子比特或数据总线—量子比特之间的交换。如果一个量子位处于闲置状态，则该处的量子比特处于零态，量子比特被存储在存储器中。如果该处的量子比特需要进行单比特操作，则将存储器中的信息交换到量子比特上，再对量子比特进行操作，操作完成后再将其重新存储到存储器中。如需实施两个量子位的操作，则将信息交换到量子比特上之后，调节量子比特的能级，将其同数据总线中的振子模式共振，通过量子比特—数据总线—量子比特的交替作用，实现两个量子位的逻辑门操作。该构建方案的优点是：除

了能够保持超导电路良好的可扩展性，由于用作存储器的量子振子的退相干时间要长于超导比特的退相干时间，所以系统的相干性能够得到很好的保持。2011 年，两个量子比特的 RezQu 处理器已经在实验上获得实现，并且实施了 Noon 态的制备。进一步，该小组实现了量子的 Von－Neumann 架构。

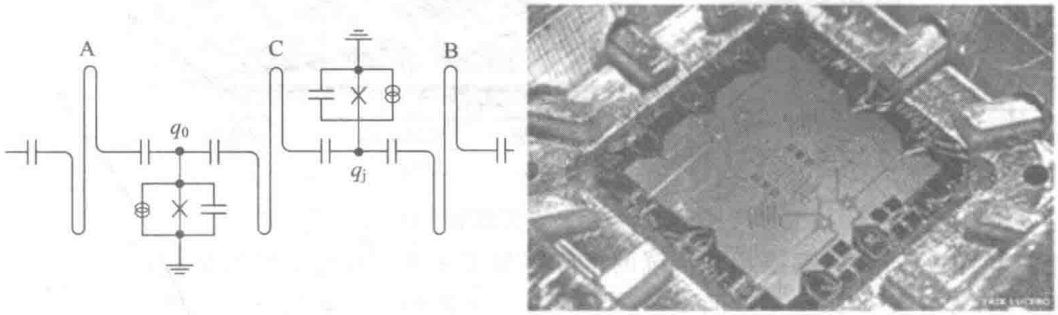


图 1.3 超导 RezQu 构建示意图及其超导芯片照片

除了上述对于量子计算进行系统性的构建之外，在超导量子比特系统中的单元技术研究方面，也取得了很大的进步。例如，在最初的超导量子计算的方案中，比特之间的耦合是不可调节的，虽然采用适当的方式可加以克服，但是会大大增加逻辑门操作的复杂程度。2006 年，Niskanen 等在实验上实现了超导磁通量子比特之间的可控耦合，其原理是使用第三个量子比特作为耦合器件，通过对耦合器件能级的射频调制来有效地开关两个量子比特之间的相互作用。在实验中，量子逻辑门的开关比达到了 19。近年来，随着材料加工和器件制备工艺的提高，超导量子比特的退相干时间也被大大延长，在电荷量子比特系统中，退相干时间 T_1 达到了 60 μs，T_2 达到了 14 μs。

超导量子比特系统除了用于标准量子计算模型的探索之外，还是绝热量子计算模式的可能候选者。通过构建耦合的磁通量子比特阵列，该系统可以模拟量子伊辛相互作用模型，通过调节系统的控制参数，可以对这个多体哈密顿系统进行绝热演化，来寻找变参数情况下体系的基态。这种所谓的量子退火算法，可用于解决特定的数学问题。2011 年，加拿大 D－wave 公司实现了 8 比特的量子退火算法。

由于超导系统具有高度可控性和易于集成的优点，它也有可能成为检验拓扑量子计算模式的候选体系。验证拓扑量子计算的第一步是获得具有非阿贝尔统计的任意子激发。2012 年，中国复旦大学游建强等人提出在超导约瑟夫森结阵列中操纵和探测 Majorana 费米子的方案。Majorana 费米子是一种已经被人们预言但迄今未被发现的具有非阿贝尔统计的准粒子，如能在实验体系中探测和证实，则具有重要的学术价值。

2. 基于门控量子点的量子计算系统

在量子计算中，通常用作量子比特的半导体量子点有两种，一种被称为“自组织生长的量子点”，一种被称为“门控量子点”。最早提出基于门控量子点上操纵单电子自旋的量子计算理论方案是瑞士巴塞尔大学的 Loss 和美国 IBM 研究院的 Divincenzo。所谓门控量子点，是指使用分子束外延方法生长出高纯净和高迁移率的 GaAs－AlGaAs 半导体异质结晶片，在其上刻蚀出金属门电极，在门电极上加负压，排空在门电极周围的二维电子气，形成一个电子受限的空间，使得只有少数电子甚至是单电子在百纳米大小的区域内运动。当只有单个电子被放置在这个受限的空间中时，系统很像一个氢原子。在外加磁场的作用