量子信息学

◆郜江瑞　谢常德

信息科学与技术已经深入到社会的各个方面，其中的主角——计算机科学与技术的发展与应用，更是极大地促进了人类文明的进程。

目前的计算机都基于经典物理规律，是经典计算机。多年来，人们已经认识到经典计算机有着某些不可克服的局限性。例如，不可能产生真正的随机数序列，无法在有限的时间内模拟一个常规的量子力学系统，不可能在可接受的时间内完成大数因子分解等等。

从目前微电子技术发展的程度来看，人们必须面对这样一个问题：当二氧化硅表面的电路线度小到原子的尺度时，电子在电路中的行为将不再服从经典力学规律，取而代之的则是量子力学规律。也就是说，人们不得不在量子理论的框架下研究信息科学和构建信息系统。

时尚的科学

量子信息（quantum information，QI）科学，是以量子力学的态叠加原理为基础，研究信息处理的一门新兴的前沿科学，是现代物理学基础理论与信息科学技术相互交叉而产生的一门充满活力的学科。量子信息学包括量子计算机、量子离物传态、量子保密通讯、量子非破坏测量等几个方面。

1980 年代，费恩曼[1]和贝内特（C. Bennett）[2]等就已开展了量子信息学的理论研究。他们指出，光子的两个正交偏振态、原子的两个自旋态或原子中两个合适的能级这些正交的量子态（例如：$|0\rangle$，$|1\rangle$）可以表示一个比特的量子信息，称为量子比特（qubit）。与经典比特不同，量子比特中的粒子（光子或原子）不但可以处于$|0\rangle$态或者$|1\rangle$态，而且可以同时处于$|0\rangle$和$|1\rangle$的任何一种叠加态。正是这种奇异的特性，使量子比特具备了经典比特无法比拟的优势。

在量子信息学的研究中，除了量子算法外，量子计算机中的量子逻辑门和量子通讯中的量子离物传态，是人们最关心、最有兴趣的研究课题，目前已获得初步的实验研究结果。

此外，在探索量子信息处理方法过程中所完成的量子力学实验，又反过来帮助人们验证、加深对量子世界规律的认识，回答那些至今尚存争议的问题。量子信息学的研究，不仅具有重要的应用前景，而且具有深远的科学意义。

强大高效的计算工具

1985 年，牛津大学的多奇（D. Deutsch）[3]建立了量子计算机的理论基础，促进了量子计算机的发展。与经典计算机类似，量子计算的实现也要依赖于相应的基本逻辑元件——量子逻辑门（quantum logical gate，QLD）。目前有四种可能的量子逻辑门的实验方案，它们分别基于腔量子电动力学（CQED）、离子阱（ion trap）、核磁共振（NMR）和量子点（quantum dot）。

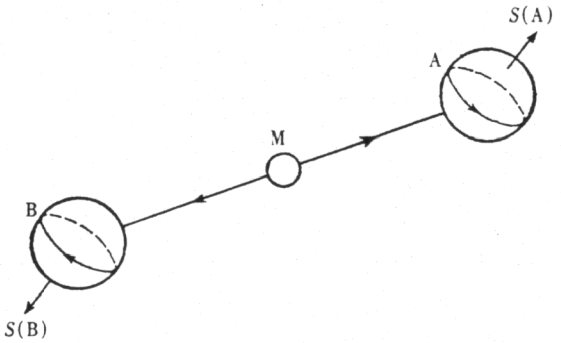
（1）腔量子电动力学

腔量子电动力学（CQED）的基本思想是，把极少数原子置于一高品质微型腔中，使腔中电磁场（包括真空场）可以受控改变，从而影响原子的辐射过程。CQED 最成功之处是研究少数粒子（光子、原子）之间的相互作用。其方法是尽可能使单个光子的电场增强，以致于它能使单个原子的响应饱和。要达到此目的，必须实现单原子和单光子在腔内的强耦合。

CQED 作为量子逻辑元件用于量子信息处理，首先是由佩利扎里（T. Pellizzari）等人提出。加州理工大学的金布尔（J. Kimble）小组采用该方案初步演示了量子逻辑门。其基本方法是将若干中性原子俘获在高品质微

郜江瑞，教授；谢常德，博士：山西大学光电研究所，太原 030006。

Gao Jiangrui, Professor; Xie Changde, Doctor: Institute of Opto-Electronics, Shanxi University, Taiyuan 030006.



EPR 效应　1935 年爱因斯坦、波多尔斯基、罗森为证明量子力学是非完备的而提出了一个假想实验——EPR (Einstein-Podolsky-Rosen)佯缪。其基本思想是，一个角动量为零的系统 M 分裂成两个反向传输、自旋为 1/2 的粒子 A 和 B，沿任何方向测量每个粒子的自旋处于 ±1/2 的概率都是 50%。无论 A 和 B 相距多远，都处于关联、纠缠的状态，只要测量其中一个的自旋状态在 x(或 y) 方向的投影为 ±1/2，则另一个的自旋状态在该方向的投影立刻塌缩到 ∓1/2。

型光学腔中，将量子信息存储在原子的内态上，即中性原子的基态和一个亚稳态上。载有一个量子比特的量子态是处于原子基态 $|g\rangle$ 和一个长寿命的亚稳态 $|e\rangle$ 的线性组合。该态可以较长时间存贮量子比特，同时，处于微腔中的原子能很好地与外界隔离。

CQED 是实现量子逻辑门较为理想的方案之一。但在高品质腔中，多量子门之间的连接仍然有一定的技术困难。

(2) 离子阱技术

采用离子阱实现量子逻辑门的方案首先由西拉克(J. Cirac)等人提出，目前在实验上已初步实现。在实验中，每一个量子比特被赋在俘获于线性保罗(Paul)阱中的单个离子上。载有一个量子比特的量子态，是处于离子基态 $|g\rangle$ 和某一个长寿命亚稳态 $|e\rangle$ 的线性组合。因此，同原子一样，它也能实现量子比特的存储。

离子阱的好处是，离子之间的库仑相互作用使离子之间相距较远，因此将单个激光脉冲的能量调谐到某一离子的 $|g\rangle$ 态和 $|e\rangle$ 态能级差，就能实现量子信息的读取和变换。

离子阱方案的最大问题是，以此建立的离子阱量子计算速度会受到制约。原因是时间 - 能量不确定关系决定了激光脉冲能量的不确定度应比质心振动的特征频率小，每个光脉冲的持续时间应长于该特征频率的倒数；而声子的振动频率一般较低，实验中特征频率约为 100 千赫，因此运行速度较慢。而在 CQED 中，由于光场与原子作用时间很快，因此不存在离子阱中响应速度慢的问题。

(3) 核磁共振技术

基于核磁共振技术的量子计算方案，是近几年发展起来的一种新的量子信息处理方法。在 NMR 中，量子比特被赋在特定分子的一定核自旋态上。在恒定外磁场中，每一个核自旋要么向上要么向下。系统自旋状态在退化和退相干之前可以保留较长时间，量子比特因此可以得到存储。

可以通过一个脉冲磁场作用于自旋态实现自旋的拉比振荡，选定合适的磁脉冲同样可以实现单个磁自旋态的变换，因为只有那些处于与外加磁场共振的自旋态才会产生作用。同时，自旋态中也存在偶极相互作用，这种作用可以用来实现逻辑门。

但是 NMR 用于量子计算并不是像前面两种方案那样易于接受。因为 NMR 系统很“热”，核自旋的温度(常温下)一般引起的能量涨落比上下核自旋能级之差要高出上百万倍。这意味着，由单分子中的核自旋构成的量子计算机中的量子态处于非常大的热噪声之中。这些噪声会把量子信息淹没掉。进一步讲，实际过程中处理的还不是单个分子，而是包含有 10^{23} 个“量子计算机”的宏观样品。

从这个装置中读出的信号实际上是大量分子的系综平均，但量子算法是概率性的，它来自量子计算本身的随机性，而人们正是利用这种随机性。系综平均绝对不等于在单个装置上进行量子计算。人们曾对上述困难提出过一些解释，指出多次计算的平均不会消除有用的量子信息。据报道，采用 NMR 方法已经产生了多量子比特逻辑门，并用此实现了量子离物传态。

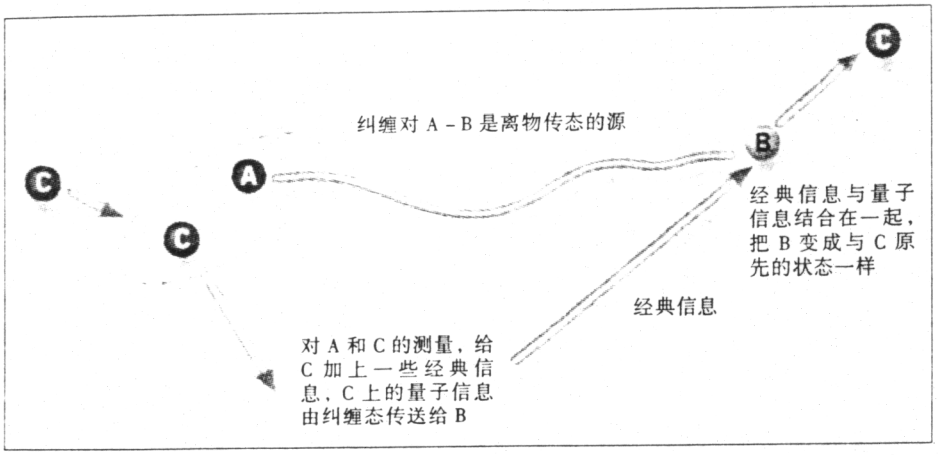
目前许多学者认为，现有的 NMR 系统不可能产生纠缠态；而产生纠缠态是量子信息中的关键。NMR 作为量子信息的硬件会遇到许多困难，其中来自原理上的限制是：相干信号与背景噪声之比会随着每个分子中核自旋数目的增加而指数衰减。在一个实际系统中，用 NMR 完成 10 个量子比特的计算就会遇到严重挑战。当然也有学者对上述论点持有不同看法，对 NMR 实现量子逻辑门持乐观态度。无论如何，NMR 会帮助人们弄清一些核自旋方面的东西。

(4) 量子点

量子点涉及到纳米尺度的半导体区域。这些区域内呈现少数电子态，将单电子导入量子点可改变电子的状态，从而有可能用于量子信息处理，将量子点置于 CQED 中又可能控制材料的自发辐射、增强光和物质的相互作用。如果将成熟的半导体技术与量子器件结合起来，可能产生一种实用的量子信息系统。但是，如何

保证材料中量子点的纯洁仍然是一个挑战。

在企图真正开始量子计算之前，需要尝试各种不同的量子逻辑门方案，这是一件极富挑战性的工作，它才刚刚开始。实际的量子计算，要以在量子比特数目和量子逻辑门方面都取得重要进展为前提。



量子离物传态示意图 量子态发送者和接收者分别利用 EPR 纠缠对的一半，发送者将被传送的量子态 C 和纠缠态的一半 A 进行联合测量，所测得的经典信息由经典通道发送，而测量过程中的量子信息通过非局域关联自然地传给了纠缠态的另一半 B。EPR 纠缠对是信息传送的量子通道，接收者同时利用经典通道与量子通道的信息最后来恢复被传送的量子态。可见纠缠态是一种能使量子状态从一个粒子转移到另一个粒子的工具。

神奇的魔法——量子离物传态

离物传态(teleportation)源于一个科幻电影，意思是脱离实物的一种“完全”的信息传送(disembodied transport)。

由于受到相对论效应的限制，不可能将实物在瞬间从一个地方传送到另一个地方。那么可以对物体实现瞬间的离物传送吗？在不超越光速极限的前提下，似乎是可行的。因为，原则上说只要了解构成物体的全部信息，所有的量子态可以在任何地方重构。然而，量子力学告诉人们，不可能对量子态进行精确测量，不可能精确了解任何物体的全部信息。所以这种方法的重构是无法实现的，这也是量子不可克隆定理[4]所限制的。但量子力学中的另一现象——纠缠态（EPR）的非定域性（non－local）[5]——为实现量子离物传态提供了新的途径。

1993 年，6 位来自不同国家的科学家，提出了利用经典与量子相结合的方法实现量子离物传态的方案。利用 EPR(纠缠态) 对的非定域性，在不违反量子不可克隆定理的情况下，可以把一个未知的量子态从一个地方传到另一个地方。在这个方案中，EPR 源起着至关重要的作用。量子力学的非定域性已被违背贝尔不等式的实验结果所证实。

量子离物传态不仅在物理学领域对人们认识与揭示自然界的神秘规律有非常重要的意义，而且可以用量子态作为信息载体，通过量子态的传送完成大容量信息的传输，实现原则上不可破译的量子保密通讯、超密集编码等，量子计算与量子通讯因此成为当前迅速发展的量子信息领域的核心内容。

秘密的保护神

密码的研究与使用是一个非常古老、广泛的问题，目前使用的密码除一次性密码（Vernam 密码）外，并非不可破译，其保密性主要取决于破译算法的困难程度与计算时间。采用量子密码就可以从原理上保证通信的保密性。通信的双方可以通过公共信道建立自己的密钥。

与经典力学不同，在量子力学中，对系统的任何一次测量都是对系统的一次作用，都会改变系统的状态（除非是处于作用算符的本征态）。量子密码术中可以用单光子偏振态进行编码。在两个不相容的正交偏振基中测量一个光子的偏振态，其结果是完全随机的，不可能在一次测量中得到一个光子在两个不同的偏振基中的结果。

窃听者由于无法知道通信的双方每个时刻会随机选取哪一种偏振基，所以也就无法准确地复制窃听信号，通信的双方只要在公共信道随机比对部分测量结果就会知道密钥是否被窃听，发现密钥不安全，可以重新建立密钥，直到满意为止。

精确无比的量尺

量子力学基本原理告诉人们，由于量子不确定性原理，采用一般的方法，测量的精度最终会受到散粒噪声极限的限制，不可能对一个量子体系进行无限制的精确测量。同时，测量过程不可避免地干扰、影响被测体系的量子状态，这往往会导致测量结果更加不准确。利用光场的非经典效应（即独特的量子效应，没有对应的经典特性），采用量子测量的方法，可以巧妙地“避开”量子不确定性的影响，从而提高测量精度。

(1)量子非破坏测量

量子非破坏测量（quantum non－demolition detection，QND），1970年代由布拉金斯基(V. B. Braginsky)[6]等提出，其目的就是为了克服测量过程对被测体系量子状态的干扰所导致的测量结果的不精确，以便能够对被测体系重复测量而不影响被测量。

QND测量的主要特点之一就是可重复性。测量过程中首先要选一对好的共轭量，使测量过程中对其中一个量的干扰不影响另一个共轭量，同时将被测量（信号场）复制到探针场。

1989年科学家利用非线性参量过程从实验上实现了这种反作用逃逸，1993年格朗吉耶(P. Grangier)通过钠蒸气相位调制实现了QND测量。随后，各国量子光学实验室又采用不同系统实现了不同类型的QND测量，其传输效率与量子态制备能力都在不断提高。1998年山西大学光电研究所首次实现了强度差起伏的类QND测量[7]。

(2)突破散粒噪声极限的测量

由于受量子力学原理支配，光场存在一最小不确定状态，即散粒噪声极限。对一般的相干态光场而言，散粒噪声极限是指两共轭量的起伏相等，乘积为一由不确定关系限制的确定值。在一般情况下，测量的精度总是受到散粒噪声极限的限制，而与测量仪器无关。

利用非线性过程产生的非经典光场——光场压缩态，可以在保持两共轭量起伏乘积不变的条件下使一个共轭量的起伏远远小于另一个。这也就是说，其中一个共轭量的起伏已经小于散粒噪声极限。利用压缩光场的这一特性，可以使测量精度突破散粒噪声极限的限制，当压缩度为百分之百时，测量精度原则上可无限提高。

1987年，肖(M. Xiao)与格朗吉耶分别用正交压缩真空态光场，使测量灵敏度突破散粒噪声极限。1997年，山西大学光电研究所直接用强度差压缩光场（孪生光束对）进行弱吸收测量，使测量结果突破信号光散粒噪声极限，信噪比(S/N)较信号光散粒噪声极限提高4分贝。此外，还有许多各种类型的压缩光场在测量中应用的报道。

尽管量子信息处理具有速度快、容量大、安全性好以及测量精度高的巨大优势与非常诱人的应用前景，而且也引起了科学家与政府部门的关注，但除量子保密通讯有可能很快进入实用阶段外，要实现真正的量子计算机、实物的离物传送，还有很长的路要走。

一个重要的原因是因为量子态非常“脆弱”。任何与外界环境的微小作用都会导致量子态的塌缩，即退相干。因此必须在一定时间内保持量子态与外界隔离，在态塌缩之前完成必要的量子计算。虽然理论上证明这是可能的，实验实现却需再做努力。另一方面，量子信息处理对系统的存储性、隔离性以及量子逻辑门操作的准确性都具有一定的要求，这里面牵涉到的有关单光子与单原子相互作用等技术问题也绝非易事。

目前，理论与实验物理学家也正在努力试图通过各种可能的途径解决这些问题，相信在不久的将来，量子信息科学将会有突破性的进展。

[1] Feynman R. *Int J Theor Phys*, 1982, **21**: 4627
[2] Bennett C. *J Stat Phys*, 1980, **22**: 563
[3] Deutsch D. *Proc Roy Soc Lond*, 1985, **A400**: 97
[4] Wootters W, *et al*. *Nature*, 1982, **298**: 802
[5] Einstein A, *et al*. *Phys Rev*, 1935, **47**: 777
[6] Braginsky V, *et al*. *Usp Fiz Nauk*, 1979, **114**: 41
[7] Wang H, *et al*. *Phys Rev Lett*, 1999, **82**: 1414

关键词：量子信息学　量子计算机　离物传态　非破坏测量

跟踪·扫描

性行为模式影响免疫系统的进化

据美国 *Science*，2000，**290**：1168报道，科学家找到了滥情必须付出代价的生物学依据。“放荡”的灵长类种群在免疫系统上须投入更多精力以抵御性传播疾病。这项研究意味着性行为方式可能影响着免疫系统的进化过程。

科学家对免疫系统如何进化向来知之甚少。他们猜测一些要素（如群体大小与密度、土壤病原体的数量、性伴侣数目等）增加了患病的危险；但这些力量如何在若干代后塑造该种群的免疫系统，仍是一个谜。美国弗吉尼亚大学的纳恩(C. L. Nunn)等人找到了血液白细胞数目（白细胞是抵御疾病的第一道防线）这一线索。他们希望以此探讨，面对传染病的高度危险性是否可导致一个特别活跃的免疫系统。

他们查看了世界各地动物园中的41种健康的灵长类动物，并根据每一种类的性交模式和其他要素的数据，比较它们的白细胞数目。结果表明，某个种类的自然群大小和地面活动时间（意味着暴露于土壤病原体的时间）没有显著影响，但在群交的种群（如大多数猕猴）中，白细胞数目明显高于那些单配偶的种群（如长臂猿）。

显然，性交模式越混乱的种群，在免疫系统上必须投入更大精力。作者同时指出，人类的白细胞水平与那些“一夫一妻”的灵长类动物一致。

（孙庆安）