量子计算与量子计算机

张登胜　　詹明生

(中科院武汉物理与数学所波谱与原子分子物理国家实验室　430071)

最近,量子计算与量子计算机引起了人们的极大兴趣.一个光子的偏振或一个自旋为1/2的粒子(两态系统),对应于布尔态0和1,可构造量子计算机存储单元.量子计算的原理是计算机科学家在大约15年前将量子力学的叠加原理应用于计算机算法时提出来的.两态系统能够作为量子位(或量子比特).两态系统之间的相互作用能构造量子逻辑门,它遵守非经典的逻辑运算.早在半个世纪前,在研究简单的量子门操作和数个量子位缠绕过程中,量子力学的先驱者就想弄清经典与量子世界的界限.这种研究领域极大地得益于计算机专家提出的概念,即将数学与物理交叉结合起来.

量子计算机显著特征是相干叠加性及运算过程中的幺正变换性.量子计算比经典计算效率高得多,并且能够解答离散的对数、求解大数的因子等等.原则上讲,许多量子逻辑门形成的网络能够以叠加态的形式操纵大量量子位,并以比经典机器更小的计算步程进行并行计算.P.Shor在Bell实验室发现,量子计算能有效地分解大数的因子.大数因子的分解在当今的经典计算中几乎没法解决,但它在安全密码方面非常有用.由于能快速分解因子,量子计算机放弃了目前使用的老式的密码系统.

一、量子逻辑门

量子计算机的最基本的构造单元是逻辑门.它有两种相互作用的量子位:控制位和目标位.控制位保持不变,但它的状态决定目标位的演化.如果控制位是0,则目标位不发生任何改变;如果控制位是1,则目标位将经历一个确定的变换.量子逻辑门是一个输入输出设备,它的输入和输出量是分离的量子变量(比如说自旋).它作用于输入量用一个幺正算符U来描述,即输入量的态矢由$|\Psi\rangle$变成$|\Psi'\rangle = U|\Psi\rangle$.我们知道,对于一台数字计算机而言,如果有线性逻辑门,如NOT门和COPY门,也有非线性逻辑门,如AND门,则它可以完成任何一种逻辑或算术任务.对于量子计算机,同样的要求也是成立的,牛津大学的A.Barenco等论证了这一点.1982年,Fredkin和Toffoli提出了一个可逆计算的逻辑门(简称Fredkin门),这是一个有三根输入线和三根输出线的设备.其中有一根(假定为a线)设计为控制线,它的逻辑状态在通过该门时不改变.如果控制线的位是0,则其余两根线(b、c线)的位不发生改变;如果控制位是1,则其余两根线的位相互交换.量子力学允许更多的选择,如果控制位是0和1的叠加态,量子门的输出则是缠绕的态,也就是说,在一个非分离的态中,两个量子位相关性很强,类似于Einstein-Podolsky-Rosen佯谬中的粒子对.输入的量子位的叠加和输出态的缠绕是量子逻辑门区别经典逻辑门的基本特征.至少从理论上讲,量子计算为计算容量提供了更广阔前景.

一些物理学家和计算机专家指出,多种实验(如囚禁粒子或微腔中的原子和光子)能够提供量子门所需要的成分.原子或场的状态可以用两能级系统描述.利用两能级系统间的相互作用,我们能完成必要的量子位操作.这就是量子计算目前变得如此热门的关键所在.当初用于检测量子理论的基本特征的实验装置,现在已用来论证量子逻辑操作,尽管操纵单个量子逻辑门并不非常困难,但要操纵由大量量子门构造的计算机,情形就

完全不一样了，似乎是不可能的.进行计算的过程中，机器必须包含大量量子位状态的叠加，而这些态是由大量的经典的可选择的路径形成的量子干涉.

为了实现量子计算，物理学家和计算机专家提出了一些设计方案，如原子力显微镜(AFM)，齿轮箱量子计算机以及用冷却的囚禁粒子和核磁共振(NMR)进行计算.最近，有文献对NMR应用于量子计算进行了原理性探讨，这说明NMR应用于量子计算具有可能性.NMR用来构造量子计算机存储单元具有特殊优点.早在1946年，Bloch就注意到核自旋的特性，它的弛豫时间较长.此外，在现代NMR光谱学技术中已经证明，原子核自旋可以携带量子信息，并可用射频来操纵.NMR是原子核的行为.原子核象一个微小的磁棒，有南极和北极，当把它放在磁场中，其自旋将沿场的方向排列，由于其他力的作用，尤其是热的扰动，系统最终达到一个动态平衡.自旋在合适的频率下传递一个脉冲，它随着自旋元的类型和原子核的环境而变化，某些原子核自旋将反转到相反的方向.当脉冲结束时，这些自旋将进动(摇摆)，象一个微小的陀螺一样，在进动中，它产生一个可探测到的电磁波信号.NMR系统用作量子计算，有两个明显优点，第一，原子核向上向下的自旋作为一个量子系统，通常有较长的寿命.其他的量子系统，解相干如果不是10^{-12}或10^{-15}秒量级，一般也在10^{-3}秒量级.而NMR能在数千秒时间内保持有相同的量子位相，原因是原子核中的自旋能很好地隔离于外部环境，原子核周围的电子云将它与外界隔离起来，起屏蔽作用.另外，存在于分子中的自旋总是"耦合"在一起，因此，某个自旋在一合适的频率下的自旋方向的改变几率依赖于邻近自旋的状态.比如说，一个孤立的碳原子核自旋可能在某一频率下改变方向.假设一个靠近氢原子核的碳核，在氢原子的自旋向下时，在某一频率下反转，但是，当氢原子的自旋向上时，碳核的自旋将在另一频率下反转.当选择一个精确的频率发送给碳核，使氢核的自旋只有向上时，碳核的自旋反转，这对应于量子受控非门(Controlled NOT gate)，它是量子计算机的基本的也是最重要的量子门之一.室温上处于热平衡的大量原子核自旋，是纯态的统计混合.如果用这样的混合态进行量子计算，将导致不同态之间相干破坏，不能进行有效的量子计算.NMR量子计算的这种欠缺已被注意到.有人建议构造一种仪器在某一时刻存放单个核自旋，这类似于在离子阱中操纵单个离子(原子).这种方法将避免热平衡问题，因为如此定义的单一系统总是处于纯的量子态.但是探测单个核自旋诱导的微弱信息非常困难.因此，研究核自旋的制备、控制、相干演化以及测量是很有意义的课题.但是，设计者面对的最大挑战是量子信息传输过程中，如何在实现量子信息载体间强的可控制的相互作用(如两个原子核自旋被AFM引起的接近或者两个原子通过高精细的腔进行耦合)的同时，保持量子信息足够好地隔离于宏观的环境，以避免快速的解相干过程.

二、解相干问题

一个美妙的想法是生产一种机器，它能完全隔离于外部环境.但是事实上，量子干涉是相当灵敏的，它不可避免地与环境相耦合，这种事实在许多研究文献中被研究过，单个的影响处于激发态的量子位的弛豫事件将毁坏量子计算机所必需的相干性.

一个简单的讨论将帮助我们了解解相干(即相干性被破坏)问题.如果T是单个量子位的弛豫时间，t是单个量子门的操作时间，则$R = T/t$可作为衡量理想计算机特征的物理量.假如我们要成功地进行计算，R必须是量子位的个数与量子门操作数目两者的乘积.作为例子，我们考虑Shor的因子分解的代数问题.因子分解4位数，大约需要20000个量子门操纵20个量子位.因此R将大于4×10^5.这是目前能达到的最好的量子光学系统的乐观结果.假如要解决一个更接近实用的任务，比如分解400位的数字，则R将增至分解4位数时的3次方倍，达4×10^{11}量级.在最近提出的囚禁粒子

构造的量子门，t一般为10^{-4}秒，那么弛豫时间必须达一年左右.乐观者认为解相干问题难不倒我们，因为他们认为Pascal机器及Pentium处理器两者已有长足的进步，并且科技和金钱的能力尚无明显的限制.但是，持这种观点的人必须假定t和T是独立且能类似反比地变化.然而，在今天的已知的物理系统中并非如此，物理的相互作用导致环境与量子位的耦合，增加了系统自身的噪声，最后导致量子位的随意性变化.

在囚禁粒子构造的量子门中，量子位是用粒子的基能级的两个亚稳态进行编码.一般而言，基态的能级寿命是相当大的，但是量子位的操作是用激光诱导的Raman过程来实现的，这个过程包含粒子向短寿命激发态能级的虚跃迁.假如我们用增大激光功率来缩短虚跃迁持续的时间，则同时增加了不需要的向激发态能级真实跃迁的可能性，随之而来的自发发射将毁坏量子位的量子相干性.因此，不可能达到既缩短t而又增加T.如果不考虑激光功率，对于囚禁粒子量子门而言，R一般在精细结构常数立方的倒数的量级，大约3×10^6.一些基于电偶极光学跃迁的量子门大约在这个量级.因此，如果不能有效地纠正解相干，我们用光学的量子计算机能达到的最好结果是实现4位数字的因子分解.

值得一提的是，宏观的量子系统如超导金属，或最近研制成功的Bose-Einstein原子凝聚并不会被解相干所毁坏，为什么量子计算机的相干性如此容易破坏呢？原因是它们有根本性的不同.宏观的凝聚态，当大量粒子不是协作运动，可用单个量子态来描述，它的态可用0来表示.而在假想的量子机器中，量子状态将是大量不同态的叠加.例如，对于一个有1000个量子位的存储器，将具有$2^{1000}\approx10^{300}$个状态，在上百亿次操作过程中，所有这些状态的相干性必须被保持.操纵如此的量子"怪物"等同于使著名的"薛定谔猫"处于死态与活态的叠加态一样困难.

围绕解相干问题，最近已提出一个精细的方案，即利用监视器策略.由于自发发射是产生解相干的主要原因，我们时刻监视它并纠正它引起的解相干，使量子位被破坏时立即恢复原量子相干性.所有这些方案依赖于多余信息(量子位)的使用.我们给单个量子位进行编码时，实际上是利用三个或更多个量子位态(0或1)进行编码.当一个量子位偶然被翻转(0变成1或1变成0)时，将由灵敏的监视器检测出来并纠正它.多粒子的缠绕态是如此难以制备，以致目前尚未成功.假如将来科技的进步使得能在实验室制备多粒子的缠绕态，监视器检测的微小偏差也将导致附加的解相干.因此，我们认为，除非一些现在未能预见的新的物理方法被发明，否则，纠错码的实现将变得如同操纵大量量子门一样困难.

三、小　结

量子计算和量子计算机需要制备、控制、相干演化以及纯量子态测量四个过程.这四个过程中还有大量的理论和实验难题没有解决，有待进一步研究和探讨.目前有人认为用量子门进行计算，也有可能利用某些简单的量子系统的自然时间的演化进行运算，像晶体的量子态，它自身能实现某种有用的计算，在此基础上已做成"量子分格自动化".也许我们目前认为量子计算需要精确的隔离是没有必要的，也许一些开放的量子系统的密度矩阵的时间演化也是一个有力的计算工具.

尽管量子计算的想法包含一些迷人的新的物理思想，但是要真正地实现量子计算，还是一个全球性的难题.因此，在可预见的将来，实现大规模的量子计算仍然是不现实的.不过，量子信息方面的物理学家在几个量子位方面研究的成功还是非常迷人的.囚禁粒子的态或腔中的原子将帮助我们对量子系统的精细光谱的关键问题进行认识.我们对量子计算和量子计算机的实现充满信心.

(张登玉工作单位：湖南衡阳师专物理系)