奇特的量子效应

——量子纠缠

王 明 美

（安徽教育学院物理系 合肥 230061）

量子力学从1925年诞生以来，经过大量的实验检验和理论发展，肯定了它的正确性。量子力学与信息技术的结合也是必然的。当今，信息科学在推动社会文明进步和提高人类生活质量方面发挥着越来越重要的作用。现有信息系统的功能开发已经接近极限，电子计算机的每个芯片上集成的晶体管数目随时间呈指数增长。这预示着，若干年以后计算机存储单元有可能是单个原子，而电子在电路中的行为就将不再服从经典力学规律，取而代之的是量子力学规律。于是自然而然地提出了量子效应究竟会对计算机运算速度产生什么样影响的问题。因此，信息科学进一步的发展必须在量子力学中寻找新的原理和新的方法。

量子特性有着独特的非经典功能，有可能在提高运算速度、确保信息安全、增大信息容量和提高检测精度等方面突破现有的经典信息系统的极限。量子信息学应运而生，该学科是量子力学与信息科学相结合的产物，它是以量子力学的态叠加原理为基础，研究信息处理的一门科学。量子信息学包括了量子密码术、量子通信、量子计算机等几个方面，近年来在理论和实验上都取得了重大的突破。

在量子力学所描述的关于微观粒子的一系列量子效应中，量子纠缠就是近年来在量子信息领域引起广泛关注的一种量子力学效应。

量子纠缠是量子力学描述微观粒子的一种现象，在量子力学中微观粒子是指具有波粒二象性的物质。量子纠缠是指量子体系不仅能处于一系列的稳定状态（定态），也可以处于它们的叠加态中，或者说粒子以这样一种方式耦合在一起，以致整个体系不再能够用其组成成分的各自状态来描述。如果测量处于叠加态原子的某种物理属性（如能量），得到的是叠加态中所有可能的能量值中的某一个值。也就是说有时得到的是这一个值，有时得到的是另一个值。每个能量值出现的几率大小则取决于波函数的平方。实际上可以认为量子纠缠是量子相干性的表现方式。量子纠缠不能够用经典物理解释，它实际上是由几率波叠加而成的，具有非定域性，非常奇特。下面介绍量子纠缠在量子密码术、量子通信以及在量子计算机中的用途。

一、量子密码术与量子通信

量子密码术是密码术与量子力学结合的产物，它利用了系统所具有的量子性质。

量子密码术并不用于传输密文，而是用于建立、传输密码本。根据量子力学的不确定性原理以及量子不可克隆定理，任何窃听者的存在都会被发现，从而保证密码本的绝对安全，也就保证了加密信息的绝对安全。

首先想到将量子物理用于密码术的是美国科学家威斯纳。威斯纳于1970年提出，可利用单量子态制造不可伪造的“电子钞票”。但这个设想的实现需要长时间保存单量子态，不太现实。贝内特和布拉萨德在研究中发现，单量子态虽然不好保存但可用于传输信息。1984年，此二人提出了第一个量子密码术方案，称为BB84方案，由此迎来了量子密码术的新时期。1992年，贝内特又提出一种更简单，但效率减半的方案，即B92方案。最初的量子密码通信利用的都是光子的偏振特性，目前主流的实验方案则用光子的相位特性进行编码。量子加密要利用量子纠缠效应以实现反克隆，但由于潜在效率的耗散现象的存在会降低纠缠程度。因而如何提纯高品质的量子纠缠态是目前量子通信研究中的重要课题。

量子通信是指基于对信息进行完全传输的通信。该系统的基本部件包括量子态发生器、量子通道和量子测量装置。按其所传输的信息是经典还是量子而分为两类。前者主要用于量子密钥的传输，

后者则可用于量子隐形传送和量子纠缠的分发。所谓隐形传送指的是脱离实物的一种"完全"的信息传送。隐形传送的过程是:先提取原物的所有信息,然后将这些信息传送到接收地点,接收者依据这些信息,选取与构成原物完全相同的基本单元,制造出原物完美的复制品。

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隐形传送的方案:将某个粒子的未知量子态传送到另一个地方,把另一个粒子制备到该量子态上,而原来的粒子仍留在原处。其基本思想是:将原物的信息分成经典信息和量子信息两部分,它们分别经由经典通道和量子通道传送给接收者。经典信息是发送者对原物进行某种测量而获得的,量子信息是发送者在测量中未提取的其余信息;接收者在获得这两种信息后,就可以制备出原物量子态的完全复制品。该过程中传送的仅仅是原物的量子态,而不是原物本身。发送者甚至可以对这个量子态一无所知,而接收者是将别的粒子处于原物的量子态上。在这个方案中,纠缠态的非定域性起着至关重要的作用。在量子力学中能够以这样的方式制备两个粒子态,在它们之间的关联不能被经典地解释,这样的态就是纠缠态,量子纠缠指的正是两个或多个量子系统之间的非定域非经典的关联。量子隐形传送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信。可以说,量子通信的重点在于完全传输量子纠缠的信息。1997 年,在奥地利留学的中国青年学者潘建伟与荷兰学者波密斯特等人合作,首次实现了未知量子态的远程传输。这是国际上首次在实验上成功地将一个量子态从甲地的光子传送到乙地的光子上。实验中传输的只是表达量子信息的"状态",作为信息载体的光子本身并不被传输。最近,潘建伟及其合作者在如何提纯高品质的量子纠缠态的研究中又取得了新突破。最近潘建伟等人发现了利用现有技术在实验上可行的量子纠缠态纯化的理论方案,原则上解决了目前在远距离量子通信中的根本问题。这项研究成果受到国际科学界的高度评价,被称为"远距离量子通信研究的一个飞跃"。

量子纠缠态还可用来制备光场量子态,两个子系统通过相互作用,即经历一个幺正变换过程后可以产生纠缠,从而提供所需的量子态。

量子纠缠态不仅已经应用于量子信息系统,也成为量子计算机的基础。

二、量子计算机

量子计算机是一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置。当某个装置处理和计算的是量子信息,运行的是量子算法时,它就是量子计算机。量子计算机的概念源于对可逆计算机的研究。研究可逆计算机的目的是为了解决计算机中的能耗问题。

在经典计算机中,基本信息单位为比特,运算对象是各种比特序列。经典计算机从物理上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。

量子计算机是以量子态作为信息的载体,其信息单元是量子比特(qubit),运算对象是量子比特序列。量子比特是两个正交量子态的任意叠加态,从而实现了信息的量子化。人们已提出了用光子、电子、原子、离子、量子点、核自旋以及超导体中的库珀对等物理系统作为量子比特的方案。特别是,量子比特序列不但可以处于各种正交态的叠加态上,而且还可以处于纠缠态上。这些特殊的量子态,不仅提供了量子并行计算的可能,而且还将带来许多奇特的性质。与经典计算机不同,量子计算机可以做任意的幺正变换,在得到输出态后,进行测量得出计算结果。因此,量子计算对经典计算作了极大的扩充,在数学形式上,经典计算可看做是一类特殊的量子计算。量子计算机对每一个叠加分量进行变换,所有这些变换同时完成,并按一定的概率幅叠加起来,给出结果,这种计算称做量子并行计算。除了进行并行计算外,量子计算机的另一重要用途是模拟量子系统,这项工作是经典计算机无法胜任的。

由此可见,量子计算对经典计算作了极大的扩充,经典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,所有这些经典计算同时完成,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。量子并行处理大大提高了量子计算机的效率,使得其可以完成经典计算机无法完成的工作。量子纠缠及相干性在所有的量子超快速算法中得到了本质性的利用。

三、量子计算的困难及其克服途径

量子计算的优越性主要体现在量子并行处理

薛定谔猫佯谬与重离子耗散反应激发函数的测量

王　琦　董玉川　李松林　田文栋
（中国科学院近代物理研究所　兰州　730000）

量子力学的建立与相对论的提出，是20世纪物理学最伟大的成就，它们构成了现代科学的理论基础，也是当代人类物质文明的理论基础。有趣的是，一方面量子理论已经为无数的实验事实所证实，到目前为止甚至还找不到一个与它的预言相悖的实际事例；另一方面，量子力学的基本概念又与人们对现实宏观世界的传统认知极不协调。这种不协调实质上是对量子理论的根基的质疑。所以，从量子力学诞生前后一直到现在的近百年间，对量子理论的争议一天也没有停止过。其中，最著名的议题之一就是所谓的薛定谔猫佯谬。

1935年，薛定谔提出了一个思想实验，人称薛定谔猫。他设想有一只猫被关在一个笼子里，这个笼子里有一个毒药瓶，瓶的开关由一个放射性原子装置控制。当这个装置中的原子处于激发态时，瓶子关闭，猫是活的；当原子跃迁到基态时，伴随有光子释放，毒药瓶被打开，猫立即被毒死。薛定谔用下列波函数来描述这个猫与原子组成的复合体系：

$$|\Psi\rangle = \alpha|\text{活猫}\rangle|\uparrow\rangle + \beta|\text{死猫}\rangle|\downarrow\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$

其中，$|\alpha|^2$ 表示原子处于激发态且猫是活着的概率，$|\beta|^2$ 表示原子处于基态且猫是死的概率，这个波函数表示猫处于不死不活的状态。

薛定谔用他描绘的介于生与死之间的猫，不仅想形象地说明量子力学的基本原理，而且想袒露他对量子理论的疑惑。我们知道，放射性元素中的原子不是在某一特定的时间点蜕变，而是以某种概率在某一特定的时间段内发生蜕变。换句话说，一个特定的原子的蜕变在时间上是不能准确预报的。量子理论认为，无论是粒子、光、力，还是整个世界，都具有这种不确定因素。一个粒子可以同时分布在几个不同的位置；一道光可以在这里，而同时又在另一个地方，它们相互之间能够以超过光速的速度沟通；即使真空中也存在许许多多这种不确定的微粒和波。对笼子里的猫来说，因为没有人知道原子蜕变的准确时间，所以外面的观察者也没有人知道里面的猫此时此刻是活着还是已经死了。从某种意义上说，这只猫生与死并存，或两者都无从谈起，它处于一种介于生与死之间的混合状态之中。而在现实的宏观世界中，猫非死即活，两者必居其一。猫是活的，猫也是死的，显然有悖于我们日常的生活经验，令人难以接受。

哥本哈根学派的解释是，一旦进行测量，这种奇特的、既模糊又不确定的世界，顿时就会转变为我们习以为常的、确定的可知世界，而进行测量非得采用宏观的测量仪器不可，这种遵循经典物理学定律的仪器，破坏了量子状态的叠加，它使得量子状态塌缩。这时，量子物理靠拢经典物理，微观世界过渡到

上，无论是量子并行计算还是量子模拟，都本质性地利用了量子相干性，即量子纠缠态的有效保持。失去了量子相干性，量子计算的优越性就消失殆尽。但在实际系统中，量子相干性却很难保持。消相干（即量子相干性的衰减）主要源于系统和外界环境的耦合。因为在量子计算机中，执行运算的量子比特不是一个孤立系统，它会与外部环境发生相互作用，其作用结果即导致消相干。有研究表明量子相干性的指数衰减不可避免。一旦相干性丢失就会引起运算结果出错，这就是量子错误。因此，有效地保持量子纠缠态及相干性是量子计算机进行可靠的量子运算的基本保证。

量子信息学的发展方兴未艾，最突出的特点是量子物理学的原理和计算机科学的交融和相互促进，更多的有如量子纠缠这样的量子效应也会成为当代人们耳熟能详的名词。人类也将更加积极地致力于量子技术的开发，推动科学和技术更迅速地发展。