量子信息论及其哲学思考
Quantum Information Theory and Its Philosophical Thoughts

郝宁湘
(湛江师范学院政法系　　广东湛江　524048)

量子信息论是经典信息论与量子力学相结合的新兴交叉学科, 它是一门用量子力学的世界观来重新构建信息理论的科学。如今, 量子信息论已经成为一门独立的学科, 并且在许多方面已显示了它超越经典信息论的地方。这一点可以体现在量子信息领域的两位权威 Bennett 和 DiVincenzo 最近在《自然》杂志上对量子信息所做的总结性评价上: 从经典信息到量子信息的推广, 就像从实数到复数的推广一样。[1]

一、量子信息的实质与表征

经典信息是以比特作为信息单元。从物理角度讲, 比特是两态系统, 它可以制备为两个可识别状态中的一个, 如是或非、真或假、0 或 1。在传统计算机中电容器平板之间的电压可表示信息比特, 有电荷代表 1, 无电荷代表 0。量子信息论中量子信息的基本单元是比特的量子推广——量子位 (qubit), 或称为量子比特。

直观地讲, 一个简单的量子比特是一个双态系统, 如半自旋或两能级原子: 自旋向上代表 0, 自旋向下代表 1; 或基态代表 0, 激发态代表 1。事实上, 任何两态的量子系统都可以用来制备量子比特, 常见的有: 光子的正交偏振态、电子或原子核的自旋、原子或量子点的能级、任何量子系统的空间模式等。与经典比特不同, 量子比特不但可以处在 0 或 1 的两个状态之一, 而且一般地可以同时处于两个态的迭加态。即:

$$|\varphi\rangle = c_0|0\rangle + c_1|1\rangle, \quad |c_0|^2 + |c_1|^2 = 1$$

经典比特可以看成量子比特的特例 ($c_0 = 0$ 或 $c_1 = 1$)。由 L 个量子位组成的量子寄存器能够一次存储 2^L 个"数字"。即量子寄存器随着位数的增加能够指数级地增加存储的数据量。

用量子态来表示信息是量子信息论的出发点, 有关信息的所有问题都必须采用量子力学理论来处理。信息一旦量子化, 量子力学的特性便成为量子信息的物理基础, 信息的演变遵从薛定谔方程, 信息传输就是量子态在量子通道中的传送, 信息处理 (计算) 是量子态的幺正变换, 信息提取便是对量子系统实行量子测量。[2]

那么到底什么是量子信息呢? 它是一种本质上不同于 (经典) 信息的信息吗? 还是仅为信息的量子表征呢? 如果量子信息只是一种新的表征方式, 经典信息与量子信息的区别就仅在 (信息的) 表达方式上, 而不是 (信息的) 本质的区别。相反, 如果量子信息是一种本质上不同于经典信息的信息, 那么它们的区别就不仅是在表达方式了。我们以为要回答这个问题, 就要看看用量子方式表征的信息与用经典方式表征的信息是不是等价的, 即用量子方式表征的信息都能用经典方式表征, 用经典方式表征的信息都能用量子方式表征。如果是等价的, 我们就认为, 量子信息实质上就是信息的量子表征, 而不是本质上不同于经典信息的另一种信息; 人们所谓的量子信息与经典信息有着本质的区别, 那就只能是从信息表征方式的意义上而言了。

从现在的研究状况来看, 我们认为, 量子信息就是信息的量子表征 (用量子态表示信息)。这是因为, 经典信息单元典型地表示为 0 或 1, 量子信息单元则为 0 和 1 的叠加态。即:

$$c_0|0\rangle + c_1|1\rangle, \quad (|c_0|^2 + |c_1|^2 = 1)$$

这个表征的区别并不能或并没有反映出信息本质的区别。量子叠加态只是能表示多个数 (即它可以同时表示 0 和 1), 对量子叠加态的操作, 也只是意味着对多个数同时多路操作运算, 即所谓"量子并行计算"。说得更具体点, 对于一个 L 个物理比特的存储器, 若它是经典存储器, 则它只能存储 2^L 个可能的数当中的任一个; 若它是量子存储器, 则它可以同时存储 2^L 个数; 而且随着 L 的增加, 其存储量子信息的能力将指数上升。例如, 一个 250 量子比特的存储器 (由 250 个原子构成) 可能存储的数目比现有已知的宇宙中的全部原子数目还要多。另外, 量子计算机在实施一次的计算中可以同时对 2^L 输入数进行数学运算。其效果相当于经典计算机要重复实施 2^L 次操作, 或者采用 2^L 个不同的处理器

实行并行操作。由此可见，信息的量子表征只是在信息的存储、处理(计算)以及传输方面区别于并有优越于信息的经典表征的地方。由此我们也进一步看到，信息的表征方式是多种多样的，既可以是经典的，也可以是量子的；但信息的本质是不因表征方式的变化而变化的。

信息的表征或表达是一个过去很少讨论的问题，其实它是一个很重要而基本的问题。信息是物质载体与语义内容构成的统一体，物质载体是信息表达的外在形式，语义是信息表达的内容。表达或表达方式，就是信息的存在、呈现或显现方式。众所周知，信息总是以存储、传输和处理(计算)的形式而存在、呈现或显现。因此，信息的存储、传输和处理(计算)都是以信息的表达为前提的，有什么样的信息表达方式就有什么样的信息存储、传输和处理方式。物理的、化学的，电子的、生物的，经典的、量子的，各种各样的表达方式决定了各具特色的信息存储、传输和处理方式。如今，量子信息的产生，实际上也就是找到了一种用量子表达信息的方式，由此在信息的存储、传输和处理(计算)等方面也就有了许多新的特性。

不可否认，量子信息与经典信息相比，由于它的表征方式发生了重大的变化，因而具有了许多量子力学的特性，现今认识得比较清楚的主要有：(1)量子纠缠——N(大于1)的量子比特可以处于量子纠缠态，子系统的局域状态不是相互独立的，对一个子系统的测量会获取另外子系统的状态；(2)量子不可克隆——量子力学的线性特性禁止对任意量子态实行精确的复制；(3)量子叠加性和相干性——量子比特可以处在两个本征态的叠加态，在对量子比特的操作过程中，两态的叠加振幅可以相互干涉，这就是所谓的量子相干性。这些特性是经典信息所不具备的。下面我们主要就前两种特性作些介绍，并阐述一下它们的哲学意义。

二、量子纠缠及其哲学意义

量子纠缠是存在于多子系量子系统中的一种奇妙现象，即对一个子系统的测量结果无法独立于对其它子系的测量参数。虽然近些年来，随着量子信息这一新兴领域的蓬勃发展，量子纠缠逐渐成为人们的热门话题，但它并不是什么新生事物，“纠缠”这一名词的出现可以追溯到量子力学诞生之初。早在1935年爱因斯坦同Podolsky和Rosen一起提出EPR佯谬时，便第一次提出了纠缠态的想法。不过当时谁也没有洞悉出量子纠缠态的全部含义，在经过了数十年的努力之后，它的含义才逐渐地被发掘出来。

被爱因斯坦称为“神密的远距离活动”的量子纠缠，是指粒子间即使相距遥远也是相互联结的。测量出一个被纠缠的粒子，就可推算出其它粒子的性质。因为量子力学认为粒子的基本属性存在于整个组合状态中，所以由纠缠粒子产生的密码只有通过发送器和吸收器才能阅读。窃听者很容易被查出，因为他们不可避免地要扰乱粒子的性质。

现在，量子纠缠态已被应用到量子信息的各个领域(量子通信技术、量子加密技术和量子计算技术)。对量子纠缠的深入研究无论是对于量子信息的基本理论，还是对未来潜在的实际应用都将产生深远的影响。近来美国3个独立的研究小组几乎同时在《物理评论》(5月号)上发表文章，首次论证用“量子纠缠”方式在计算机上传输机密文件。这说明“量子纠缠”不再仅仅是一个具有神秘色彩的理论概念，而且已经开始成为具有实用价值的技术。

具体地说，当两地分享了一定量的纠缠态的时候，纠缠的所有者们可以通过对纠缠态做局域操作并辅以经典通信的手段来行使量子通信、量子计算的功能。当然，这要以消耗两地共享的纠缠态为代价。纠缠状态所纠缠的粒子数量越多，对经典物理学的偏离越明显，获得有用量子效应的机会就越大。所以，在量子信息中，纠缠通常被看作是一个非局域的“信息源”。于是，如何对纠缠定量化就显得十分重要。由两子系构成的量子系统的纠缠定量化已经完成。目前，人们已广泛使用4个Bell态作为定量化两子系统纠缠的标准，每个Bell态的纠缠度定义为1，也称为一个ebit(纠缠比特)。所谓纠缠度，就是指所研究的纠缠态携带纠缠的量的多少。纠缠度的提出，为不同的纠缠态之间建立了可比关系。两态的两粒子体系的纠缠态中有如下4个Bell基：

$$|\Phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)$$

$$|\Psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)$$

它们构成特殊的表象，每个Bell基态都是双粒子体系最大纠缠态。它们是四维空间中的正交完备基，可用之对任意二粒子态$|\Psi\rangle_{AB}$实施正交测量，称为Bell基测量。每个Bell态携带非局域的两比特信息：Parity bit(宇称比特)，$|\Phi\rangle$代表偶宇称，$|\Psi\rangle$代表奇宇称；Phase bit(相位比特)，分别由+、–来表征。现已知道，两子系统中纯态的纠缠度等于任一子系统约化密度矩阵的von Neumann熵。由于两子系复合系统可以进行Schmidt分解，所以两子系统的纠缠度相等。对于混合态的纠缠度量则存在很大困难。多子系的纠缠态则具有很多为两子系纠缠态所不具备的性质，定量化非常困难，目前对其研究尚处于起步阶段。对此我们就不再介绍了。

如今，人们根据能否从两子系量子系统中通过局域操作和经典通信的手段提取出Bell态(信息)，对纠缠态进行分类。把无法通过局域操作和经典通信的手段从中提取出Bell态(信息)的这种态称为

“束缚纠缠态”；把束缚纠缠态以外的纠缠态通称为“可蒸馏的纠缠态”。最近的研究成果表明，一般的纠缠态都存在束缚纠缠态的情况。由于无法从束缚纠缠态中蒸馏出 Bell 态，所以束缚纠缠态不能胜任 Bell 态在量子通信中所扮演的角色。但近来人们发现在束缚纠缠态中存在一种“纠缠激活”的有趣现象，即当两地分享某种可蒸馏的纠缠态的同时也分享一定量的束缚纠缠态。在这种情况下，束缚纠缠态可以起到一定的“泵浦”作用，使可蒸馏纠缠态具有更强的传态能力。[3]

量子信息具有的量子纠缠这一特性，不仅在信息科学方面具有重要意义，而且也为信息的哲学研究带来了新的话题和新的实证材料。首先，由于量子纠缠，即使粒子间相距遥远也是相互联结的，测量出一个被纠缠的粒子，就能立刻得出其它粒子的性质。这一方面说明粒子的基本属性存在于整个组合状态中，反映了大自然深层的整体论特性。另一方面也表明，信息的传输可以不需要时间——信息传输过程中的这种带有神秘色彩的超距作用，使人们对信息又有了新的认识。这或许正是信息与物质最大的区别之一：物质的传输不具有超距作用，但信息的传输却具有这种“神秘”的超距作用。我们猜测，随着对信息传输的超距作用的进一步认识，将对人类的意念、意识等精神现象（其中有些是颇为神奇的）有一个真正科学意义上的说明。量子信息这一特性的意义在今天还是难以说清楚的。

另外，束缚纠缠态的存在，揭示了自然界更为深刻的一面，即信息的不可逆过程，这很类似于热力学中的熵增加现象。以往人们对信息的守恒与不守恒有过种种争论，各持其词。如今束缚纠缠态的发现，深刻地说明了信息的不守恒性。大家知道，物质不灭、能量守恒、新物质的产生以旧物质的毁灭为代价，所以物质资源可以出现短缺，同样也有能源危机。但由于信息的不可逆性或信息的不守恒性，信息资源不存在短缺的问题，存在的只是信息的获取、传递、加工、利用等问题。“没有什么信息”实质指的是没看到原事物或原事物信息的记载。这就提示我们对信息反映的事物有时也要保护。例如：古文化遗址，作为物质来说可能并不特殊，表面上存留与否并不重要，但作为信息来说，若把它损坏，那么有些重要信息就丢失了。还有信息传递，这是通信理论和通信工程所要解决的问题，因为信息也可能丢失。另外，信息有语用信息这一层的描述，它的价值不仅与客观事物本身有关，更重要的是与使用者所具备的知识能力及时间有关，所以要求我们及时、合理、科学地利用信息。

三、量子不可克隆定理及其哲学意义

自从克隆羊“多莉”出世以来，克隆一词便家喻户晓。一些人还在为能否克隆出爱因斯坦和希特勒争议不休。人们在进一步关注这样一个根本性的问题——克隆技术是否万能？殊不知，早在 1982 年，wootters 和 zurek 在《自然》杂志上就发表了一篇短文，指出一个未知的量子态不可能克隆（精确复制）。这就是量子不可克隆定理，它限制了克隆技术的适用范围。

准确地说，该文提出了这样一个问题：是否存在一种物理过程，能实现一个未知量子态的精确复制，使得每个复制态与初始量子态完全相同。文中证明，量子力学的线性特性禁绝这样的复制，这就是量子不可克隆定理的最初表述。[4]

量子态不可克隆是量子力学的固有特性，它设置了一个不可逾越的界限。量子不可克隆定理是量子信息科学的重要理论基础之一。量子信息是以量子态为信息载体（信息单元）。量子态不可精确复制是量子密码术的重要前提，它确保了量子密码的安全性，使得窃听者不可能采用克隆技术获得合法用户的信息。鉴于该定理的重要性，近年来人们对它作了进一步的研究，揭示出更丰富的物理内涵。

wootters 和 zurek 的证明是基于量子叠加原理，该证明行之有效至少需要 3 种可能的输入态，因此它没有排除克隆两个量子态的可能性。之后人们推广了量子不可克隆定理，使之适用于两态情况，指出如果克隆过程可以表示为一幺正演化，则幺正性要求两个态可以被相同的物理过程克隆，当且仅当它仍相互正交，亦即非正交态时不可以克隆。该结果在量子密码术中有重要应用。我们知道，一个简单的量子密码方案就是随机地传送两个非正交的量子态，正因为非正交态不可以克隆，所以窃听者无法窃取信息。

适用于两态的量子不可克隆定理后来进一步推广到混合态情况，并证明了一个更强的定理，文献中称为量子不可播送定理。该定理是量子不可克隆定理的强化，当有关的量子态为纯态时，显然量子不可播送定理回到两态的量子不可克隆定理。近来不可克隆定理又被推广到纠缠态情况。有人甚至指出复合系统的正交态也不可以被克隆。当然，这种正交态的不可克隆定理需要狭义相对论做基础。

总之，量子不可克隆定理断言，量子态的非正交态不可以克隆，但它并没有排除非精确克隆即复制量子态的可能性。目前主要有两种克隆机：普适克隆机和概率克隆机。这里我们仅仅介绍一下由我国科学家（中国科技大学的郭光灿、段路明）提出的概率量子克隆机（段—郭克隆机）。概率量子克隆机适用于线性无关的态集。它把幺正演化和测量过程相结合，以确定的大于零的概率产生输出，而且输出态一定是输入态的精确复制态。为构造概率量子

克隆机，测量和合适的幺正演化都是不可缺的。如果只有幺正演化，显然非正交态不可以精确克隆；另一方面，如果只有测量，当输入态为非正交态时，机器不可能对其中任意一个输入态都以大于零的概率产生输出，且输出态还应是输入态的精确复制态。因此构造概率量子克隆机的关键是要设计出合适的幺正演化并要联系测量过程。

概率克隆的含义是，测量的结果分为两类，一类结果为“成功”，另一类结果为“失败”。当测量结果为“成功”时，我们就确知该过程已产生了输入态的精确复制态；反之，若测量结果为“失败”机器的输出态，就不是输入态的复制态，我们就抛弃该输出态。我们要求机器成功地克隆输入态的概率大于零，并希望它尽可能大。应该注意的是，概率克隆与非精确克隆是两个有区别的概念。既然从一组非正交态中随机选出的态不可能通过幺正演化精确克隆，那么在非精确克隆中，人们就放松要求，允许输入态和输出态之间存在差别，但希望该差别尽可能小。因此，一个用于非精确克隆的机器对于每个输入态都能产生输出，但是对从非正交态集合随机选出的量子态，其输出与输入之间总存在差别。与此不同的是，概率克隆机的输出一定是输入态的精确复制态，但对于非正交态，有时候机器没有输出（对应于测量结果为“失败”）。[5]

量子不可克隆定理的证明，是量子力学中海森伯测不准原理在量子信息论中的直接反映。因为如果可以对单个未知量子态进行克隆，那么通过对其大量复制品的重复测量，人们便可以由此获得该量子体系的所有性质，达到精确测量的目的，而这是测不准原理所不允许的。海森伯测不准原理在哲学上已有过许多的讨论，量子不可克隆定理的证明无疑有助于我们认识测不准原理的哲学性质。

另外，量子不可克隆定理的证明也说明信息的不可精确认识性。世界是模糊的，在人类的面前它有着无法揭开的“隐私”。这“隐私”是根本性的，我们只能可望而不可及。可以说，这又是一个典型的限制性定理。20世纪有着许多最深刻和最令人难忘的科学结论，就是关于“什么不可为和什么不可知”的陈述，哥德尔不完备性定理、海森伯测不准原理是其中最著名的代表。如今，在信息世界中又有一个量子不可克隆定理，这进一步有理由使人相信，或许存在着某种科学所永远无力揭晓的关于自然和人类世界现象的答案。

由上可见，量子力学和信息论这两个看起来互不相关的学科，实际上却存在着内在的联系。量子信息可以被说是经典信息与量子纠缠的互补。经典信息可以被放任地任意克隆，但只能从时空中的一点传到后面的一点；而量子纠缠不可能被克隆，但可以把时空中的任意两点联系起来（非局限性）。

总之，量子信息论是一门新兴交叉学科，尽管量子信息论的基本框架已经形成，但还有许多尚待解决的问题。其中还有许多内容本文尚未介绍到，如量子通信（包括其中重要的量子隐形传态、量子密码理论等），以及刚刚兴起的量子对策论。这些内容不仅在量子信息论中有着重要的作用，而且在哲学上也有着它们各自的意义——这些留待以后再论。最后，我们引用我国著名量子信息论专家郭光灿和其伙伴的一句话：我们有理由相信量子信息科学的明天会更加光明灿烂，人类从信息时代进入量子信息时代已不再是一种梦想。

参 考 文 献

[1] Bennett. C. H. and DiVincenzo D P. Nature, 404(2000), 247~255

[2] 李传锋，郭光灿．量子信息研究进展．物理学进展，2000(4)

[3] 周正威，郭光灿．量子纠缠态．物理 2000(9)

[4] W. K. Wootters, W. H. Zurek, Nature, 299(1982), 802

[5] 郭光灿，段路明．量子克隆与量子复制．物理，1999(1)

（责任编辑　王宏章）

科技动态

发光硅研究取得重大进展

据英《新科学家》2002年11月16日报道：意大利的ST公司研究出一种在电流通过硅时使硅发光的技术，这预示着电子装置可能发生革命性变化。因为它意味着不再是用电而是用光相互发出信号，可以去掉导致过热和降低微型芯片速度的一层接一层的连接导线。

该公司声称，它已在室温下实现了10%的量子效应。这就是说，在电子装置中每注入10个电子，就能发射出1个光子。这一效率比以前任何研究所能达到的硅的电光转换效率高100倍。这一消息使某些与之竞争的研究人员大为“光火”，因为他们已经花了好几年的时间在研究发光硅，却从来没有达到过如此高的电光转换效率；因此他们对ST公司的成果表示极大怀疑，说：“这简直是笑话，如果他们真能达到10%的效率，我们就去种地算了”。

具体情况是，ST公司实验室的Salvo Coffa研制了一种掺有饵离子（一种稀土元素）的新型硅基半导体。方法是把饵离子掺入一层二氧化硅中，再用细小的纯硅纳米晶体密集地填满。电子注入这层二氧化硅后通过纳米晶体网运动，直到碰撞并激活饵离子。当饵从激活状态衰减松弛进入基态时，它就发出一个光子。这种跃迁的能量变化就是光子的能量，它近便地正好落到了通信所需的能量区域内。

ST公司的第一个发光硅产品可能将用光信号把电

（下转第64页）