量子计算机五条原则,量子信息科学：量子计算机、隐形传物与人脑量子运算

转载

penddymkq 于 2021-07-15 03:49:54 发布 84 收藏
文章标签： 量子计算机五条原则

自然界有三个要素：物质、能量和信息：相应的有三类学科：物质科学、能源科学和信息科学。量子力学的诞生从根本观念上改变了人类对自然的认识，20世纪人们将量子理论应用于物质科学和能源科学，开拓出诸如半导体、激光、核技术等重要高新技术，造就了人类文明社会半个世纪的繁荣昌盛。

21世纪，一门新兴的交叉学科——量子信息科学应运而生，它是量子力学与信息科学相互融合的结果。它以量子理论特有的量子态作为信息单元(称为量子比特)，信息的产生、处理、传输和检测均遵从量子力学的规律，于是量子力学固有的特性，如叠加性、纠缠性、非局域性、不可克隆性等，开发出经典信息所无法做到的新功能，在加快运算速度、确保信息安全和增大信息容量等方面突破经典信息科学的物理极限。因此，量子信息科学的诞生使信息科学的发展从“经典”跃进到“量子”时代。量子信息在人类文明社会的发展历程中将会带来难以估计的影响。

目前，量子密码已接近于实际应用：量子通信网络的研制处于关键科学和技术问题有待突破的阶段：量子计算仍处于基础研究阶段，发展的“瓶颈”在于如何研制出可扩展量子比特的物理体系，人们坚信，量子计算机的实现不存在不可逾越的原则困难，量子计算机的诞生只是迟早的事。量子信息科学的诞生，一方面可望形成量子信息技术(QIT)新产业，另一方面也引发人们对某些更深层问题的思考，这些问题的研究反过来将深化人类对自然界及人类自身的认识。

一、量子计算机究竟是什么样？它的功能有多大？

量子计算机基于量子图灵原理，其结构类似于现有的经典计算机，然而量子计算有其独有的特性。例如，量子计算机用来运算某函数，数据编码在量子计算机的初始量子态上，函数的运算体现在量子计算机施加于初始量子态上的幺正操作上，运算的结果通过对量子计算机终态实施量子测量而获得。在运算过程中，若对物理体系量子态进行测量会导致量子态的明缩、干扰甚至破坏量子运算过程。因此，适应于这个特性的量子计算网络应选取什么样的结构才能优化量子计算机的性能，便是新的研究课题。

量子操作可分解为基本通用量子门的某种组合，单个量子比特的旋转门和两个量子比特的受控非门便属于这类基本量子门，其中量子受控非门是非局域门，它依靠两个物理量子比特之间的相互作用来实现，显然，在量子芯片相距较远的两个量子比特之间要直接实现这种非局域操作难度较大，这就增大了量子计算机结构的复杂度。人们想方设法来降低这种复杂度，例如，通过量子隐形传态这类“量子软件”将量子芯片结构的复杂度转化成量子态制备和传送的复杂度上。最优结构的量子计算机是否就是量子硬件和量子软件某种最优的配置呢？

量子计算实际应用的最主要障碍是环境不可避免的消相干过程，它破坏量子体系的量子相干性，导致量子计算机自动地演变为经典计算机，于是量子计算机便丧失掉其并行计算的能力。克服消相干的有效办法是量子编码，原则上采用量子编码可以实现容错的量子计算，其代价是引进信息冗余度，即用若干量子比特来编码一个量子比特的信息，这样便会大大地增加量子计算机结构的复杂度。

总之，鉴于量子计算的固有特性，未来实用的量子计算机应是个什么样？仍然有待探索。

另一方面，量子计算的强大运算能力源于量子叠加性，因而可实施量子信息的并行处理，应用合适的量子算法便可加快某些函数的运算速度。如Shor量子并行算法能以指数效率加快与离散傅里叶变换相关的某些面数的运算，Grover量子搜寻算法能以开根号效率加速从数据库中寻找某个数据的速度，人们期待着多的有效量子算法的实现，以更充分地发掘量子计算的运用潜力。那么，量子计算的潜力究竟有多大？是否在电子计算机上难以运算的问题借助量子计算机都可以求解？量子信息科学的诞生动摇了现有计算复杂度的理论基础，人们是否能建立新的更深刻的计算复杂度理论？它将对计算机的发展产生什么样的影响？

二、信息战中保密和破密的攻防之争是否真的终结了？

在人类历史的舞台上，信息战中保密和破密的攻防之争曾上演过一幕幕惊心动魄的场面。业已证明，量子计算机可以攻破RSA和ECC的公钥体系，也可以攻破DES的私钥体系。因此，一旦量子计算机研制成功，现有密钥体系将被攻破，幸好人们又证明，量子密码体系可以抵挡住量子计算机的攻击，它提供不可破译、不可窃听的绝对安全的保密通信系统。2003年美国《时代周刊》把“量子加密”列为“改变人类未来的十大新技术之一”。似乎，量子密码的诞生就可终结信息战中这场攻防之争。果真如此吗？

量子信息技术确实把信息战从“电子对抗”带进到“量子对抗”的新阶段。然而，有“矛”必有“盾”，在量子时代，这场争斗将会延续下去。量子计算机可以攻破现有的公钥体系，这些体系的安全性是建立在诸如大数因子分解这类在电子计算机上难解的问题之上的，鉴于量子计算将这类难解问题变成了易解问题，从而导致这类公钥体系失去其安全性的基础。然而人们会问，倘若量子计算机无法有效地求解所有电子计算机难解的问题，那么就存在这样的可能性，即可以应用量子计算机无法求解的函数，来建立新的公钥体系，确保通信的安全性。这并非绝对不可能！

另一方面，量子密码技术是将量子密钥分配的不可窃听性和一次一密的不可破译性相结合，确保了量子通信的安全性。理论上，量子密钥分配可以发现任何物理定律所允许的窃听行为，然而，实际的量子密码系统绝不可能是理想的，系统的不稳定性、噪声、探测器的暗计数、不理想的探测效率等都无法确保绝对安全性。窃听者是否能借助于环境曝声作隐蔽成功地窃取信息？为减少噪声的影响，有种方案是将单个光子一次传输改变成返回传输，结果确实显著地提高了系统的稳定性，但人们发现，这个方案会由此产生新的不安全隐患，人们可采用特洛伊木马光子窃取密钥而不被发现。量子密钥分配的速率远远低于传递文本所需的比特速率，因此，就不易实时地做到“一次一密”，于是人们在诸如加密算法等方面做了改进，这样一来，能否确保“绝对安全”便成为新的研究课题。

总之，量子密码学确实为密码学带来根本上的变革，然而这并不意味着信息战的长期争斗从此终结，而是另一轮新的争战重新开始罢了。

三、隐形传物果真能实现吗？

在科幻电影或神化小说中，常常有这样的场面：某人突然在某地消失，其后却在别的地方莫名其妙地显现出来，“隐形传物”(teleportation)一词就来源于此，这是指一种无影无踪的传送过程。从物理学角度，人们可以这样地想像隐形传送的过程：先提取原物所有的信息，然后将这个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(如原子)，制造出原物完美的复制品。遗憾的是，量子力学的不确定性原理不允许精确地提取原物的全部信息，这个复制品不可能是完美的。因此，长期以来，隐形传物只不过是一种幻想而已。

1993年，Bennet等在PRL上发表一篇开创性的论文，提出量子隐形传态的方案：将某个粒子的未知量子态$|\varphi\rangle$传送到另一个地方，把另一个粒子制备到态$|\varphi\rangle$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之后，就可以制造出原物量子态的完全复制品，这个过程中传送的仅仅是属物的量子态，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(甚至可以是与原物不相同的粒子)处于原物的量子态上，原物的量子态在此过程中已遭破坏。

目前，实验土已实现了单个粒子量子态的隐形传送，随着Bell基测量技术的发展，人们相信，光子、原子、离子等单个粒子的粒子隐形传态不存在原则上的障碍。于是，人们不禁要问：人类是否最终能实现隐形传物？就像“封神榜”上“土行孙”那样，在某处突然消失掉，随后出现在宇宙的任何想去的地方，古老的神话最终会变成现实！

原则上讲，物体是由某些基本成分(如原子)构成，两个由完全相同种类、相同数量的基本成分以完全相同的方式构造而成的物体看起来是一模一样的。按照量子理论，世界是量子的，每个物体原则上可用相应的量子态来描述，两个外观相同的物体只有当他们处于相同的量子态时，在物理上才可视为不可区分的相同物体。假定某个欲被传送的物体处在某量子态|φ>，运用量子隐形传态的方法，原则上可将态|φ>传到远处，使其原先的量子态被破坏而变成另一个态，从信息学角度看，原物消失了，而在远处重新出来这个物体。因此，原理上讲，量子隐形传物是可行的，当然要实际做出来却困难重重。

即使我们具备有实现隐形传物的能力，要实现隐形传送人或其他生物也是难以想像的。量子隐形传态必须将经典信息传送同量子信息传送相结合才可能实现。迄今人们仍不能确定，生命过程和生物体如何用量子力学来描述，有人甚至认为这根本是不可能做到的事。因此，隐形传人能否实现就涉及更多的未知数，起码按照、目前人们所采用的量子隐形传态的原理和方法是如此！那么，究竟是目前人类的智力所不能及，但总有一天能做到呢？还是这根本上就是一个神话而已？

四、量子计算机可以模拟宇宙的演化吗？

量子计算机具有巨大存储数据的能力，存储量随量子比特数N指数增加。一台由300个量子存储单元构成的小型量子计算机可以存储的数据比宇宙中原子数目还要多。设想，我们将来制造一台超级量子计算机，其存储数据的能力当然是难以想像的，那么，我们可否用这台量子计算机来模拟宇宙的演化呢？宇宙是量子的，用量子计算机模拟其演化，计算复杂度是多项式函数，因而是个可解问题。宇宙诞生于“大爆炸”，初始状态是真空态，因此，如若我们能正确地研究出驱动宇宙演化的哈密顿量，并用之来操控量子计算机的运行，原则上讲，

我们就能正确地模拟宇宙的演化过程，从诞生起如何演化到现在，然后从现在又将如何演化到未来。这个命题十分有趣，但不难想像也是相当困难的，也许是幼稚可笑的。当我们谈到“宇宙”，自然包括宇宙中的一切，所有的星体、黑洞、暗物质等，以及所有生物，甚至包括用来模拟宇宙演化的那台超级量子计算机本身，这似乎陷入不可解的循环之中！计算机能否模拟计算机自身的演化？

当然，若我们将研究对象界定在宇宙中某个“子集”内，那么这台超级量子计算机是可以模拟其演化的，只要研究清楚“子集”的初始状态，支配其演化的哈密顿量，包括'子集'外部对它的作用。至于这个能被模拟的“子集”的范围有多大，取决于人类的智力发达水平和这台超级量子计算机的能力。

五、人脑是台量子计算机吗？

“人脑”十分奇特，其功能是任何先进仪器所无法比拟的。随着人类对“脑功能”认识的深入，便不断地开发出模拟脑功能的更精密的仪器。但人脑究竟是如何运作的呢？人的敏感性和分辨能力显然与其处理信息的能力紧密相关。人眼观看物体时是采用扫描式的串型处理外来的信息呢？还是高度平行处理这些信息？有人说，人脑是台量子计算机，它具有量子计算的超强信息处理能力。然雨，无论是神经元或其他作为信息处理的基元，其消相干过程非常之快，以至于“大脑”的系统的量子相干性会迅速地消失掉！单从这点看，大脑不可能实现量子计算。

当然，人们已证明，量子编码可以有效地抑制消相干，它以引入信息冗余度为代价来实现容错的量子计算。也许大脑具有自动量子编码的能力？一旦外界有信息输入，大脑便自动地启动相应的程序运作：根据外部信息来制备脑信息处理单元的量子态，施行并行信息处理过程并自动启用量子编码程序，迅速提取最终的处理结果，传送到大脑相关的区域。当然这只是个纯属主观想像的图像。

总之，要证明人脑确实是如同量子计算机那样运作，目前还缺乏可靠的科学依据。必须具有在量子力学的框架下研究脑功能过程的能力和条件，才可以给出正确的答案。

当然，倘若人们已研制出超级量子计算机，用它来模拟人脑的信息处理过程，这倒可能是个好的研究课题。

郭光灿，中国科学院院士，教授，光学和量子信息专家。1942年12月9日出生于福建患安，1965年毕业于中国科学技术大学无线电电子学系。现任中国科学院中国科学技术大学量子信息重点实验室主任，中国物理学会量子光学专业委员会主任，国家科技部“973”项目“量子通信与量子信息技术”首席科学家。已在Phys.Rew.Lett、Phys.Rew.A发表主要论文220多篇，被SCI他引600余次。曾荣获国家自然科学二等奖、何梁何利奖和中国科学院自然科学二等奖。主要研究兴趣在于量子光学、量子密码、量子通信和量子计算的理论和实验研究。曾提出概率量子克隆原理，并推导出最大克隆效率公式“段-郭概率克隆机”、“段-郭界限”；在实验上研制成功概率量子克隆机和普适量子克隆机；发现不会消相干的“相干保持态”，并提出量子进错编码原理；提出一种新型的量子处理器，可有效地降低腔消相干的影响，并实现多种信息功能；在实验上验证了可否定与环境无关隐参量理论的K-S理论；发现奇偶相干态的奇异特性；在实验上研制成功远距离的量子密码保密通信系统，理论上提出“千言道加密”的新方案等。