量子信息、量子通信和量子计算释疑

施　郁

（复旦大学物理学系　200433）

1. 什么是量子信息

目前，量子通信和量子计算是国际上的研究热点，它们都属于量子信息科学。对于这个领域，存在不少困惑和不解。在本文中，笔者对若干问题作一些解释。

传统的信息服从的规律与量子力学无关，虽然很多信息处理的微观物理过程用到量子力学。这称作经典信息，其基本单元，即比特，可以表示成 0 和 1 这两个 2 进制数。随着承载经典信息的载体越来越小，量子力学将开始起作用，所以经典信息处理向小尺寸的延续会遇到极限。

微观系统是量子系统，由量子态描述。人们可以利用这一点，化不利因素为有利因素，直接用量子态来代表信息。这就是量子信息，服从量子力学规律。

量子信息以量子比特为基本单元。量子比特就是以两个量子态 $|0\rangle$ 和 $|1\rangle$ 为“基本单位”的量子态，就好比平面上的任何矢量 (有方向和大小的箭头) 以两个互相垂直的单位矢量为基本单位。事实上，量子态在数学上也是一种矢量，而“基本单位”称作“基矢态”，一套基矢态称作一个基，就好比一个坐标系。一个量子比特的任意量子态可以是两个基矢态的任意线性叠加，就好比平面上的任意一点由两个坐标确定。

2. 量子纠缠

N 个量子比特有 2^N 个基矢态。两个或者以上的量子比特构成一个复合量子系统，它的量子态可能是所谓的量子纠缠态，这是指子系统没有独立的量子态。数学上来说，整体的量子态不是子系统的量子态的直积。比如两个量子比特可以处于量子纠缠态

$$\frac{1}{\sqrt{2}}(|0\rangle|0\rangle-|1\rangle|1\rangle)。\qquad(1)$$

有一个比较广泛的误解，认为量子纠缠与相对论有矛盾。

事实上，作为量子力学中的一个概念，量子纠缠体现了一种非定域关联，与定域实在论矛盾，但是与相对论不矛盾，因为这是量子态的纠缠，纠缠粒子之间并没有超光速的物理信号传送。而且，短程的量子纠缠在各种量子系统中是自然、广泛地存在的，不纠缠的情况才是特例。比如，十几年前，笔者提出量子纠缠概念可以用来研究多体物理和量子场论。关于贝尔定理的研究只是要揭示它与定域实在论的矛盾，并不是量子纠缠这个概念本身及其应用的前提。

困难在于在实际中产生并维持某些量子通信过程需要的长程纠缠以及量子计算中需要的可控的大量量子比特的纠缠。在理想情况下，两个粒子如果存在与时空无关的内部自由度的纠缠态，那么无论它们相距多远，对此都没有影响。但是在实际中，与这个自由度耦合的环境会破坏这个量子纠缠态。而量子态对环境扰动是非常敏感的。如果要保持原先的量子纠缠，就需要克服环境扰动。因此量子信息，特别是量子计算的物理实现，还有很长的路要走。但是千里之行始于足下，需要从简单的情况逐步前进。

3. 量子通信

量子通信指在不同地点之间传送量子信息，是个比较广泛的概念，可以有各种各样的方案和目的。2016 年 8 月 16 日，中国发射了一颗量子科学实验卫星，可用于星地之间的量子通信以及向相距很远的两地分发相互之间具有量子纠缠的光子，等等。

量子通信中的一个重要内容是量子密钥分发（或称分配、协商、分享，等等）。普通文本可以通过一个密钥变为加密文件，比如一串 2 进制数串加上另一串 2 进制数串构成的密钥，就变为加密的 2 进制数串。密码术的主要问题不是加密文件的传送，而是密钥分发。因为敌手可以分析多个使用同一密钥的加密文件而破译密码，所以为了安全，最好使用一次性的密钥。传统来说，这是很困难的，所以一次性密钥只用于特

别重要的领域。而一般领域采用公钥系统，比如 RSA 系统 (美国科学家李维斯特 (R. Rivest)、萨莫尔 (A. Shamir) 及阿德曼 (L. Adleman) 在 1977 年开发的一种加密与鉴权系统)。但是它们是以不存在有效分解整数的算法这个假设为基础的，所以如果有人发现了这样的经典算法，或者量子计算机实现，这些公钥系统就瓦解了。

量子密钥分发提供了新的产生密钥的方法，目的是让双方共享一组只有他们知道的密钥。它用量子方法生成一串经典比特，作为文件加密所需要的密钥。也就是说，密钥本身是经典的。其中一个主要方案是 BB84，由美国 IBM 研究实验室的班尼特 (C.Bennett) 和加拿大蒙特利尔大学的布拉萨德 (G. Brassard) 于 1984 年发明。它是一个利用量子力学的不同基的测量之间的不相容，并借助公开的经典信道来产生私钥的方案。细节可参见本文最后提及的文献。

另外一些量子通信过程利用量子纠缠进行，比如英国牛津大学的艾克 (A. Ekert) 于 1991 年提出 E91 量子密钥方案。假设 A 和 B 分别控制一个量子比特，这两个量子比特处于 (1) 式所列的量子纠缠态。 A 和 B 在同样的基上 (类似于选择同样的坐标系) 测量各自拥有的量子比特，所得的结果必然是一样的。A 和 B 用若干对处于这个纠缠态的量子比特，分别在两种基中随机选择测量基，然后交流所用的基，保留相同的基得到的结果，就可以得到一个二进制数串，作为共享的密钥。其他人事先不知道两人分别用了哪个基，所以无法窃听。

量子密钥分发产生的只是密钥，而不是加密文件。为了这个密钥分发的安全，当发现有窃听者时可以暂停一下。这谈不上为了安全而牺牲通信的稳定性。有人认为量子通信使得敌手消失了，有了敌手就干不成事。事实上，让敌手无法隐遁与让敌手消失不是一回事，敌手总是存在的，让他们无法隐遁是一大优点。经典的一次性密钥的分发除了安全问题，也是“有了敌手就干不成事”。相比于经典公钥系统依赖于数学上没有证明的假设以及量子计算机还没有实现的情况，量子密码术依赖于物理定律，是彻底的安全保障。这是一个范式改变。密码学工作者不必墨守成规，只考虑敌手能窃听成功的传统情况。而且，这样产生的私钥通过公开信道产生，在这一点上比携带或者用经典方式传送一次性密钥不但更安全，而且更方便。

量子密钥分发虽然利用了量子态，但是最后产生的密钥仍然是一串经典的比特串，然后可以用于传统的经典加密和经典通信。量子通信并不排斥经典通信，反而是与之结合。在量子隐形传态中，经典通信也是必不可少的一环。

而且量子通信是个广泛的概念，不仅有密码术，还有其他各种各样的过程。比如利用量子纠缠还可以进行量子隐形传态。A 和 B 除了分别拥有处于以上纠缠态的两个量子比特外，A 还拥有另一个量子比特，其量子态 $|\varphi\rangle$ 可以是未知的。A 对他控制的两个量子比特在某个特定的基上进行测量。这个基称作贝尔 (Bell) 基。A 的测量结果有 4 种可能，将此结果用经典通信方式通知 B。B 据此对他控制的量子比特作相应的某种操作，就可以使得这个量子比特处于量子态 $|\varphi\rangle$。

4. 量子计算

量子计算是在一个由很多量子比特组成的机器上根据某个算法完成一系列幺正变换。幺正变换即量子态的演化，归根到底由量子力学的薛定谔方程实现，是量子力学中的基本过程。最后再进行量子测量，从而解决数学问题。正如经典计算可以由几种简单的门操作组成，量子计算的幺正变换也可以由几种简单的幺正变换，即量子门操作组成。设计好的一系列幺正变换就是量子算法。

量子计算的步骤如下。首先使量子计算机的量子态处于某个确定的初态，然后操控它完成规定的一系列幺正变换，最后进行测量。为了完成某个特定的计算任务，就必须给出相应的量子算法，规定完成哪些幺正变换及如何进行测量。

量子计算受到普遍重视在很大程度上是因为 1994 年 Shor 算法的提出 [P. Shor, Proc. 35th Annual Symp. Foundations of Computer Science 124 (IEEE, 1994); SIAM J. Sci. Statist. Comput. 26, 1484 (1997)]。Shor 算法用于将一个正整数有效地分解成素数的乘积。因为 2 是偶数的因子，所以这个任务本质上是求正奇数的素数因子。“有效”是指计算时间是这个正整数的 2 进制位数的多项式函数 (即这个 2 进制位数的有限个各

种乘方，乘以系数再相加)。这在目前公开的经典算法中是不可能的。这个不可能正是现实生活中的很多保密方案 (比如上面所述的 RSA 系统) 的基础。所以如果量子计算得以实现，很多经典保密方案就失效了。而量子算法对经典算法的超越往往与量子纠缠有关。

对于素因子分解这个任务，最好的经典算法需要 $\exp(O(L^{1/3}(\log L)^{2/3}))$ 次操作。这里符号 O(X) 代表上限是 X 乘以一个常数，$L=\log_2 N$，N 是需要因子化的数，也就是说 L 是 N 的 2 进制位数。而 Shor 算法只需要 $O(L^2 \log L \log\log L)$ 次操作。因此我们说量子算法可以有效地解决因子分解问题，而经典算法不能。

下面简单描述一下 Shor 算法。对于将要素因子化的奇数 N，准备 2 个寄存器。所谓寄存器，就是若干量子比特。第 1 个寄存器由 t 个量子比特组成，t=O(L)，可取 t=2L。第 2 个寄存器由 L 个量子比特组成。首先使第 1 个寄存器的初态处于所有 2^t 个比特态的等振幅叠加态，也就是说其中每个量子比特是基矢态 $|0\rangle$ 和 $|1\rangle$ 的等振幅叠加态。而第 2 个寄存器的每个量子比特都处于 $|0\rangle$ 态。所以这两个寄存器的态称为

$$\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}|k\rangle|0\rangle 。$$

然后由某种幺正操作实现指数模操作，也就是说使得这两个寄存器的态演化为 $\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}|k\rangle|f(k)\rangle$，其中 $f(k)=x^k \bmod(N)$，即 x^k 除以 N 的余数。

然后再对第 1 个寄存器作所谓逆傅里叶变换。最后对第 1 个寄存器测量。由测量结果可以得到满足 $x^k \bmod(N)=1$ 的值 r。如果 r 是偶数，可以有很大的几率从一个公式直接得到 N 的因子。如果实际测量中没有得到，或者 r 是奇数，则重新执行这个量子算法。

量子算法的论证是通过对任意初始基矢态进行的，从而给出从一般情况的叠加态中的任意一项出发所需要的量子门操作，即幺正变换。这也就给出了从叠加态出发所需要的量子门操作。这是量子力学基本的线性叠加原理所致。 从另一个角度来说，这些量子门操作 (幺正变换) 构造好以后，是不依赖于被作用的初始态的。比如，正如舒尔 (P. Shor) 的原文以及尼尔森 (M. Nielsen) 和艾萨克创 (I. Chuang) 的著作指出的，指数模操作只需要 $O(L^3)$ 个量子门操作，与任意叠加态的项数无关。

我们再说一下 Shor 算法中最后的测量。这个测量实际上只是对于第 1 个寄存器而言。但是因为第 2 个寄存器从此没有任何操作，所以根据所谓隐性测量原理，可以假设对两个寄存器同时测量。这不改变第 1 个寄存器的测量结果的几率分布，但是使得讨论方便。根据量子力学的规则，这个联合测量的概率用两个寄存器各取某值所对应的基矢态与原量子态的内积的模平方得到。这是联合概率。在 Shor 最初的论证中，他引用了数学上一个基于联合概率的结论。

Shor 算法和其他量子算法之所以能够比经典算法指数级加快，是因为巧妙地使用了纠缠态。所以量子计算在实际上的物理实现需要操控大量的纠缠的量子比特，这是研究的目标。基于量子力学原理的量子纠缠概念本身没有问题，量子算法的研究作为理论工作可以先行展开。

正奇数因子化的最简单的非平庸例子是 15。为此目的，一般情形下，Shor 算法的两个寄存器分别需要由 8 个和 4 个量子比特组成。迄今报道的用 Shor 算法分解 15 的实验中用到的量子比特比这少。这是因为这些实验只是在知道答案的前提下的特殊演示，而不是作为实际使用的量子计算机。在原来的算法中，指数模运算中的指数的底数需要随机选择。但是在这些演示实验中，利用了 15 因子化的答案，这个底数是事先确定的，这就导致量子比特数可以减少。21 的因子化也类似地演示过。让我们期待经过更多努力后，将来会实现可以随机选择底数的 Shor 算法实验。

5. 结语

总之，量子通信和量子计算的物理实现与工程实践会遇到不少需要解决的问题，但是基本原理是清晰的。作为一个交叉学科，量子信息领域既有很多物理学家，也不乏计算机科学专家，比如 Shor 和 Brassard。这个领域较权威的著作是 M. A. Nielsen and I. Chuang, Quantum Computation and Quantum Information (Cambridge University, Cambridge, 2000)。关于量子态、量子纠缠和量子通信更详细的通俗介绍，包括 BB84 量子密钥方案和量子隐形传态，可以参见本人的另一篇文章 [施郁，揭秘量子密码、量子纠缠与量子隐形传态，自然杂志，38 (4)，241 (2016)]。