量子计算机、量子通信学习中的最大难点

张凤祥

华中科技大学计算机学院，武汉，430073
fxzhang@hust.edu.cn

摘　要　本文指出在量子计算机和量子通信的学习中存在的几个最大的难点，一是在量子计算机的 Qbit 中 0 和 1 共存的问题。例如 8 个 Qbit 表示的数，不是一个，而是 256 个，而在电子数字计算机中 8 位 bit 只能表示一个 8 位数。二是量子计算机的并行运算，为什么量子计算机的计算速度要快电子数字计算机计算速度快那么多倍。三是量子通信中的 2 个纠缠的量子的超距和传送信息不要时间。这些都是与经典科学格格不入的，或者讲经典科学认为是伪科学的。

关键字　量子计算机，量子通信，量子纠缠，超距

Biggest Challenges in Study of Quantum Computers and Quantum communications

Fengxiang Zhang

School of Computer Science and Technology,
Huazhong University of Science and Technology Wuhan, 430073 china
fxzhang@hust.edu.cn

Abstract—The paper presents three most challenging aspects in the study on quantum computers and quantum communications. 1), the coexistence of 0 and 1 in Qbit in quantum computers. For example, eight Qbits does not represent one value but 256 values. In contrast, eight bit in conventional digital computers can only denote one value at a time. 2), the parallel computation in quantum computers. Why the computing speed of quantum computers is much faster than that of digital computers. 3), action at a distance of two entangled particles in quantum communications. No time is required to transfer messages between two entangled particles. This is contradicted with classical science, which may be treated as pseudoscience.

Keywords—quantum computers, quantum communications, quantum entanglement, action at a distance

1　前　言

在我们的周围，还在文革结束前，谈到一个物体的状态可以是1还可以是0，两个状态并存时，嗤之以鼻。谈到信息传送不要时间（超距）时谈虎色变。因为这是反动的，是伪科学。讽刺的是，在这个时期以前，我国的好多高校物理系和电子类专业已经开设了量子力学课程。

现在科学技术发展已经使量子计算机研制成功，使量子通信得以实现。量子计算机和量子通信虽然还没有商品化，还没有达到普遍应用程度，但是，再也不会有人怀疑这是唯心主义、是伪科学了。我们国家在量子计算机的研制上在某些方面在世界领先，还发射了墨子号量子卫星。

然而，人们长期在这样的思想和理念的束博下，已经固化了一些理念，在这种理念下要学习量子计算机和量子通信就非常困难，感到非常困惑、不可理喻。本文指出学习中的最难的一些难点。

2　学习的难点之一：是0又是1

在经典理念的人们的头脑中，一个物体只有一种状态。例如，一个晶体三极管，它的集电极的电压要么高（可以记作1），要么低（可以记作0），不能是1又是0（是高同时又是低）。

在电子数字计算机中，用高电位表示1、用低电位表示0（或者反过来用低电位表示1，高电位表示0）。这样一排晶体管可以唯一地记录一个多位数，例如8个晶体管可以记录这样的8位数：10101101，晶体管的电位为“高低高低高高低高”。注意，是记录这1个8位数。

而在量子计算机中，一个量子同时有1和0两种状态，用8个量子可以记录数10101101外，还可以记录其它的数，从0000000到11111111，8个量子可以同时记录2^8共256个8位数，是经典科学头脑的人不可理喻的。

这是量子计算机和数字电子计算机极大的差别之一 ：在电子数字计算机里要同时存储256个8位数，至少需要256*8=2048个晶体管，而量子计算机里只要8个量子！按此推理，再量子计算机中用16个量子能同时存储0000000000000000-1111111111111111中的任何数，而电子计算机同时存储这么多数需要晶体管2^{16}*16个=102.4万个!

这是量子计算机和电子数字计算机之间的一个极大的差别，顽固经典头脑者不可理喻，斥之为“伪科学”。

要攻破这个难点，首先要彻底转换观念。千百万年以来，人类凭自身的感官和发明的科学仪器认为任何物体只能有一个状态。例如水，H_2O,在0^0C以下时是固体，有形状、硬度、体积，在0^0C以上、100^0C以下时，有体积、没有形状、没有硬度、可以流动，是液体。在100^0C以上时没有体积、没有形状、没有硬度、可以流动，是气体。水有几种状态，可是在某一个时刻，它只有一种状态。这是人们颠簸不破的真理。可是，德布罗意说，当物体小到10^{-9}m以下时，是粒子又是波，一个物体（量子）同时具备2个状态——这个理论当时并没有实验支撑。

$$\lambda = \frac{h}{p} \tag{1}$$

量子的位置描述为：

$$\Psi\ (\boldsymbol{r},t) = Ae^{\frac{i}{\hbar}(\boldsymbol{p}\cdot\boldsymbol{r}-Et)} \tag{2}$$

该物体出现的位置的概率是：

$$\left|\Psi\ (\boldsymbol{r},t)\right|^2 \tag{3}$$

2年后薛定谔根据德布罗意的理论提出波动方程。

$$i\hbar\frac{\partial\Psi}{\partial t} = -\frac{\hbar^2}{2m}\nabla^2\Psi + U(r)\Psi \tag{4}$$

这是一个与人们用感官能接受到的经典观念完全不同的观念，学习量子计算机和量子通信只有接受和竖立这个观念，才真正理解量子计算机，这就是要彻底“洗脑”。否则，即使在技术上学会了怎么做量子计算机还是不懂量子计算机！这是突破量子计算机学习难点的一个极为重要的关键。

在电子数字计算机中用bit表示位，1个晶体管可以表示1个位，一个8位字长的加法器为8位——8bit。

对应地在量子计算机中用Qubit（qunten bit）表示一个量子位,量子位Qubit可以处于“0”和“1”的叠加态。

$$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle \tag{5}$$

例如用量子自旋方向来表示，如果用自旋轴向向下表示“0”，自旋轴向向上表示“1”，则量子位有百分之几十的可能向下或向上。一个 Qubit 同时表示为$|0>$和$|1>$，是“1”和“0”的叠加状态。也就是一个电子的 Qubit 同时有自旋向上（“1”）和自旋向下(“0”)两种状态，

他们出现的概率（自旋方向向上和向下的概率）分别为$|\alpha|^2$， $|\beta|^2$

$$|\alpha|^2 + |\beta|^2 = 1 \tag{6}$$

这在数字电子计算机中是不可能的，也是不可理解的—— 一个物体同时具有2个状态，是违背经典科学和相对论科学的最基本原理的。

8 Qbit的量子可以同时存储2^8个数——256个8位数！

这个理论在量子力学中讲解。国内量子力学课程的主流教材《量子力学教程》从上世纪的60年代用到现在，历经60多年！这本教材的“特点”是讲量子理论时重点讲量子理论的数学，不讲量子理论的根本，不与经典科学“冲突”。该教程的目录如下：

《量子力学教程》目录

在这本教程里量子理论中关键的、与经典科学不一致的、具有量子特性的量子双峰实验、纠缠、超距、薛定谔的猫等都不讲，所以，这本书与经典科学没有碰撞，不引起经典科学学者的质疑。可是，学生在学完这本《量子力学》后只会计算势阱等，还是不懂什么是量子，跟没有学差不多。本文作者在 1965 年学这门课程学校用的是这本教程，我本人听了课、做完作业，通过了考试，自以为懂得了量子理论。哪知道在 40 年后到国外读到量子计算机的原理的书时才知道根本就不懂什么是量子，对于量子计算机、量子通信的这些根本理论极为困惑！这才深深体会到这个问题的严重性。

3 学习的难点之二：并行计算

量子计算机的计算与电子数字计算机的计算有根

本的不同处。

例如在16位字长的电子数字计算机里，有16位（16bit）的加法器，1次运算2个16位数字一起加，例如1000100010110010+0000000000000011，计算（翻门）1次——得到 1000100010110101。

16位字长的数字有2^{16}个（64k个），他们只能逐个计算，他们的计算是串行，全部计算一遍最少需要64k次完成，而量子计算机中的计算是并行，相当于64k台电子数字计算机同时运行，这64k个数的计算一次完成！这是不可理喻的！

在数字电子计算机中，加法器是靠晶体管的翻门来计算的，需要时间，例如时间为1ns，则计算上面的时间需要：64kns。而量子计算机计算是量子的演化，尊从薛定谔波动方程，用Hamilton算符和Dirac算符表示为：

$$i\hbar\frac{\partial}{\partial t}|\psi(t)> = \hat{H}|\psi\ (t)> \qquad (7)$$

这个演化不需要时间！

现在的最好的加密方式是RSA，解密这样方式加密的文件（密文），用最快的数字电子计算机最少需要200多天，而现在用量子计算机几分钟就解出来了，使得现在无秘可言！

4 学习的难点之三：传送超距和不要能量

在经典理论里，任何两物体之间传送信息需要时间。相对论中也这样认为，而且定义传送速度不能超过30万公里/秒。

例如月亮与地球之间相距 384,401km，传送时间不少于： 384401 km/（30万km/秒）=1.28秒。而在量子通信中，居然从月球到地球不需要时间——超距传送！

微观世界的这一系列的问题曾经争论几十年，一方是爱因斯坦带领的一批科学家，它认为是里面有隐参数，于是爱因斯坦带领一批科学家找隐参数，几十年无果。后来，贝尔提出了一个不等式，如下：

$$|Pxz-Pzy|\leqslant 1+Pxy \qquad (8)$$

这个不等式说，如果有隐参数存在，以下的不等式一定成立。所以，可以用这个不等式来检测这个系统存在还是不存在有隐参数。然而到今天为止，所有的实验都支持在量子领域“贝尔不等式”不成立，也就是不存在隐参数。

我国量子卫星“墨子号”的测试结果表明隐参数不存在。

那么，这意味着什么？

在量子通信中，两个纠缠的量子一个放到月亮上，一个放到地球上，当月亮上量子的状态变化时，地球上的纠缠的量子同时变化。这里有几个问题：

问题一： 从月亮上变化的信息传到地球上，为什么不要时间？

一种假说可以是：两个纠缠的量子在宏观上看是分开在月亮和地球，实际上他们并没有分开，他们实际上还是挨在一起的——一个大双量子体，中间有物质连通，所以两纠缠的量子之间传送信息不要时间。

另一种假说可以是：对于纠缠的量子来讲，月亮和地球之间没有空间，他们一直挨在一起——改变空间的理念。

可是到现在为止，都拿不出证据。

问题二： 对于纠缠的量子，放在地球上的那个量子跟随月球上变化而出现的状态变化是谁给它的能量。

人为的力量（或其他外部力量）使得月亮上的量子的状态发生改变，可是，与其纠缠的地球上的量子为何自己会一起改变，是谁使它改变，这改变的能量从何而来？

这里是不是可以引出更大的问题：物体状态的变化是不是一定要能量？那能量是什么？

以上的问题到现在为止，科学上没有答案，哪怕争论的理论都没有。就像当年孔子无法回答“小儿辩日”那样：一个小儿说早上太阳比中午大，所以早上太阳离地近，另一个小儿说中午太阳比早上太阳热，所以中午太阳离地近。孔子无法回答，因为他还没有地球围着太阳转的知识。我们现在也像孔子那样无法回答以上超距和超速问题，我们缺乏相应的知识。

这是学习量子通信中的又一个难点。没有很好的办法突破，只有等待新的理论出现。

5 结束语

量子计算机和量子通信的理论是科学发展第2次断层的理论，比经典科学前进了2个阶梯。

经典科学是牛顿等一批科学家在16世纪到19世纪建立起来的科学，是伟大的科学。之后，爱因斯坦突破了这个科学的理论，建立了相对论。相对论不是建立在经典科学的研究方法——实验的归纳和推理上的，而是建立在“思想实验”上的。他的“思想实验”人类不可能做——不可能做30万公里长的列车、不可能开出30万公里/秒的速度，所以不可能用实验归纳法得出相对论。相对论里的理论在一些关键的理念上与经典科学格格不入，于是，长期以来在一些国度里称之

是伪科学。可是，爱因斯坦恰恰用这个“伪科学”发明了原子弹——实践了物质转化成能量的理论。到这个时候，那些顽固的经典科学观念们还是认为“物质转化成能量”是伪科学。他们也学习和制造原子弹，不过，他们只学习技术，不理睬其理论。

现在，我们学习量子计算机和量子通信又遇到了这样的问题：如果学习量子计算机和量子通信中我们头脑里固化的经典科学观念拒绝我们接受真正的量子理论，这就成了一个不可突破的难点。这要涉及到我们学习量子计算机、量子通信的目的和要求，希望学到什么程度。

如果只要学技术不要真懂，只管学习如何制造和如何使用量子计算机和量子通信设备就可以了，别人怎么做我就怎么做，跟着学！在学习量子计算机和量子通信中就不存在本文所述的难点，这些难点可以跳过去。

如果是希望能了解一点量子计算机的真谛和量子通信的真谛，本文是借鉴。

参 考 文 献

[1] 戴葵、宋辉、刘芸、谭明峰，量子技术引论，国防科技大学出版社，2001年3月

[2] Goulio Benenti,Giulio Casati,Giuliano Strini 著，王文阁，李保文译. 量子计算机与量子信息原理. 第一卷，科学出版社，2011年3月

[3] M. Reiher, N. Wiebe, K.M. Svore, D. Wecker, M. Troyer. ”Elucidating Reaction Mechanisms on Quantum Computers”. Proceedings of the National Academy of Sciences of the United States of America, July 2017

[4] K. Michielsen, M. Nocon, D. Willsch, F. Jin, T. Lippert, H.D. Raedt. ” Benchmarking gate-based quantum computers”. Computer Physics Communications 220(2017)44-45

[5] John Preskill D. Gottesman H. -K. Lo N. Lutkenhaus, Making Weirdness Work: Quantum Information and Computation . IEEE Aerospace and Electronic Systems Magazine (Volume: 21, Issue: 12, December 2006)

[6] Miroljub Dugić & Milan M. Ćirković , Quantum parallelism in quantum information processing, International Journal of Theoretical Physics volume 41, pages1641–1649 (2002)

[7] Bennett, Charles H, Quantum Information: Qubits and Quantum Error Correction, International Journal of Theoretical Physics . Feb2003, Vol. 42 Issue 2, p153-176. 24p.

.....