从量子计算机和量子通信设备的研制看技术发展断层

张凤祥

华中科技大学计算机学院，武汉，430000

摘　要　《相对论》是科学发展第 1 次断层出现的理论，《量子理论》是科学发展第 2 次断层出现的理论，由于他们与前面的理论不连续，并且许多理论相反，使得许多科学家和绝大多数人不信。之后，技术发展也随之发生断层，《相对论》科学催化出来的技术制造出原子弹，原子弹的爆炸威力使得人们不得不信相对论。量子理论催化出来的技术制造了量子计算机、量子通信装备。本文论述量子计算机的强大：计算速度比原有的电子数字计算机快千万倍、可以解密所有的加密密码，量子通信的通信速度远远超过现有的通信速度，而且可以真正的防泄密等。这些功能不得不使人们相信量子理论。所以，真正使得科学推广的是这些科学催生出来的技术。

关键字　科学发展断层，技术发展断层，量子计算机，量子通信

Technology Development Faults from the Perspectives of Device Design in Quantum Computers and Quantum Communication

Fengxiang Zhang

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

Abstract—The Theory of Relativity appears after the first science development fault, and quantum theory the second. Due to the discontinuity of the science development and a great many of theories, to which they are contradictory, most scientists and the great majority of people do not accept them. Later on, technology advances also in a discontinuous manner. The success of the atomic bomb developed based on the Theory of Relativity convince people to believe it. Quantum computers and quantum communication equipment provide strong evidence to the quantum theory. Quantum computers are powerful, with the computing speed millions of times faster than digital computers and the ability to decode all encrypted code. The communication speed based on quantum theory far exceeds the existing communication speed, etc. Therefore, the driver that pushes science to advance is the technology.

Key words—science development fault, technology development fault, quantum computers, quantum communication

1　引　言

人类进入 20 世纪后科学发展出现断层，也就是新出来的科学不是已有科学的延伸和发展，如果将科学发展用曲线来描述，新老科学头尾不相接。本文以相对论为例，论述科学断层式发展出新科学时，由于它与前面的科学理念好多是相反的，绝大多数人不信。只有用该新科学催生出新技术，用这些新技术做成装置，而这个装置起很大作用时，人们才会相信。在人类多少万年形成的理念里认为科学发展一定连续——新科学的开头一定是老科学的结尾. 见图 1。

然而，在 1905 年起科学发展出现断层，见图 2。

新科学的开头不少老科学的结尾。这是因为 1905 年爱因斯坦提出了《相对论》，在相对论中有不少科学理论、科学理念与经典科学相违背，推翻了老科学的一些定律。

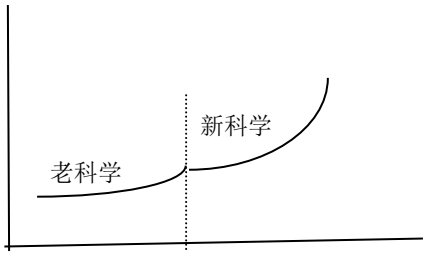

图 1　经典科学理念中的科学发展曲线——连续

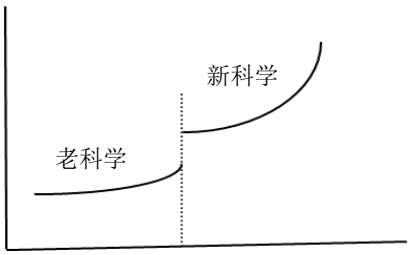

图 2　科学发展断层的科技术发展曲线——断层

例如，在当时的经典科学里，物质和能量是不同的两种东西，风马牛不相及。物质有自己的守恒定律——物质守恒定律，能量有自己的定律——能量守恒定律。这两个定律相互独立。然而，1905 年爱因斯坦提出《相对论》，在相对论中认为物质可以变成能量、能量可以变成物质，按以下公式：

$$E = MC^2 \qquad (1)$$

按这个理论，一个几克重的烟头，乘以 C^2：

C^2=900000000000000000000000（厘米/秒）^{2}，将变成多么巨大的能量，一旦爆炸起来可以在地球上炸出一个大窟窿！

更为不可接受的是，能量还可以变为物质——在那空空无物的地方，可以 无中生有“来”就可以出现一个有物质的东西!当时几乎没有人可以相信，所以，认为这是“伪科学”。

可是在这个理论提出 40 年后（1946 年），爱因斯坦根据这个理论研制出原子弹。这是用中子撞击 1 个 U^{235} 原子,将 U^{235} 原子核撞破变成 2 个其他的原子的核，并打出 2 个中子（为 0-6 个中子，平均 2.5 个，简化讲解时称为 2 个），反应前后少了大约 2 原子量的物质，该物质转化成能量发出来（称为“核能”）。打出来的 2 个中子再撞击其它 U^{235} 原子，又将 2 个 U^{235} 原子撞破，原子核 2 个分裂成 4 个（2^2），放出 4 个中子。同时又将 2 份核物质转换成能量。再下一代，4 份核能，……，这样一代一代下去，呈现链式反应。这种反应按几何级数增长（2、4、8、16、32、64、128、……），例如，瞬间 1000 代就放出 2^{1000} 份核能（巨大的能量）！这种链式反应形成的大爆炸可以炸毁一座城市！这时科学发展出现断层——这个科学与原科学毫不相干，在科学发展曲线上断裂。这个断层发展的科学在 40 年后（1946 年）催化出出相应的技术——研制出原子弹，结束了第 2 次世界大战！

这种从科学发展断层中研究出来的理论催化出新的技术，也就是技术发展断层，是完全不同与以前的技术。在这以前的所有爆炸技术都是用化学反应：“火药+高温点火”发生爆炸，是化学能！而原子弹与早先的炸弹的技术完全不同，它不是用化学反应，它不需要高温点火。它需要维持链式反应，要体积足够大——链式反应要求大于临界体积。平时将 U^{235} 制成制成小于“临界体积”的 U^{235} 半球分开存放，要爆炸时将这 2 块 U^{235} 半球面对面快速压在一起，使其体积超过临界体积自动出现链式反应。平时它放在那里非常安全，绝不会自行爆炸！

它不需要点火、不需要起爆，只要他的体积超过临界体积它自己会点火、自己起爆。这与原有的爆炸技术完全不同，爆炸技术发展出现断层，按原先的爆炸技术，不可能研制出原子弹。

2 技术发展的第 2 次断层

这是第 2 次科学断层发展催化来的技术断层发展。

1924 年德布罗意提出粒子又是波，

$$\lambda = \frac{h}{p} \qquad (2)$$

$$E = h\nu \qquad (3)$$

1926 年薛定谔根据德布罗意的理论继续写出粒子的波动方程，

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

于是出现量子理论（量子力学）。量子理论并没有使科学发展断层，因为可以认为是“隐参数”在起作用。“隐参数”可以解释量子现象。

而波尔认为不存在隐参数，而是概率现象——一种与原来科学完全不同的理论。如果他成立，那就是科学发展断层！

从爱因斯坦寻找隐参数之日起，已经百年了。找不到隐参数。1964年贝尔提出了一个不等式（贝尔不等式），说：如果有隐参数存在，以下的不等式一定成立，

$$|Pxz-Pzy| \leqslant 1+Pxy \qquad (5)$$

然而所有量子理论的实验都表明这个不等式不成立，包括我国发射的量子卫星中的实验也表明不等式不成立，也就是说隐参数不存在！

这个问题就大了。波尔的概率说解释完全颠覆了原来的理论，在科学发展上大大跳了一步，呈现科学发展的断层。称为科学发展的第 2 次断层，而这次科学断层发展的科学催化出断层式发展的技术。本文论述这些技术。

3 技术发展断层之 1——1 个存储单元 Qbit 同时存储 1 和 0

这在以往的计算机里是不可能的。例如，在早先的磁性单元（小磁环），在一个磁环只能存储一个状态——1 或 0，不能同时为 1 又为 0。后来的晶体管存储器里，晶体管电位高为 1、低为 0，不能同时电位既高（1）又低（0）。

在量子计算机里，存储单元，例如量子自旋状态，正转记 1，反转记 0，量子可以正转（1）同时又反转（0），经典科学头脑者无法理喻！可是，已经做成了这样的量子计算机，不信也得信！

$$|0>\equiv\begin{bmatrix}1\\0\end{bmatrix}\qquad |1>\equiv\begin{bmatrix}0\\1\end{bmatrix}\qquad (6)$$

在现代电子计算机里，32 个存储器可以存储 1 个数——2^{32}个数中的某一个数。例如： 1111…10…000（32 位二进制数），不能同时又表示为 1111…10…001（32 位二进制数）。而在量子计算机里，32 位量子单元可以存储 2^{32}个数，既表示 1111…10…000（32 位二进制数），又表示 1111…10…001（32 位二进制数）。

计算机的这个技术是科学发展断层发展出的量子理论催化出来的技术，是计算技术发展断层。

4 技术发展断层之 2——量子计算机能执行真正的并行运算，破解密码，使得世界上无秘可保

在数字电子计算机中，一个位bit只能有一个数值，要么1，要么0，绝不可以同时表示1又表示0。

在量子计算机中，一个位Qubit可以同时为1和0，处于“0”和“1”的叠加态。

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle\qquad (7)$$

只是他们出现的概率不同。他们的概率分别为$|\alpha|^2$， $|\beta|^2$

$$|\alpha|^2+|\beta|^2=1\qquad (8)$$

在数字电子计算机里，无论多复杂的运算，在运算中间任何时刻和最终运算结果都只是一个唯一的、确定的数字，所以，数字电子计算机运算是串行。

而量子计算机运算，每个Qbit单元都不是唯一的数，中间和结果都不是唯一的数字。用Hamilton算符和Dirac算符表示为：

$$i\hbar\frac{\partial}{\partial t}|\psi(t)>=\hat{H}|\psi(t)>\qquad (9)$$

这表明数字电子计算机里面的“计算”是并行。

为此，Shor（彼得·秀尔）于1994年提出来量子质因子分解算法，颠翻了经典科学，出现技术发展断层——这个技术与原先的技术不衔接。

世界上加密最强的技术是用RSA（非对称加密算法）对其加密，要破译密码，随着数字电子计算机的技术的发展逐渐进步：从电子管计算机、晶体管计算机，到集成电路、超大规模集成电路计算机，到现代最大的数字电子计算机，对RSA密码的解密能力一点点提高，解密速度一点点缩短，解密的能力是连续发展的。到当代最强大的数字电子计算机对RSA加密的密码解密还需要几百年。

可是，量子计算机对RSA密码的解密能力一个跳跃：一下子提高到仅仅需要几分钟，使任何加密失去意义。他们用的不是串行技术，而是并行技术，解密技术发生断层！

这个技术断层的结果使得无秘可言，对于军方和商业极大打击！所以，研制量子计算机最早和最大投入之一的是“国际商业机器公司”（IBM），装备量子计算机积极的是军方。

5 技术发展断层之 3——量子计算机计算几乎不要时间

电子计算机的计算靠晶体管翻门，晶体管翻门需要时间，所以，数字电子计算机的计算速度受到晶体管翻门时间的限制。1 个复杂的计算要经过几千上百万晶体管翻门，时间就短不了。然而，在量子计算机里，是量子的演化，量子演化基本上不要时间，所以，量子计算机计算速度远远超过数字电子计算机，约复杂的计算，超得越厉害。

2019 年，谷歌(Google)研究人员展示其最新 54 比特量子计算机，该计算机只用 200 秒便可计算完毕当前世界最大的超级计算机需 1 万年进行的运算。

这是科学发展断层中催化出来的技术发展断层！

6 技术发展断层之 4——量子密钥

量子计算机用量子密钥分发使通讯双方可以生成一串绝对保密的量子密钥，用该密钥给任何二进制信息加密，都会使加密后的二进制信息无法被解密，因此从根本上保证了传输信息过程的安全性。这是一个通信技术上的极大的飞跃。再加上量子的不可克隆性，偷听者无法复制光子。他要偷听只能在接收者收到以前盗听，必然会导致密文变化。接收方再接受的密码里有“测量基”，如果被偷听，接收方就立即发现“测量基”变了，也就是有人偷听了，立即中止传送，已传密文作废。

7 技术发展断层有待突破之 1——量子远程通信超光速

以上的技术使得信息传输可靠！这些技术也是在科学发展断层的量子理论中催化出来的技术，是原来通信技术的断层使发展。但是，有些科学断层的技术催化还有困难。例如，自从1887年莫雷实验证实光速不变后，几百年来一直认为，任何物体移动都不能超过光速，也就是两地传输需要时间，这个时间最少不得少于两地之间的路程除以光速。爱因斯坦就是依据光速不变提出相对论。这是科学界不可动摇的“铁律”。

可是，科学发展出现的量子理论中的量子纠缠却说，两个纠缠的粒子分放在很远的两地，一个状态改变，另一个也会更着改变，而且不要时间，也就是可以超距传送信息。这是动摇速度不能超过30万公里/秒的铁律的。

可是，到现在为止，在量子通信技术里还没有完全实现，原因是纠缠态不能干扰，一读就变了，还得想办法用经典传送来弥补，这样一来，总的传送速度就超不过光速。用隐形传送，只传送信息，不传送量子，是一个突破的方向。

8 技术发展断层有待突破之 2——找大体积量子

现在制造的量子计算机也好、量子通信设备也好，所用的量子极小，例如中国的量子计算机“九章”就是用光子。一个一个的光子去控制，光子这么小，想想都很难。找大一点的量子作为技术上的需要，在量子计算机和量子通信里极为重要。上百年来，一直没有找到。

本作者提出，从薛定谔的猫能不能启发找大量子。薛定谔的猫实际上就是一个标标准准的宏观猫，不具有量子性质，可是按薛定谔那么一解释，他被关在笼子里，成了概率猫，能不能从这里得到启发研制出大量子？

9 怪现象和努力方向

量子理论提出后出现了一个不可思议的怪现象——自己否定自己。量子理论是德布罗意、薛定谔在爱因斯坦大力扶助下提出的，他们 3 人是量子理论的创立人。可是，量子理论能解释得通得只有概率说，否则不成立！而这几位创立者恰恰否认概率说，还在专门召开的世界最高级会议上面对面论战！这真是“怪现象”!

爱因斯坦是世界上地位最高的科学家，量子理论的创立者德布罗意、薛定谔，他们扎在一把反对波尔等的量子理论概率说，又拿不出隐参数说的依据，被反对的波尔这样的科学家该有多么困难核难受！

本作者以为，爱因斯坦的力量败下阵来的根本原因是他们找不到隐参数还要坚持。而波尔等已经在这样的压力下用概率说催化出相关技术，做出了量子计算机和量子通信设备。量子理论概率说的科学家们应当被赞扬！

但是，量子理论的技术发展还远远没有达到实用阶段——量子计算机还不能称为计算机，只能称为“量子处理器”，因为它只能解决特定的问题，还不是“通用”。而量子通信则还处于实验阶段。

10 结束语

本作者认为，“相对论”从提出到技术上研制成产品仅仅 40 年（1905 年提出，1946 年制造出原子弹）。“量子理论”从提出（1924 年左右）到现在近百年，还拿不出可用的产品（通用量子计算机和可实用的量子通信设备），这个研制速度不正常，显然还存在有量子理论以外的问题！这也是科学工作者要努力的。这一问题不能忽视！

本文论证了一个真理：一个完全新的科学要得到人类的承认，不是靠科学家的论证——这些论证是基础，但是人们不信。而是靠将其催化出相应的技术，再用这个技术做出相应的设备。如果没有原子弹，到现在可能还没有几个人相信物质变能量！

相对论后科学发展再次断层出现了量子理论。量子理论更离谱，更加使人们不信，可是它所催化出来的技术研制的量子计算机、量子通信设备不得不信。所以，推动量子科学发展的极大动力在于他催化出来的技术，这个技术于原来的技术完全不同，他不是与原来的技术的连续，而是技术发展的断层！

参 考 文 献

[1] National Academies of Sciences, Engineering, and Medicine, Quantum Computing: Progress and Prospects(2019). Washington, DC: National Academies Press

[2] Jiajun Chen. 2021 Journal of Physics: Conference Series 1865 022008

[3] Baldeep Singh Dhillon1 and Manisha J Nene. Future of Quantum Communication A Study. 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT)

[4] Zhen Sun, Liyuan Song, Qin Huang, Liuguo Yin, G. L Long, J. Lu and L. Hanjo, ”Towards practical quantum secure direct communication: A Quantum memory free protocol and code design” IEEE transaction on communications (2020)

[5] M. Gupta and M.J. Nene ”Quantum computing: A measurement and analysis review” Research Article published in Wiley Journal ’Concurrency and computation : Practice and Experience’ Online ISSN: 1532- 0634 Apr 2021

[6] M. Gupta and M. J. Nene, ”Quantum Computing: An Entanglement Measurement,” 2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI), 2020, pp. 1-6, doi: 10.1109/ICATMRI51801.2020.9398441.

[7] Alamira Jouman Hajjar : ”Quantum Entanglement: What and Why it is important in 2021” AI multiple research https://research.aimultiple.com/quantum-computing-entanglement/