

不懂量子也不懂计算机， 那么，你能理解量子计算机吗？

（来源：科技日报微信公众号，2018-10-09）

你无数次听过量子计算机的大名，但就像所有带“量子”两字的概念，你大概率（100%）不甚了然。

量子计算机的概念 1980 年代提出，投入研发 20 年，迄今还没有一台真正走出实验室。但传说它（将来会）很厉害。谷歌、IBM、阿里巴巴和许多初创公司在竞争，想第一个实现“量子霸权”，也就是让量子计算机在一个计算任务中快过传统计算机。

为了在芸芸众生中彰显你的卓尔不凡，不妨粗浅了解一点量子计算机的原理。其实它和我们熟知的电脑差不了多少。

量子计算机：量子版的计算机

“别把量子计算机想成全新的系统，它就是经典计算机的扩展版，处处模仿经典计算机。”安徽问天量子科技股份有限公司首席科学家、中国科学技术大学中科院量子信息重点实验室韩正甫教授告诉科技日报记者。

韩正甫说，经典计算机以电压高低代表数字 1 或 0，即为一比特（bit）。

而量子计算机里对应的是量子比特（Q-bit），那可能是自旋箭头向上或向下的一个电子，也可能是“立直振动”或“躺平振动”的光

波……等等。

传统计算电路由各种“逻辑门”组成，对应的就是量子计算机的各种“量子逻辑门”。都是根据一定的规则，变化存储位的 0 和 1。

韩正甫说：“传统计算机是这么玩的：一排存储位写进去一个初值（比如 10011001）。接下来若干步操作，每一步存储器里边的数都变换成另外一组数。走完程序停下来，把里面的数读出来，比如 00101010，就是计算结果。”量子计算机同样如此。

量子计算机不同之处，是丘比特（Q-bit）特别灵活，没 bit 那么死板。它同时是 0 和 1。比如：它是六成的 0 和四成的 1。这让它有了超能力。学过一点量子力学才能理解 Q-bit 的奥妙。

模糊又精确的 Q-bit

什么叫“它是六成的 0 和四成的 1”呢？

补习一下高中物理：20 世纪初的实验发现，物质细小到极限，就无法被准确测量。因为测量意味着干涉，哪怕你只看一眼。

当对象微小到了量子级别，它的状态会被观测彻底破坏。（顺便一说，“一触即溃”的效应被用于量子通信。用量子来承载密码，可以做到有人窃听这个密码信号，一定会被发觉。）这就叫“测不准原理”。东西越小，就越显得模糊。你去测量一个电子的位置，这次测出来在北京，下次测出来在天津。我们只能说一个量子“大概率在北京”，“大概率自旋箭头冲上”，“大概率平躺着振动”……

这些概率，是可以多次测量确定的，虽然单次测量的读数不一定。

所以量子比特是模糊的也是精确的：同一个数时而读出 0，时而

读出 1；但多次去读，出现 0 的概率会趋于一个定值，比如说 60%。

为什么量子计算更快？

“在传统计算机里，一个高电压叠加另一个高电压，仍然是一个高电压；量子比特的叠加则不同。”韩正甫说。

量子比特存储的是一个矢量，就好像一个时钟，时针对应着概率。

时针可以指向零点（量子比特读数 100%是 0），或指向三点（读数 100%是 1）。或指向一点半（50%是 0，50%是 1），或指向任意一个角度。

传统计算机存储的是“10011001”。

量子计算机存储的是“钟钟钟钟钟钟钟钟”。（请自行想象酒店大堂挂的一排）

传统计算中，1 和 0 叠加为 1，再叠加一个 1，得到 0。

量子计算中，“三点”和“零点”叠加为“一点半”，再叠加“三点”，得到的是“两点一刻”。

比起 bit，Q-bit 更有表现力。一个 Q-bit 可蕴含无限复杂的数字。在这个意义上“以一抵多”。一个 Q-bit 投入变换，等于多位数字一起变换，即所谓“并行计算”。

并行计算潜力发挥到极限的情况下，量子计算机的算力比起传统计算机，是 2^n ：1。

但要强调的是：量子计算机的结果来自概率统计。量子计算机与传统不同，它要一次次重复程序，一次次地读数（每次结果都不一样）。周而复始，足够多次（让概率的可信度超过 99.99999%）后，

统计出各量子位为 1 和 0 的比例，那才是需要的数字。所以碰上不太复杂的计算任务，量子计算可能比经典计算机更慢。

彩虹与斑马

有量子计算机之前，数学家就在畅想利用量子比特的“丰富内涵”大大缩减计算时间。不过迄今数学家只证明在两种场景中，量子计算大大快于传统计算机。

首先是破解 RSA 算法。RSA 是现在最常用的加密方法，其机理是利用因数分解的困难——把两个大质数相乘很简单，而把乘积拆成两个质数，计算机可能得算几万年。

所以银行可以公开发送一个几千位的数字，并掌握它的两个质因数，而不担心有人算出这两个质因数——用于制造私有的数字钥匙。

但二十多年前 Peter Shor 证明一种基于量子计算机的算法，可以轻松分解因数，这也让学界研发量子计算机的兴趣大增。

另一种可能的应用是“搜寻未排序的大数据库”，或者叫“大海捞针”。传统计算机只能一个一个比对目标，而量子计算机则可以并行计算。传统计算机用时是 T 的话，量子计算机用时是“根号 T ”。前者要花费 1 百万小时的任务，后者一千小时就能解决。

除了以上两类计算，量子计算机还被寄希望于未来在化学、制药等领域大发神威。理由是：不同于传统计算机，量子计算机是真正的模拟计算机，可以重现真实的自然（物理学家费曼第一个指出这点）。

传统比特的 0 和 1 相当于黑白两色，量子比特的“可以指向任何角度的时针”就相当于全彩色谱，可显示出任何一种颜色。

如果说传统的存储器是斑马，量子存储器里就是彩虹。世界是多彩的，用彩虹去描绘世界，当然更直接，更便捷。

才刚起步

量子很脆弱，动不动就会崩溃。

“要将信息编码在一个非常微小的东西上去，比如一个电子，或一个原子核，都首先要把它孤立开来，让它跟周边不作用。这种细微的控制是很难的。”韩正甫说。

各种量子载体都伴随着独特的困难，比如光子时刻前进，电磁场又左右不了它，操控起来很麻烦。目前研究者在大概在实验几十种载体：电子、光子、陷阱里的离子……

韩正甫说：“隶属中科大的中科院量子信息重点实验室，现在正副教授就有 50 多人，在读的博士生有 170 人，博士后 30 多人，一个团队里有很多不同的组，研究的事情虽然互相可以理解，但术业有专攻，比如‘做硅’的就会去研究曝光、清洗等等半导体行业关心的工艺；‘做光’的研究激光发生器、振荡器、光纤之类。”

“国内从 1980 年代初开始量子光学研究。现在多了不少人，但还是个冷门。专业人才稀缺。”韩正甫说，“其实全世界人才都不够。所以谷歌花了几亿美金从加州大学圣芭芭拉分校挖了一个团队过来，主要研究超导量子计算机。”

目前各大公司和研究机构仍在提升量子比特量——争取几十个量子同时稳定，别太快塌陷。超导机器为了让环境接近绝对零度，成本高达成百上千万美元。工程实验机在进步，但几时走到实用还不知

道。

回顾 1946 年第一台计算机 ENIAC，用了 18000 个电子管，那是一种抽成真空电子飞行其中的玻璃管。ENIAC 重 30 吨，每秒钟仅计算 5000 次。没有十多年后的半导体革命，就谈不上今天的电脑和手机。

应该说，量子计算机刚进入它的“真空管时代”。（科技日报记者高博）

原 文 链 接 :

<https://mp.weixin.qq.com/s/Chu0brfXkGzhaA7ha6hT3Q> ，转载请注明。