**初识量子计算机**

出于好奇，之前也在网试图上了解过量子计算机，但是由于当时从未接触过计算机领域，遂不了了之。近日听闻老师提起量子计算机，便又心生念头，打算多下点功夫，解开量子计算机神秘的面纱。当然，我自知仅仅以我现在的水平无法理解那么高深的知识，但也借此机会在心中埋藏探索的种子，日后多多了解，培养自己的兴趣，或许真的就会慢慢涉足这个领域。写此篇也算是对量子计算机的初认识和理解。

首先是Wikipedia对量子计算的描述：“Quantum computing is a type of [computation](https://en.wikipedia.org/wiki/Computation) whose operations can harness the phenomena of [quantum mechanics](https://en.wikipedia.org/wiki/Quantum_mechanics), such as [superposition](https://en.wikipedia.org/wiki/Quantum_superposition), [interference](https://en.wikipedia.org/wiki/Wave_interference#Quantum_interference), and [entanglement](https://en.wikipedia.org/wiki/Quantum_entanglement). Devices that perform quantum computations are known as quantum computers. Though current quantum computers are too small to outperform usual (classical) computers for practical applications, larger realizations are believed to be capable of solving certain [computational problems](https://en.wikipedia.org/wiki/Computational_problem), such as [integer factorization](https://en.wikipedia.org/wiki/Integer_factorization) (which underlies [RSA encryption](https://en.wikipedia.org/wiki/RSA_encryption)), substantially faster than classical computers. The study of quantum computing is a subfield of [quantum information science](https://en.wikipedia.org/wiki/Quantum_information_science).”不难看出，量子计算会利用量子力学现象，如叠加、干涉和纠缠。而执行量子计算的设备就叫量子计算机，在解决某些计算问题，比如整数分解(RSA 加密的基础)时 ，比经典计算机要快得多。也正因如此，量子计算已经成为了世界各国未来科技发展的必争之地。不管是国外的英特尔、谷歌，还是国内的百度，都在进行量子计算机的研发。那么这个量子计算机到底厉害在哪里，为何让各国都投入大把的资金去研发跟进？他又有什么好处呢？

首先，我们要知道，量子计算机的速度非常之快。可是只一个快字却并无法给人以直观的感觉。那么把它和传统的计算机相比一下，2021年，我国中科大潘建伟院士团队研发了光量子计算机“九章二号”和超导量子计算机“祖冲之二号”，前者在处理特定问题的速度比超级计算机要快上亿亿亿倍，而后者在量子随机线路采样问题上的计算速度，也比目前最快的超级计算机快一千万倍，更别提我们日常使用的计算机了。如果还没有什么概念，那不妨看一下具体的例子。对于将一个数进行质因式分解这样一个问题，我们人类可以很容易地将15分解成3\*5，而传统计算机也可以很容易地将63分成3\*3\*7，但是当这样一个数达到了三百位呢？再将它进行质因式分解，估计人类靠手算是不可能算出来了，而传统计算机也要算上15万年，但是对于量子计算机却只需要一秒钟就可以计算出来。这样的对比，确实给人带来了强烈地冲击，我瞬间对其崇拜起来，它倒像是现实意义上地钢铁侠这样的超级英雄，又或是更加强大。

这也驱使着我去进一步了解它如此之快地原因是什么。原来量子计算机并不像传统计算机那样使用晶体管去存储数据。传统计算机的工作模式是其最小的组成单位晶体管负责用开和关表示1或0进而用二进制来表示各种数据，cpu则负责对这样一些用0或1组成的数进行运算。每一个晶体管在同一个时刻只有一个值，因为晶体管的状态要么是开要么是关，所以只能表示0或者是1，也就是说做一次计算只能得到一个固定的结果，所以如果要进行大量计算的时候只有两种办法，一个就是加快每次计算的速度，比如说我们可以提高CPU的计算频率，另外一个就是多个计算同时进行，比如说采用更多的CPU内核或者是买更多的计算机并行运行，或是更多的晶体管共同嵌在cpu那样一个小方块上，就像苹果M2芯片，采用了第二代5纳米制造工艺，并在芯片上配备了200亿个晶体管。但是既然希望搭载更多的晶体管，那么纳米工艺就要更加精益，但终有一天会达到极限，那么这种传统的计算机运作模式便也出现了性能上限。

但是，量子计算机的运作模式与传统计算机却不一样，量子计算机并没有晶体管，其最小单位亦不是晶体管所决定的比特了，取而代之的是量子比特（qubit），他有0和1，以及介于0和1之间的任意的状态，这种有趣的特性又叫做量子叠加（superposition），

这里就不得不说说薛定谔那既死又活的猫了。薛定谔的猫是一个非常著名的思想实验。假定一只猫被关在一个密闭盒子里面，盒子里有一装有剧毒的玻璃瓶，瓶子上方有一个装有放射性原子的盒子，放射性原子有一定概率发生衰变。盒里还有一个机关侦测放射性原子是否发生衰变。若发生了衰变，机关将控制一个锤子砸碎玻璃瓶，释放出毒气，从而使猫死亡。

　　但有一个问题出现了：假定关猫的盒子不透明且隔音，倘若我们不打开盒子便无法知道猫的死活。如果问猫是死是活，怎么回答？不打开盒子的话只能推断猫可能是死的，也可能是活的。

量子比特存在相似的情况。量子比特可以同时具有两个或两个以上的多重状态（叠加态），这种现象就是量子叠加。

当多个量子比特放在一起的时候，还有一个非常重要的特性叫做量子纠缠，用非常简单的话说就是多个量子比特会相互作用纠缠在一起，从而形成一个整体。那么量子叠加和量子纠缠这两个特性是量子计算的关键，借助这个特性，量子计算机就能做出很多有意思的事情，可以一次性完成多个计算，从而极大提升计算的速度。举个例子，传统计算机两个比特可以表示四个数，但对于某一刻，其只能拥有一个值，而量子计算机则可同时表示这四个数。随着量子比特的增加，其可以表示的数也呈指数级增加，n个量子比特就可以同时表示2^n个值，即可以在同一时刻进行2^n次运算。对于这么多次的运算，并不都是我们所需要的，这个时候就要进行人为的干预，即通过设计专门的量子电路，通过改变量子叠加的状态对结果进行筛选，进而得到想要的结果。

那么，制造一台量子计算机难在什么地方呢？其实，量子计算机对量子芯片的要求并不像传统计算机的芯片那样苛刻，而是对芯片周围的运行环境有着极高的要求，要精确地控制量子芯片周围的温度、电磁波、噪音、振动等。量子芯片周围要有一层外壳包围，在里面制造零下273.14摄氏度的低温。其次，芯片的用料也要更加讲究，比如要使用更高纯度的硅。第三，对于量子计算机所用的软件也需要重新设计开发，也需要进行编程，这样就更需要一批学识渊博的人才进行开发研究。

量子计算机这么厉害，是否会取代传统的计算机呢？至少目前还不可替代，尽管它可以非常快地解决数学问题，但是却并不能供你打游戏刷视频，再加上其昂贵的造价，使得其无法取代传统计算机。他们更多的是相互补充，在各自的领域大放异彩。

很多人都认为量子计算机会继互联网和个人计算机的兴起、移动互联网和智能手机的兴起、万物互联和智能设备的兴起之后，引领下一波技术变革的浪潮，也让我们怀揣着对未来技术地美好憧憬，坚定地选择自己所走的路，朝着一个方向精益求精，相信有朝一日，我们也可以在某个领域贡献出自己的力量！