关于量子计算的认识

江欣余

(北京大学地球与空间科学学院 2015 级本科 1500012415)

【摘要】由于传统计算机的计算能力面临物理极限，人们在寻找下一代的技术。量子计算作为新兴的计算方式，以其高效率，低能耗的优点提供了一个绝佳的解决方案。本文从量子计算的原理出发，结合量子力学，介绍了一些算法，分析了这一极具潜力的技术的特点、优势、发展障碍与应用前景。

【关键词】量子计算，量子力学，算法，计算机

1 传统计算机的危机

传统的电子计算机诞生至今，经历了电子管、晶体管、中小规模集成电路和大规模集成电路四个时代。计算机科学的发展依然难以追赶人类日益增长的信息处理需求。尽管根据摩尔定律，传统硅芯片的性能可以做到周期性的翻倍，但工艺达到一定极限后，芯片内部微观粒子性越来越弱，相反其波动性逐渐显著，传统宏观物理学定律因此不再适用，传统的结构已无法满足稳定的计算的要求。另外，集成度的提高也带来耗能与散热的问题，制约着芯片集成度的规模。芯片耗能源于计算中的不可逆过程。处理器对输入两串数据的异或操作而最终结果却只有一列数据的输出，过程不可逆，能量守恒定律决定了消失的数据信号必然会产生热量。而摩尔定律本身的魔力也渐渐消失，硅芯片的集成度提高已到了一个瓶颈阶段。当芯片工艺进入更加极端的微观世界，量子力学的规律开始发生作用，同时量子计算在计算、编码、信息处理和传输过程等方面提供了的全新的方式，大幅度地降低了能耗，提高了计算能力。量子计算的突出优点使人们将其看作是下一代计算机的大势所趋。

2 量子计算的基本原理

2.1 量子理论的重要特性

拉夫勒姆说：“量子力学告诉我们，量子（计算）位或量子硬币同时既是头又是尾。这的确改变了世界的运作方式。”

自上世纪 70 年代始，以理论物理学家费曼为首的一些科学家开始对量子计算产生兴趣。量子计算的理论基础是量子力学。“薛定谔的猫”是人们在谈论量子力学的重要特性“叠加态”时最常引用的一个思想实验。观察者打开盒子之前，猫处于一种“既死又活”的状态，一旦观察者打开盒子观察，猫呈现的只会是“活”或“死”的某一状态。换言之，当一个量子系统处于叠加态时，如果不对它进行观测，它会一直处于既是此又是彼的状态。一旦对它进行观测，它则立刻呈现为非此即彼。量子叠加态的存在，才使量子计算和量子通讯成为可能。

量子计算机的另一个基本原理是量子缠结态。以电子为例，它本身具有两个自旋态：向上或向下，如果不进行观测，它可以处于不上不下的叠加态。可以通过某种物理手段将两个电子耦合在一起，耦合之后的特性是，两个电子的自旋方向保持一致。这两个电子形成的耦合态，就是量子缠结态。由于每个电子的自旋在未被观测的情况下是处于叠加态，所以它们组合而成的体系也处于叠加态。两个电子一旦量子缠结在一起，在不破坏它们状态（即不对其中任何一个进行观测）的前提下，即使将它们分隔很远，其量子缠结态也会继续保持

不变。这就相当于将信息瞬间从一处传递到了另一处。量子通讯就是基于这种原理。

2.2 量子计算的原理

传统电子计算机采用比特作为信息存储单位。比特是两态系统，即“1”或者“0”。然后通过逻辑电路实现四则和逻辑运算。量子计算的信息存储单位是量子比特，其两态的表示常用以下两种方式：

⑴ 利用电子自旋方向。如向左自转状态代表“1”，向右自转状态代表“0”。电子的自转方向可通过电磁波照射加以控制。

⑵ 利用原子的不同能级。原子有基态和激发态两种能级，规定原子基态时为“0”，激发态时为“1”。量子计算在处理 0～n 个数相加时，采用的是并行处理方式将“00”、“01”、“10”、“11”等 n 个数据同时输入处理器，并在最后做一次运算得出结果。无论有多少数据，量子计算都是同时输入，运算一次，从而避免了传统计算机输入一次运算一次的耗时过程。当对海量数据进行处理时，这种并行处理方式的速率足以让传统计算机望尘莫及。量子计算能实现并行运算的根本原因便是其“叠加态”的性质。量子比特不仅可以取“0”或“1”，还可同时取“0”和“1”，即其叠加态。以此类推，n 位传统比特仅能代表 2n 中的某一态，而 n 位量子比特却能同时表示 2n 个叠加态。

量子计算除可并行运算外，还能快速高效地并行运算，这就用到了量子的量子相干性。量子相干性还可应用于存储当中。

3 几个重要的量子算法

3.1 量子幺正操作和量子逻辑门

在量子力学中，满足某种特定关系的一种被称为幺正算符,幺正算符对应的变化通常被称为幺正变换或幺正操作。演化算符的幺正性使得量子信息过程有如下一些特殊的性质:(1)保几率性，即量子态的归一化性质不随时间的改变而改变，量子系统的总几率保持不变；(2)可逆性，即量子信息处理中的所有逻辑操作都是可逆的。在量子信息处理过程中,系统的幺正演化通过量子逻辑门来完成，根据作用的量子位数目，量子逻辑门被分为单量子比特门、二量子比特门和多量子比特门。

3.2 量子并行性与量子算法

量子并行计算贯穿于量子算法之中，使得量子算法与经典算法相比，以更高的效率得到所期望的计算结果。量子算法目前可以归为以下几个种类:

(1)模拟量子力学体系性质的量子仿真。从理论上说，量子计算机对此类问题具有指数化的加速；

(2)基于葛洛沃量子搜索算法的量子振幅放大类算法。量子振幅放大算法即放大所需要的输出值的振幅。它的基本思想是对量子态进行幺正变换,从而放大所需要的输出值,使得在测量的时候可以很大的概率得到该结果,这类算法包括了葛洛沃搜索算法及其改进和推广算法；(3)相位估计量子算法。舒尔算法就属于这一类算法。它的思想是通过量子酉变换,估算特定态的相位,而这个相位与本征值成正比；(4)“相对黑盒”指数加速的量子算法。这类算法是一些特别设定问题的算法,在这些问题中,量子算法显示出明显的优越性,如道亦奇算法等。

4 算法复杂性理论

算法复杂性是衡量算法难易程度的尺度。在算法复杂性理论中,有容易的“多项式时间算法”与难的“指数时间算法”之分。用 n 表示需要输入的信息量大小时，解这个问题的算法需要的时间(或计算步数) 用 T(n)表示,一般认为

T(n)是 n 的某个函数。当 n 增大时，T (n)的增加不比 n 的一个多项式函数增加更快，则称该算法为“多项式时间算法”，否则就是“指数时间算法”。对指数时间算法，随 n 的增大，运算时间出现爆炸性增长。一台每秒执行 10^6 次基本运算的计算机，当 n = 50 时，若计算复杂性函数 T(n)=3n，计算时间需 2*10^8 世纪，这个时间已经超过了估计的宇宙年龄(一百多亿年)。在经典计算理论中，还有 P 类和 NP 类问题，人们把能够用“多项式时间算法”求解的判定问题，称为 P 类问题。把另一类迄今还没找到其“多项式时间算法”(但并未证明它没有多项式时间算法)的称为 NP 类问题。解决 NP 类问题就会导致一个指数时间算法，而分解大数质因子的问题，就属于 NP 类问题。对这类问题，如果能找到一个可以在多项式时间内解决的算法，就可把它化为易解的 P 类问题。一种 Shor 量子算法就是化 NP 类问题为 P 类问题的。人们推测，通过量子计算机，其它 NP 类问题都可转化为 P 类问题。

5 量子计算的应用前景

5.1 超级计算

量子计算最突出的便是其计算能力。美国最大国防承包商洛克希德•马丁公司将购自加拿大 D-Wave 公司的量子计算机系统用来“设计和测试复杂的雷达、空间和飞机系统”。这是第一家尝试将量子计算机用于商业用途的公司。如果洛克希德•马丁公司尝试获得成功，这可能就是量子计算起飞的标志。

5.2 量子通信

量子通信是量子信息学的一个重要分支，是量子信息中研究较早的领域。量子通信是以量子态作为信息单元来实现信息的有效传送的。在量子通信中，除了需要传统的经典信道外，更为主要的还需建立通信各方之间的量子信道。所谓量子信道实际上就是通信各方之间的量子纠缠。量子纠缠在通信中的应用，创造出了用量子信道传送经典比特的“ 量子密集编码”、用经典辅助的办法传送量子态的“量子隐形传态”以及信息保密传送所需的“绝对安全的量子密码”等经典信息理论不可思议的奇迹。这将彻底改变历史悠久的密码学等保密通信研究。

5.3 量子计算机

算法都只是为量子计算提供了重要的理论依据。要想真正实现量子计算，必须得能建造量子计算机。1994 年，劳埃德 (Seth Lloyd)和金布尔(Jeff Kimble)等人利用原子与光子耦合技术，创造了最初的量子逻辑门。同一时间，瓦恩兰（Dave Wineland）和门罗（Chris Monroe）则用离子阱与激光技术实现了类似的量子运算。不久之后，麻省理工学院的科研人员使用核磁共振技术建造具有七个位元的量子计算机，并在其上应用秀尔算法成功分解了整数 15——这标志着量子计算由理论走入了实践。尽管最近十几年来量子计算机的研制取得了长足的进步，但总体上说仍然处于摸索阶段，专家们对于建造量子计算机的最佳途径也没有共识。制造量子计算机最大的难题是如何克服外界对处于叠加态的量子系统的干扰。量子位元不但相互之间能够形成我们需要的量子缠结，它们也可能与外界的原子、分子之间形成量子缠结。如此一来，外界一个微小的扰动就有可以引发量子计算机中量子位元一系列的连锁反应，使量子叠加态遭到破坏（这种现象被称为量子退相干），从而导致计算错误。因此，量子计算机不得不消耗大量的资源用以控制和克服量子退相干引起的偏差。这个问题至今也没有找到比较完美的解决办法，可以说是现有的各种量子计算机的软肋。为了有效地对付量子退相干，科学家们正在寻求新的突破口。其中有两个研究方向

很值得注意：拓扑量子计算机和以玻色－爱因斯坦凝聚为基础的量子计算机。前者是以所谓“ 量子辫子”来作为量子位元，由于“量子辫子”是由二维空间上的奇异粒子（非阿贝尔任意子）在时空中的演进而形成的，它的拓扑性质不会因外界的扰动而改变，从而可以有效抑制量子退相干的影响。后者则是利用某些物质在极低温度下进入玻色-爱因斯坦凝聚态后所具有的合作效应来建构宏观尺度下的量子位元——它们与外界的微观粒子之间形成量子缠结的可能性会大大降低。

6 结束语

尽管目前传统计算潜力尚存，但人们为了避免山穷水尽的局面，依旧在积极探寻下一代的计算技术，而蕴含着强大计算能力的量子计算，伴随着量子力学的发展和计算机科学的进步，无疑是其中极具生命力与发展潜力的一种。尽管量子计算理论框架已经成型，但最终要充分施展其巨大能量，还存在许多亟待解决的理论和技术问题。Bennett 和 Zoller 教授说，“现在的量子计算机只是一个玩偶，真正做到有实用价值也许要 10、20 年甚至是 50 年”。诸如寻找适合构造量子计算机的物理系统,克服由于量子计算机和环境的相互作用而导致的量子耗散、量子消相干现象等问题，启发人们进一步去认识和揭示量子力学的奇妙特性。可以相信，未来量子计算的研究将会收获巨大成功，并对人类和社会发展起到巨大的推动作用。神奇而高效的量子计算时代，承诺着一个辉煌的未来。

【参考文献】

1 大数据与量子计算 王书浩①②, 龙桂鲁①②③ (① 清华大学物理系, 低维量子物理国家重点实验室, 北京 100084;② 量子物质科学协同创新中心, 北京 100084;③ 清华大学信息科学技术国家实验室(筹), 北京 100084)

2 量子计算—下一场信息革命 赵煦/ 编译 世界科学 2014.4

3 量子计算的挑战与思考 张焕国，管海明，王后珍 (武汉大学计算机学院空天信息安全与可信计算教育部重点实验室，湖北武汉 430072)

4 量子计算的进展和展望 周正威，涂涛，龚明，李伟锋，胡勇，杨勇，郭光灿（中国科学技术大学量子信息重点实验室，合肥 230026）

5 量子计算算法介绍 龙桂鲁 (清华大学原子分子与纳米科学重点实验室 清华大学物理系 北京 100084)

6 量子计算的研究现状和发展动向 陈平形 1，2，吴伟 1，2，吴春旺 1，2，吴俊杰 1，唐玉华 1(1. 国防科学技术大学高性能计算国家重点实验室，长沙，410073；2. 国防科学技术大学理学院，长沙，410073)

7 量子计算与超级计算机 赵春雷/ 编译 世界科学 2012.2

8 量子计算与计算机科学李建明 1，李锋 2 (1. 广东轻工职业技术学院，广东广州 510300；2. 广东交通职业技术学院)

9 量子计算及量子算法研究进展 王蕴，黄德才，俞攸红(浙江工业大学计算机学院，杭州 310023)

10 量子计算的昨天、今天和明天 汤双 博览群书 2013.07

11 量子计算进展与展望 郑建国,覃朝勇 (东华大学工商管理学院,上海 200051)

12 量子通信与量子计算 苏晓琴 1,2 ,郭光灿 1 (1 中国科学院中国科学技术大学量子信息重点实验室, 安徽合肥 230026 ;2 运城学院物理与电子工程系, 山西运城 044000)