量子计算机

0.引言

当前的计算机科学是建立在图灵机基础上的。图灵机是一个理想的模型，它由两部分组成:(1)具有无限长储存单元的记录带。每个储存单元的内容用“0”或“1”表示(2)一个具有内部状态并可在带上每次只能移动、读取、改写一个存储单元的阅读头。图灵机的操作每个周期有三个步骤：读、写、移动，即(1)读取当前位置上存储单元的内容；(2)根据阅读头的内部状态和读到的信息改变阅读头的状态，以及存储单元中的内容，并决定下一步移动的方向；(3)按照步骤(2)的方向，将阅读头移动一个存储单元。

图灵认为，图灵机的本能与其物质实现无关。但现实中，当存储单元小到原子大小时，微观尺度内的量子效应是否会影响图灵机的操作，或者能给它带来什么样的新特点呢？这个问题图灵未考虑过。现有经典计算已具有每秒上百亿次的计算速度，它是否仍可提高呢？随着计算机技术的飞跃发展，人们想知道计算机的运算速度有无上限。这一个问题也无法从图灵的理论中得到解答。这促使人们开始了量子计算机的研究。

1.量子计算机的历史

在1969年，史蒂芬·威斯纳最早提出“基于量子力学的计算设备”。而关于“基于量子力学的信息处理”的最早文章则是由亚历山大·豪勒夫（1973）、帕帕拉维斯基（1975）、罗马·印戈登（1976）和尤里·马尼（1980）年发表。史蒂芬·威斯纳的文章发表于1983年。1980年代一系列的研究使得量子计算机的理论变得丰富起来。1982年，理查德·费曼在一个著名的演讲中提出利用量子体系实现通用计算的想法。紧接着1985年大卫·杜斯提出了量子图灵机模型。人们研究量子计算机最初很重要的一个出发点是探索通用计算机的计算极限。当使用计算机模拟量子现象时，因为庞大的希尔伯特空间而数据量也变得庞大。一个完好的模拟所需的运算时间则变得相当长，甚至是不切实际的天文数字。理查德·费曼当时就想到如果用量子系统所构成的计算机来模拟量子现象则运算时间可大幅度减少，从而量子计算机的概念诞生。半导体靠控制集成电路来记录及运算信息，量子计算机则希望控制原子或小分子的状态，记录和运算信息。

量子计算机在1980年代多处于理论推导状态。1994年彼得·秀尔提出量子质因数分解算法后，证明量子计算机能做出离散对数运算，而且速度远胜传统电脑。因为量子不像半导体只能记录0与1，可以同时表示多种状态。如果把半导体比喻成单一乐器，量子计算机就像交响乐团，一次运算可以处理多种不同状况，因此，一个40比特的量子计算机，就能在很短时间内解开1024位电脑花上数十年解决的问题。因其对于现在通行于银行及网络等处的RSA加密算法可以破解而构成威胁之后，量子计算机变成了热门的话题，除了理论之外，也有不少学者着力于利用各种量子系统来实现量子计算机。

2.量子计算机的算法理论

量子计算机，顾名思义，就是实现量子计算的机器。是一种使用量子逻辑进行通用计算的设备。不同于传统计算机，量子计算用来存储数据的对象是量子比特，量子计算机使用量子算法来进行数据操作。

传统计算机在计算上有两大限制:(1)其输入态和输出态都是经典信号，用量子力学的语言来描述，也即是：其输入态和输出态都是某一力学量的本征态。所有的输入态均相互正交。对传统计算机不可能有叠加态；(2)经典计算机内部的每一步变换都演化为正交态，而一般的量子变换没有这个性质，因此，传统计算机中的变换（或计算）只对应一类特殊集。

对于这两点限制，量子计算机分别作了推广。量子计算机的输入用一个具有有限能级的量子系统来描述，如二能级系统（称为量子比特），量子计算机的变换（即量子计算）包括所有可能的幺正变换。

(1)量子计算机的输入态和输出态为一般的叠加态，其相互之间通常不正交；

(2)量子计算机中的变换为所有可能的幺正变换。得出输出态之后，量子计算机对输出态进行一定的测量，给出计算结果。

由此可见，量子计算对传统计算作了极大的扩充。

3.浅谈量子计算机的应用

正如大多数人所了解的，量子计算机在密码破解上有着巨大潜力。当今主流的非对称（公钥）加密算法，如RSA加密算法，大多数都是基于于大整数的因式分解或者有限域上的离散指数的计算这两个数学难题。他们的破解难度也就依赖于解决这些问题的效率。传统计算机上，要求解这两个数学难题，花费时间为指数时间（即破解时间随着公钥长度的增长以指数级增长），这在实际应用中是无法接受的。而为量子计算机量身定做的秀尔算法可以在多项式时间内（即破解时间随着公钥长度的增长以k次方的速度增长，其中k为与公钥长度无关的常数）进行整数因式分解或者离散对数计算，从而为RSA、离散对数加密算法的破解提供可能。但其它不是基于这两个数学问题的公钥加密算法，比如椭圆曲线加密算法，量子计算机还无法进行有效破解。

针对对称（私钥）加密，如AES加密算法，只能进行暴力破解，而传统计算机的破解时间为指数时间，更准确地说，是O(2^n)，其中n 为密钥的长度。而量子计算机可以利用Grover算法进行更优化的暴力破解，其效率为O(√(2^n))，也就是说，量子计算机暴力破解AES-256加密的效率跟传统计算机暴力破解AES-128是一样的。

更广泛而言，Grover算法是一种量子数据库搜索算法，相比传统的算法，达到同样的效果，它的请求次数要少得多。对称加密算法的暴力破解仅仅是Grover算法的其中一个应用。

在利用EPR对进行量子通讯的实验中科学家发现，只有拥有EPR对的双方才可能完成量子信息的传递，任何第三方的窃听者都不能获得完全的量子信息，这样实现的量子通讯才是真正不会被破解的保密通讯。

4.量子计算机的发展现状

4.1拓扑量子计算

该方案最初由数学物理学家Kitaev于1997年提出。他利用特殊系统不受小扰动影响的拓扑量子性质来构造量子计算机，从而可以实现容错的量子计算。目前，这一领域在国际学术界得到很大的重视，哈佛大学、哥伦比亚大学、芝加哥大学、加州理工学院等一流学校己开始了理论和实验方面的研究。

二维空间系统存在具有分数统计的准粒子，被称为任意子，任意子的统计包含阿贝尔和非阿贝尔两种，非阿贝尔任意子的拓扑性质能够用来做拓扑量子计算。用于做拓扑量子计算的任意子具有以下特点:

(1)有一系列不同类型的准粒子，用于信息的初始化。

(2)任意子的交换和旋转满足群论中的辫群规则，可以实现拓扑量子门，用来处理信息。

(3)拓扑量子计算中信息编码是非局域的，基本上不受周围环境的影响，因此错误率很低，具有自动容错的功能。

(4)满足干涉测量中的Bunching规则，可用于信息读取。

目前的研究表明，二维系统的非阿贝尔统计的任意子态最有可能在填充因子为5/2的分数量子霍尔效应中实现2009年，美国哈佛大学和以色列Weizmann研究所同时报道在实验上证实了这类态的存在，并在此态上构建了基本的量子位。

4.2单向量子计算

单向量子计算是R. Raussendorf和H.Briegel在2000年提出的一种新的途径。其思想是利用量子纠缠态以及局域操作和经典通信过程，可以传递非局域的相互作用，从而等价地实现非局域哈密顿量的功能。因此，可建立一种高度纠缠的状态(至少是二维的)，称为图态，只需要通过对相邻的几个量子比特进行LOCO过程，测量结束之后，可以等效地实现对出发端的量子比特的普适逻辑门操作。这样一来，图态就像是一个面包板，我们将有待实施的量子电路设计出来，将每个原件插上去就可以实现相应的量子操作。显然，量子计算标准模型的难度在这里就转化为如何高效而精确地实现一个超大量子比特数目的图态上。

4.3绝热量子计算

绝热量子计算最先是由MIT的Golbstone等人提出，其核心思想是通过绝热演化的特性来等效地实现量子么正变换。我们知道，在绝对零度时，如果系统的初态处于基态，那么绝热地变换系统哈密顿量的参数，只要不出现基态和激发态的能级交叉，原则上体系始终处于基态。然而，系统演化前后的基态之间必然有一个么正变换联系。如果这个么正变换恰恰就是我们所需要的么正变换，那么量子计算也就可以通过这个绝热过程完成。

该方案的优点在于，在理想情况下，系统始终处于基态，从而不存在退相干问题;其缺点是绝热的条件依赖于基态和第一激发态的能隙，能隙越小，所需要的绝热演化的时间就越长，如果随计算量的变大，绝热演化时间指数相应地变长，那么就失去了量子计算的意义。

近十多年来，著名刊物Vzture和Science平均每个月发表一篇量子计算机研究的论文，但至今量子计算仍然未有突破性的进展。在少数量子比特的物理体系统中，人们成功地演示了量子计算的原理、逻辑门操作、量子编码和量子算法等，证实量子计算的实现不存在原则性困难。但真正要研制出量子计算机，存在两大主要障碍，其一是物理可扩展性问题，即如何实现成千上万个量子比特，并能有效地进行相干操控;其二是容错计算问题，即量子操作的出错率如何能减少低于阀值，确保计算结果的可靠性。

当前，人们一方面寻找可扩展可容错的量子计算体系，另一方面着手研究技术难度较低的量子仿真。量子仿真的目的就是发展出一套多体系统相干操控的手段、通过实验直接操控、观测人工多体系统的演化行为，为强关联物理学等提供完美的检测场所。量子仿真的研究很可能带来全新的科学发现（如新物质的发现）。