计算的量子飞跃*

王 安 民

(中国科学技术大学量子通讯和量子计算开放研究实验室 中国科学技术大学近代物理系 合肥 230027)

摘 要 利用量子力学的迭加和纠缠等特性进行的量子计算是计算技术的巨大飞跃.它能够比经典计算远为有效地解决一些问题.例如最为著名的 Shor 的算法原则上能够以多项式的时间因子化大的合数,从而使得经典计算机难以计算的这一问题得以解决.文章介绍了至今所发现的主要量子算法的基本原理和步骤,并且概述了量子计算的优越性、现状和发展前景,同时讨论了量子计算在物理学上的应用和意义.

关键词 复杂性理论,量子计算,量子算法,量子模拟

A QUANTUM LEAP IN COMPUTING

WANG An-Min

(*Laboratory of Quantum Communication and Quantum Computation, Department of Modern Physics, University of Science and Technology of China, Hefei* 230027)

Abstract By exploiting quantum mechanical features such as super-position and entanglement, quantum computing is a huge leap forward for computing technology. It can solve certain problems much more effectively than classical computing. For example, Shor's algorithm could in principle factor large composite integers in polynomial time, thus solving a problem that classical computers still find difficult to calculate. An introduction is given to the fundamental principles and processes of the main quantum algorithms discovered so far. The advantages, current progress and future prospects of quantum computing are mentioned. In addition, the applications and significance of quantum computing in physics are discussed.

Key words complexity theory, quantum computing, quantum algorithm, quantum simulation

1 引言

计算是人类思维能力的最重要的方面之一.计算能力的提高与人类文明进步息息相关.从古老的算盘到现代的超级计算机,人类的计算技术实现了革命性的突破.综观当今,计算机的广泛应用已经并且仍在继续改变着我们的世界.一方面,人们为计算机的神奇能力所倾倒.另一方面,人们也为它无力完全满足实际的需求而烦恼.因此,加速计算机的运算速度以提高计算机的运算能力成为计算机科学的中心任务之一.

如何加快计算机的运算速度呢?这一问题大体可以从两个方面着手解决.一是制造更为先进的计算机硬件,另一则是设计恰当的计算机运算流程.后者可以称之为"算法".

算法这一词汇来源于 9 世纪波斯数学家阿布·雅发·穆罕默德·伊伯思·缪莎·阿勒霍瓦里松.尽管算法的例子有其悠久的历史渊源,但一般算法概念的准确表达从 20 世纪起才有明确的记载.事实上,这一概念的各种不同的表述都是在 20 世纪 30 年代给出的.历史上,虽然计算理论的先驱者 Turing, Church, Post 和 Gödel 等各自直观地把握到了正确的物理图像,但由于他们的工作并不明显地涉及物理学,长期以来,经典计算理论的基础被错误地假定为不言自明和纯粹抽象的.仅仅近 20 年来,关于计算的物理学问题才被提出和回答.

为了更清楚地阐明这一问题,我们必须强调指出的是:计算机是一物理系统,计算过程是这一物理系统随时间的循序演化.算法本身则作为该物理系统演化的一系列过程.正如大家所熟知的那样,如果认为计算机是一经典的物理系统,则其演化所遵循

* 国家自然科学基金资助项目
1999-07-21 收到初稿,1999-10-25 修回

的是经典的物理定律,或者说它受到基本的经典物理学规律的制约或限制.只有认识了它们之后,人们才能完全理解经典计算机的物理限制,才能有目的地改进计算机和它的计算速度.

更进一步讲,如果认为计算机可以是一个量子系统,情形又该如何呢?早在1982年,诺贝尔物理学奖获得者 Richard Feynman[1]最先给出了答案.他发现经典计算机不可能有效地模拟某些量子力学效应,由此推测利用量子效应一般能够进行更为有效的计算.

实际上,计算机将成为量子系统是计算机进一步发展的必然结果.因为计算机发展的"Moore(穆尔)定律"表明每个芯片(chip,即计算机的复杂度)上晶体管的数目随着时间指数地增加,更精确地说它每年翻一番.在过去的30年中,我们已经看到这一定律几乎被精确地遵循.如果这个指数增加规律被外推到不远的将来,到2017年,信息将被在单一的原子中编码.事实上,在此之前,到2012年,量子效应将变得非常重要.一旦量子效应多得对于计算有着显著的影响而不能够再被忽略时,那就必须用量子力学来描述计算过程.而且当量子效应变得重要时,例如在单个原子和光子的水平,现存的纯粹抽象的经典计算理论基本不再适用,全新的计算和信息处理的模型成为可能.从另一个方面看,认为今天的计算机是经典的观念实际上不是完全明显的,有必要作进一步阐明.现代计算机的基础建立在使用半导体技术之上.晶体管是所有现代计算机的"神经元",它通过利用半导体的性质而工作.然而,人们不能简单地从经典上理解半导体的功能,需要用量子力学来表述它.这就表明信息和计算的物理本质使得研究用量子力学进行计算成为必然.从科学研究的方法论上看,丰富的成果常常来自于两个好像不相关的观念的有机结合.量子力学和计算机科学的结合正是其中的一个杰出的例证.

既然计算机能够被看作量子系统,则支配它演化的就是量子物理的基本规律.也就是说,计算机可以成为用量子力学进行计算的量子计算机.那么,经典计算机所给出的物理限制是否依然存在呢?新的物理限制又是什么呢?1985年,Deutsch[2]发现这样的量子计算机能够处在迭加态中,每个态连贯地遵循不同的计算路径而相干产生最后的输出.这一在单片硬件中得到的"量子并行"超过了至今在经典计算机中所能够想象的任何并行,因此势必提供量子计算机具有前所未有的能力.这意味着经典计算机不能或难以处理的特定问题有可能通过量子计算机有效地解决.

令人振奋的结果终于出现了.1994年,Shor[3]提出一种基于量子相干性的量子并行算法,并证明量子计算机可以将一类问题从现有的指数增长的运算变成为多项式增长的运算,从而使运算速度有突破性提高.例如能够用几百万步完成因子化1000位数字的任务,而目前的经典计算机需要约10^{25}年才能做到.那么,当前被公认为最安全的、经典计算机不能破译的公开密钥密码系统 RSA 将能够用量子计算机容易地破译.1996年,Grover[4]提出量子搜寻算法,证明量子计算机在通过穷尽搜寻解决问题中比经典计算机戏剧性加速.用此算法,可以仅用2亿步取代经典计算机的大约3.5×10^{16}步,破译广泛使用的56位数据编码标准(DES,这是一种被用于保护银行间和其他方面金融事务的标准).只需几个至几十个比特的装置的简单量子计算机便可能进行许多有意义的量子模拟计算的工作,而且这些计算是经典计算机系统所难以承担和准确实现的.这些模拟计算对推动当代物理学、生物学、材料科学等诸多领域的发展有十分重要的意义.

量子计算具有经典计算所不曾有的、也不可能有的威力.它使计算技术出现了真正的量子飞跃.量子计算通过其强大和快速的计算能力将可能使得科学的许多分支产生重大变革.尤其是在社会的经济发展、国家的安全保障和人类的文明进步方面已经展现出具有一些重要的用途,并且将十分可能有着非常巨大的应用潜力.

2 复杂性理论和算法

计算理论所研究的一个十分基本的问题是:什么是可计算的和它们能够怎样被有效率地计算.历史上,Turing机是一个典型的范例,由此我们定义了可计算性和效率.为了按照解计算问题所需的物理资源将计算问题分类,复杂性理论得以诞生.此处所说的物理资源通常指时间和存储量(常称为空间).只要物理框架选定,分类应当不依赖于特定的计算模型,而仅仅度量了问题的固有难度.许多计算问题都有代表问题规模的特征量 N,例如取它为需要完全确定问题输入的比特的总数目.计算时间随 N 变大以一定的方式增长.如果所需时间是 N 的幂次或多项式,例如 N, $N\log N$, N^2, N^3 等等,那么可以通过计算机求解.相应的问题称为"多项式时间

问题”,记为 **P** 问题,如果计算的时间随 N 指数上升,例如比例于 2^N,e^N,3^N 等等,相应的问题称为“指数时间问题”,记为 **NP** 问题,显然只要 N 足够大,就不可能在有限的时间内计算出来.当存储量被视为主要的物理资源时,类似地,能够定义空间 **P** 和空间 **NP** 问题.

为了解特定的问题,计算机遵循一组精确的指令集合,对于任何给定问题的实例,可以应用它们得出解.这个指令的集合称为算法.一些算法是快的(例如乘法),另一些是非常慢的,例如考虑如下的因子化问题:? × ? = 29083,相对于解逆问题 127 × 129 = ? 而言,它所需时间要多得多.我们已经知道关于乘法的快算法,但我们并不知道关于因子化的快算法.遵循标准的定义真正涉及了快和可用的算法不是乘一个特定对的数目所用的时间,而是当我们把相同方法用到更大的数目时所需时间并不急剧增加的事实.当两个 3 位数转换到两个 30 位数时,用同样的标准教科书方法——乘法需要很少的额外的时间.与之相比,用最简单的除法分解 30 位数比分解 3 位数多耗费约 10^{13} 倍的时间和存储量.当我们继续增加位的数目时,计算资源的使用是巨大的.甚至没有人能够设想怎样才能有效地分解比方说 400 位数,因为计算将需要宇宙的估计年龄的时间.因而我们说,乘法属于 **P**,而因子化属于 **NP**,后者是一个难解问题.难并不意味着“不可能解”或“不可计算”,因子化大数用经典计算机似乎能做,可是它所需的物理资源如此之大之多,以致于相对于任何实用的目的而言,被认为是难以做到或没有效率的.

人们必须意识到这种复杂性分类不是一成不变的.今天不知道是 **P** 的问题,明天可能被重新分类,如果一个多项式算法被发现了的话.换言之,复杂性分类之间的界限不是固定的.事实上,经典复杂性理论的主要的未解决问题是要知道是否 **P** = **NP**.

值得注意的是计算机科学家断言,按照复杂性类的分类不依赖于计算机特定的物理模型.例如,计算机的祖先 Babbage 机和现代数字计算机尽管技术上的差距十分明显,但能进行相同的计算.而且对于因子化两者有相同的难度,执行时间都是随着数的大小指数地增长.那么,能够得出结论:纯粹的技术进步仅能通过改变固定的乘积因子提高计算速度,而这一乘积因子的改变并不有助于改变输入大小和执行时间的指数相关性.不过,事情并非如此简单.例如,一个能够根据问题规模调整处理器数目的并行计算机可以用多项式时间解出指数难度的问题.但为实现此目的,可用的处理器的数目必须随着问题的复杂性以相同的比例增长.对于指数问题,这显然是一个非物理的假定(计算机的规模必须指数地增长).然而,对于这个(非物理的)计算模型,我们能定义新的 **P** 类型的问题集合,它包括了不允许指数并行的计算模型所定义的 **P** 类型的问题集合之外的问题.这个例子表明了这样一个事实,遵循问题复杂性的分类取决于计算模型的物理学.如同我们将要看到的那样,不同的物理学可意味着不同的复杂性.利用量子物理效应的量子计算扩大了可计算问题的范围,极大地提高了完成计算任务的效率,在原则上能够使得某些对于经典计算机是 **NP** 的问题转换为 **P** 问题.

3 量子计算机

正如大家所熟知的那样,在经典数字计算机中,信息被编码为位(比特)链.1 比特信息就是两种可能情况中的一种,0 或 1,假或真,是或非.例如,电容器的极板之间的电压表示 1 比特信息:带电的电容器表示 1,而放了电的电容器表示 0.取而代之,量子计算机中量子信息的基本存储单元是比特的量子推广——量子位(qubit).一个简单的量子位是一个双态系统,例如半自旋或两能级原子:自旋向上代表 0,自旋向下代表 1;或者基态代表 0,激发态代表 1(注意,量子位可以是一个纯态,也可以是一个较大、非定域系统的一部分).与经典的比特不同,量子位不但可以处在 0 或 1 的两个状态之一,而且一般地可以同时处于两个态的迭加态.物理上可表示为二维 Hilbert 空间的矢量,即 $\alpha|0\rangle + \beta|1\rangle$($|\alpha|^2 + |\beta|^2 = 1$).由 L 个量子位组成的量子寄存器能够一次存储 2^L 个“数字”(2^L 维 Hilbert 空间的矢量).即量子寄存器随着位数的增加能够指数地增加存储的数据量.

在经典计算机中,信息的处理是通过逻辑门进行的.一个逻辑门遵循真值表将输入位的状态映射到另一状态.对应的量子(逻辑)门则是遵循同样的真值表经由幺正变换实现输入基态到对应态的演化.这意味着量子计算机能够在一次计算($2^L \times 2^L$ 幺正变换,相当于该量子系统的时间演化,是按规定的方式通过改变多粒子迭加态把系统的初态演化为末态)步骤中对于被编码在 L 个量子位的 2^L 个数字进行数学运算,这就是所谓的量子并行的由来.任何经典计算机为了完成相同的任务必须重复 2^L 次

相同的计算,或者人们必须使用 2^L 个不同的并行工作的处理器.换言之,量子计算机利用了量子信息的迭加和纠缠的性质,在使用如同时间和存储量那样的计算资源时提供了巨大的增益.

一般地说,量子计算机是一类遵循量子力学规律和特性进行高速数学和逻辑运算、存储和处理量子信息的物理装置,或者说是依照量子力学的规律和特性进行实际计算或处理量子信息的功能单元.

为了进一步说明量子计算机的优越性,让我们来看看量子计算机如何处理函数.考虑函数 $f:0,1,\cdots,2^m-1\to 0,1,\cdots,2^n-1$,其中 m 和 n 是正整数.经典计算机通过演化每个标记的输入 $0,1,\cdots,2^m-1$ 进入它相对的标记输出 $f(0),f(1),\cdots,f(2^m-1)$.由于量子计算的幺正(因而可逆)特征,它以稍微不同的方式计算函数.在计算非一一对应的函数时,它通过保持输入的记录维持计算的可逆性.因此,量子计算通常需要使用两个寄存器,第一个寄存器存储输入数据,第二个寄存器存储输出数据.将每个可能的输入 x 表示为第一个寄存器中的量子态 $|x\rangle$,而每个可能的输出 $y=f(x)$ 表示为第二个寄存器的量子态 $|y\rangle$,对应于不同的输入态之间和不同的输出态之间是正交的.那么通过幺正演化算子 U_f 作用在两个寄存器上,得以确定函数的计算:

$$U_f|x\rangle|0\rangle=|x\rangle|f(x)\rangle, \tag{1}$$

在计算复杂性的考虑之内,已经证明一个可逆函数的演化,即保持与输入联系的函数演化,如同正则的不可逆演化一样的好.这意味着如果给定的函数能够在多项式时间内被计算,它也能够用一个可逆计算在多项式时间内被计算.我们在此所考虑的计算不仅是可逆的,而且是量子的,它同时对于所有迭加的态作用得出输出态全部值,即展现了"大规模量子并行".在 Shor 的因子化方案等量子算法中这是十分关键的.

量子计算机中复杂的幺正变换可以通过由几个或更多的量子门构成的网络实现.这样的量子网络是由计算步骤在时间上同步的量子逻辑门组成的基本量子计算装置,或这些基本的量子网络组合成更为复杂的量子网络.对于基本算术运算的量子网络能够用许多不同的方法构成.一般而言,任何量子算法可以利用量子网络来描述.而量子计算机通过恰当的量子算法能够在多项式时间内解决一些经典计算机需要指数时间去解决的 **NP** 问题.

4 Deutsch 算法

Deutsch 问题是至今所知的第一个和最简单的量子算法之一.然而,它阐明了一些量子计算的重要性质.仅取最简单的一个输入位 x 和一个输出位(未知函数) $f(x)$.因为每个 $f(0)$ 和 $f(1)$ 有两个可能值,我们共有四个可能函数值:$f_1(0)=f_1(1)=0$;$f_2(0)=f_2(1)=1$;$f_3(0)=0$ 和 $f_3(1)=1$;$f_4(0)=1$ 和 $f_4(1)=0$.目的是要判断 $f(x)$ 是不变的[$f(0)=f(1)$,如 f_1 或 f_2] 还是均衡的[$f(0)\neq f(1)$,如 f_3 或 f_4].直观上,最好的经典策略是对于输入 0 和 1 明显地计算 f,然后比较结果.所以人们为了回答该问题需要函数 f 的两次演算.

但是,量子算法仅需要一次演算就能够得到结果.这一算法最先由 Deutsch 提出,后经改进得到.人们需要两个量子位.算法按如下步骤进行:

(1)首先,第一个量子位被初始化在态 $|0\rangle$,且第二个量子位被初始化在态 $|1\rangle$.总的态是 $|01\rangle$;

(2)对于每个量子位作用 Hadamard 变换 $H=(\sigma_1+\sigma_3)/\sqrt{2}$,其中 σ_1,σ_3 是通常的 Pauli 矩阵.那么,使得态成为 $H\otimes H|01\rangle=(|00\rangle-|01\rangle+|10\rangle-|11\rangle)/2$;

(3)通过定义作用在基矢上的双位门 $U_f:|i,j\rangle\to|i,j\oplus f(i)\rangle$,在上述迭加上计算函数 f,其中 $i,j=0,1$,且 $\oplus$ 表示模去 2 相加;

(4)最后,再一次对于每个位进行 Hadmard 变换.容易验证两个量子位的终态是:$|01\rangle$(如 $f=f_1$),$-|01\rangle$(如 $f=f_2$),$|11\rangle$(如 $f=f_3$);$-|11\rangle$(如 $f=f_4$).

所以,最终的对于第一个量子位的测量将展现是否函数是不变(输出 0)或均衡的(输出 1).

从上述的算法中,我们能够看到量子力学的迭加和线性性质是关键所在:当 U_f 作用于态 $(|00\rangle-|01\rangle+|10\rangle-|11\rangle)/2$,它迭加的四个态上的 f 被同时有效地计算出来.而且,量子干涉也是重要的:最后的两个 Hadamard 变换导致迭加中不同部分相干涉得到有用的终态.因此,量子力学的规律起到了决定性的作用.值得强调的是,该算法仅给出了 f 的整体性质的信息,即它是不变的,还是均衡的,我们无从知道 $f(0)$ 或 $f(1)$ 之值.

5 Shor 算法

这是一个由 Peter Shor 在 1994 年发明的算法,

它能够用于快速因子化大数.所谓因子化可以简单地描述如下:我们想要找到 N 的质数因子,这等于找到 N 的最小因子 r,使得 $a^r \equiv 1 \pmod N$,其中 a 被选择为 N 的互质数,即除了 1 之外,a 和 N 没有公约数.换言之,我们想要确定函数 $a^r \pmod N$ 的周期.比方说,$N=15$,我们看看这如何得出:

首先选择 $a=2$,那么明显地 2 与 15 互质.其次分别计算 $2^0, 2^1, \cdots, 2^{15}$ modulo 15,得出在寄存器 B 中相对应的一个重复序列:1,2,4,8,1,2,4,8,1,2,4,8,1,2,4,8.这个序列是周期为 $r=4$ 的周期序列,它也满足 $2^4 \equiv 1 \pmod 15$.一旦 r 被获得,通过计算 $\gcd(a^{r/2} \pm 1, 15)$ (gcd 是最大公约数),可求得 N 的因子,在我们的例子中,$\gcd(4 \pm 1, 15) = 3, 5$.

至此我们已经分解 15 为 3×5.现在这个算法能够在经典计算机或量子计算机中实现.但是效率根本不同.Shor 所描述的量子算法能够以多项式的时间在量子计算机上高效运行.下面我们简要介绍一下这一算法的主要特征和步骤:

(1)若要分解 N,取两个具有 $k(k \simeq \log_2 N)$ 个量子位的量子寄存器,并制备第一个寄存器,使其处在从 0 到 $2^k - 1$ 连续的自然数的等权迭加中,留下第二个寄存器处在 0 态,即

$$|\Psi\rangle = \frac{1}{\sqrt{2^k}} \sum_{n=0}^{2^k-1} |n\rangle |0\rangle . \tag{2}$$

注意,将 n 转换为二进制位链即为寄存器的一般状态.

(2)在第二个寄存器中计算函数 $a^n \bmod N$,结果为

$$|\Psi_1\rangle = \frac{1}{\sqrt{2^k}} \sum_{n=0}^{2^k-1} |n\rangle |a^n \bmod N\rangle . \tag{3}$$

(3)对第二个寄存器做投影测量 $|u\rangle\langle u| = |a^m \bmod N\rangle\langle a^m \bmod N|$,可得

$$|\Psi_2\rangle = \sum_{j=0}^{[2^k/r]-1} |jr+l\rangle |u\rangle , \tag{4}$$

其中我们略去了归一化因子.例如前述的 $N=15$ 和 $a=2$ 的例子.对第二个寄存器进行一次测量,可以得到 1,2,4,8 这四个值中的一个.设测得的值为 4,根据量子测量理论第二个寄存器处于状态 $|4\rangle$,且余下的态是 $|\Psi_2\rangle = |2\rangle + |6\rangle + |10\rangle + |14\rangle = \sum_{j=0}^{3} |4j+2\rangle$.在以下的步骤中,第二个寄存器不再使用,可以略去不写.

(4)为了提取在第一个寄存器中包含的周期 r,对它进行分立傅里叶变换(DFT),

$$U_{\mathrm{DFT}} |jr+l\rangle = \frac{1}{\sqrt{2^k}} \sum_{y=0}^{2^k-1} \exp\{2\pi \mathrm{i} \cdot (jr+l) y/2^k\} |y\rangle , \tag{5}$$

根据正交条件可知,仅当 $y = mM$($m=0,1,\cdots$)时,$\sum_{j=0}^{M-1} \exp\{2\pi \mathrm{i}\, jy/M\} = M$,否则为零.那么当 $2^k/r$ 是整数时,我们有终态

$$|\Psi_3\rangle = \frac{1}{\sqrt{r}} \sum_{m=0}^{r-1} \exp(2\pi \mathrm{i}\, lm/r) |m2^k/r\rangle . \tag{6}$$

值得指出的是,当 $2^k/r$ 不是整数时,需要进行更为仔细的分析.即使在这样的一般情形下,DFT 仍然保留了在上述特定情形中说明的特征,即它转换了输入寄存器中的周期性($r \to 2^k/r$),并且它具有淘汰 l 的平移不变性.那么,通过 U_{DFT} 作用在 $|\Psi_2\rangle$ 中具有不同 l 的迭加态上,我们总能得到这样的终态,对于该态测量的输出态和发现输出态的几率不依赖于 l.

(5)在 $y = m2^k/r$ 基进行测量,其中 m 是一个整数.所以,一旦我们获得了特定的 y,必须解方程 $y/2^k = m/r$,其中 y 和 2^k 是已知的.假定 m 和 r 没有公约数(除 1 外),通过把 $y/2^k$ 约化到一个不可约的分数得到 r,那么容易根据因子化算法(最后一步)推断 N 的因子.如果 m 和 r 有公因子,那么该算法失败.整个算法必须从头重复.

因此,一般而言,Shor 的算法是概率性的.这意味着,通过运行以上的量子计算,我们得到的 N 的因子或许有时不是正确的回答.通过乘因子看是否得到 N 容易检查答案正确与否(乘法是一个易解的计算,能够被有效率地执行).如果结果不是 N,我们能够从头重复完整的 Shor 的算法,并且继续做直到得出正确的回答.Shor 证明,即使他的算法中有随机的要素,其仍然是有效率的.事实上,最多的时间耗费是第一步,它能够在 $O(k^3)$ 的时间和用 $O(k)$ 的存储量完成.而且,为了寻找周期的 DFT 也是有效率的,它能够用 $O(k\log k)$ 步运算实现.正是因为全部计算仅仅需要多项式时间被重复,该算法整体上是多项式的.

在 Shor 的原始文章中,他也证明了怎样解离散对数问题.其量子算法非常类似于上述的因子化算法.

6 Grover 算法

1996 年,Lov Grover 写下一个用量子计算机搜

寻未结构化数据比用经典计算机要快得多的算法.在经典计算机中,从具有 N 个条目的数据库中找到一个特定的条目通常需要进行 $N/2$ 步的搜寻.例如,仅知电话号码,在电话本中查寻某人的名字的问题.Grover 的量子算法使得可能在量子计算机中用 $O(\sqrt{N})$ 步完成同样的搜寻.尽管未加速到指数那样好,但随着数据大小和集成度的增加,对于时间的节省是有意义的.

上述的所谓搜寻问题可以形式化地表示为:考虑分别被标记为 $S_0, S_1, \cdots, S_N$ 的 $N(=2^L)$ 个不同的状态和一个条件 C_j,假定仅有一个态 S_j 满足该条件.我们的目的是当最小化条件 C_j 的演化数目时确定 S_j.解该问题的 Grover 算法可归纳如下:

(1)开始设置单个量子寄存器处在所有计算态的等权迭加中,如同在 Shor 算法中一样(第一个寄存器).但通常将它写为如下形式:

$$|\Psi(\theta)\rangle \equiv \sin\theta|j\rangle + \frac{\cos\theta}{\sqrt{N-1}}\sum_{i\neq j}|i\rangle, \quad (7)$$

其中 j 是要搜寻的元素 $t=S_j$ 的指标.显然初始制备的态是 $|\Psi(\theta_0)\rangle$,其中 $\sin\theta_0 = 1/\sqrt{N}$.

(2) 首先仅翻转迭加中一个特定元素的态 $|j\rangle$ 的符号,其他不变;接着做分立傅里叶变换;然后改变除 $|0\rangle$ 之外的所有分量的符号;最后傅里叶变换反演回来.所有这四步运算表现了完成下列变换的精细的干涉效应:

$$U_G|\Psi(\theta)\rangle = U_{DFT}^{-1}(2|0\rangle\langle 0| - I)U_{DFT}\cdot(I-2|j\rangle\langle j|)|\Psi(\theta)\rangle = |\Psi(\theta+\phi)\rangle, \quad (8)$$

其中 I 是单位矩阵,$\sin\phi = 2\sqrt{N-1}/N$.特定元素的系数现在稍微比所有其他元素大一些.如完成第一次运算之后,特定元素 $|j\rangle$ 的系数由 $1/\sqrt{N}$ 增大到 $(3N-4)/(N\sqrt{N})$.

(3)通过运用 U_G m 次,这个方法被简单地继续下去.在此,$m \simeq (\pi/4)\sqrt{N}$.缓慢的转动引起 θ 非常接近于 $\pi/2$,使得量子态变得几乎精确地等于 $|j\rangle$.在 m 次反复之后,态被测量,获得值 j[具有 $O(1/N)$ 的误差率].如果 U_G 被运用次数太多,成功的几率反而变小,所以知道 m 是重要的,在此我们不打算详述这一问题.

Grover 的算法能够被推广到多于一个元素满足条件 C_j.在此情形下,甚至需要更少的迭代.但为了最佳化成功的几率,人们需要有标记元素数目的预先的知识.Grover 也已经将他的思想推广到其他问题,证明了均值或中值的估计问题能够用类似的技术去解.

7 量子力学系统模拟

量子模拟指的是用特别设计的量子系统(例如量子计算机)模拟实际的量子系统.事实上,能够有效地模拟一些量子系统是量子计算机最明显的应用之一,也是量子计算非常重要的一个方面.在 1982 年,费曼最先猜想量子计算机将能够以比它可能在经典计算机上远为精确和有效地模拟量子力学系统,推测具有几十个量子位的量子计算机能够模拟在经典计算机上需耗费不能实施的时间才可模拟的任务.这是由于所用的计算时间和存储量按照所考虑的量子系统规模的指数函数增加的缘故.具体地说,为了模拟一个在 2^L 维 Hilbert 空间的态矢量,经典计算机需要处理包含数量级为 2^L 个复数的矢量,而量子计算机仅需要 L 个量子位,使得它在存储空间更加有效率.但是对于模拟演化,一般说来,经典和量子计算机都将是效率低下的.经典计算机必须处理包括数量级为 $2^L \times 2^L$ 个元素的矩阵,这需要幂为 L 指数大数目的运算(乘法、加法),而量子计算机必须建立 2^L 维 Hilbert 空间的幺正运算($2^L \times 2^L$ 维矩阵),这通常需要指数大数目的基本量子逻辑门.所以量子计算机并不能保证有效地模拟每个物理系统.当然,所有这些量子逻辑门以量子并行的方式同时作用,在此意义上与经典计算机相比又是有效率的.值得强调的是:能够证明,通过利用量子计算的一些对称性质,可设计出高效的量子计算网络,使得所需量子逻辑门的数目极大地减少.极为典型的一个例子是,量子力学中坐标表象到动量表象的变换类似于分立傅里叶变换,可以约化为分别作用在各个量子位上的 Hadamard 变换加转动后的直积,从而使所需量子逻辑门的数目是 $2L$ 个(不计及辅助的门).因此量子模拟还是能够有效地模拟一大类量子系统,其中包括许多没有经典算法的系统,例如定域相互作用的多体系统等.

在经典计算机中,量子系统的动力学能够用近似的方法模拟.可是,量子计算机通过引入它的变量之间的相互作用,可程序化地模拟系统的行为.因而模仿了所考虑系统的相互作用特征.例如,量子计算机可以模拟“Hubbard 模型”(它描述了晶体中电子的运动),这是一个超越了现今通常计算机范围的任务.

8 结语

我们已经介绍了至今所发现的量子计算机优于经典计算机的主要算法.更多的量子算法问题正在研究之中,例如图形同构和点阵中最短矢量等.那么,什么是量子算法的进一步发展呢? Kitaev(1996)[5]研究了怎样用与 Shor 根本不同的技术解因子化和相关的问题.他的想法有一点类似 Grover.继而,Jozsa(1997)[6]阐明了 Kitaev 的方法,也说明了基于傅里叶变换的几个量子算法的共同特征.量子程序员的工具箱正在慢慢地变大.然而,关于量子计算能力的许多基本问题尚未解决.例如,不知道是否任何 **NP** 问题都能在量子计算机上有效解出.

所以,考虑量子计算的前景常常集中在 **NP** 完全性问题上.特别是,量子计算的梦想是能够指数加速解出此类问题.在这一点上,Bennett, Bernstein, Brassard 和 Vazirani(1997)[7]获得了重要的结果,它们证明,对于数据库搜寻问题的 Grover 算法事实上是最好的,没有比时间量级 $O(\sqrt{N})$ 更快的量子算法.这个结果似乎暗示不能证明量子计算在多项式时间内能够解 **NP** 完全性问题.至少它指出没有这样的多项式时间依赖"量子魔术"的量子算法存在.但是,为了得到确切的结论,或许需要充分和深入地考察 **NP** 完全性问题的结构.

NP 问题可能不是量子计算机的最好的用武之地.量子计算机可以解决 **NP** 之外的问题,量子模拟就是一个例子.通过研究使用多项式量子资源指数地存储复杂的量子态能力的算法,以及设计高效量子网络,量子计算可能出现更为戏剧性的高潮.

特别值得指出,量子计算成功与否取决于量子计算机的纠错和容错能力.上述介绍的量子算法的计算效率中,尚未考虑这些因素的影响.但是,已经证明原则上量子纠错和容错对于计算资源的耗费是呈对数增加的,可以用量子并行加以解决.因而上述量子算法仍然是有效率的.

量子计算的优越性的确已经点燃了许多想象之火,似乎量子计算机无所不能,经典计算机寿命可期.但在我看来,就目前的进展而言,这不仅是言之过早,而且是一个错误的印象.量子计算机将并不取代经典计算机,如同量子力学并不取代经典物理学一样.如果实用的量子计算机一旦出现,它将用于恰恰是得益于量子信息处理的那些特殊的任务.

我们已经确切地知道量子计算的能力与量子纠缠、量子并行和巨大的 Hilbert 空间性质有关,并且量子测量的本质也有影响.但是可以说,目前对于量子算法运行的深刻理解仍不足够,对于量子算法本质特征的认识仍需进一步探索.一个十分大胆猜测的基本问题是:Planck 常数 $\hbar$ 怎样进入量子计算,并且什么是 $\hbar \to 0$ 的极限.或许对于这类问题的较好的理解有助于我们逼近新类型的量子算法.当然,这正是物理学家十分感兴趣的工作.

关于量子计算的更为永恒和令人激动的理由是它所导致的思考物理学基本定律的心得,所涌现的应用物理学和其他科学技术的有创见的方法,以及给我们那种意识到尚未揭开关于自然的某些深刻奥秘的感觉.事实上,对于量子计算的进一步研究将使得我们能够发现更深层次的科学问题,例如涉及纠缠、消相干、传送、量子系统制备、控制、操作和量子测量方面的新物理学.

最近几年,量子计算的理论研究已经取得了重大的突破和实质性的进展.S.Lloyd 描述了许多有可能类似于量子计算机行为的物理系统,Peter W Shor 证明了量子计算可用于大数分解,Grover 提出了快速量子搜寻算法,I.L.Chuang 等提出了尝试解决"Deutsh 问题"的一个简单的量子计算机模型,C.H.Bennett等进一步澄清了纠缠问题,使量子纠错的理论方案和量子容错计算的模型得以建立.实验研究也有一系列令人振奋的进展,例如 2 个量子位的所有量子逻辑门已经被实现.各种量子计算的实验实现不断涌现.尤其是 NMR(核磁共振)量子计算已经能够验证简单的量子算法和量子纠错,制备 GHZ 态和实现量子超距隐形传态(teleportation).德国科学家已经进行了 5 个量子位的 NMR 试验,美国 Los Alamos 国家实验室正在进行 7 个量子位的 NMR 试验.如果成功,将是量子计算走向实际运用的关键一步.按照现状来看,科学家已经能够控制几个位的量子逻辑运算,在不远的将来,他们很可能用几十位或几百位来进行量子计算.基本物理学原理和许多科学家们的研究告诉我们:建造量子计算机理论上和原则上没有根本的障碍,但在实际上和技术上仍然是一个巨大的挑战.尤其是实用的、具备一定规模的量子计算实现尚在探索之中,与之相联系的量子计算理论仍在发展之中.当你了解量子计算机具有改变世界的威力的时候,你将感到值得和乐意为之奋斗.大家的共同努力会使得它为期不远,它的最终的成功是我们的坚定信念.

(下转第 373 页)