DOI:10.19484/j.cnki.1000-8934.2007.01.006
第23卷 第1期 自然辩证法研究 Vol. 23, No. 1
2007年 1月 Studies in Dialectics of Nature Jan., 2007

文章编号:1000-8934(2007)01-0022-05

计算复杂性、量子计算及其哲学意义

吴国林 黄灵玉

(华南理工大学 政治与公共管理学院,广东 广州 510640)

摘要:量子计算机具有超越经典计算机的能力。量子计算具有并行性和整体性,某些量子算法具有加速性。量子计算揭示了:数学与物理学之间的紧密关系,量子力学的波函数具有实在性。量子计算具有克服计算复杂性的能力。

关键词:量子计算;量子算法;计算复杂性

中图分类号:N031 文献标识码:A

探索复杂性是20世纪以来形成的重大趋势。计算机是人类创造出来的最伟大的技术人工物之一,它是探索复杂性的关键性工具。1985年,多依奇(David Deutsch)定义了量子计算机。1994年,肖尔(Peter Shor)发现了具体的量子算法。1993年,本内特(C. H. Bennett)等6位科学家发表量子隐形传态的重要论文。20世纪后半期,量子计算、量子密钥分配算法和量子纠错编码等3种基本思想的出现,标志着量子信息理论基本形成。量子信息理论之前的计算复杂性基于经典计算机理论,量子计算将会改变原有的经典计算复杂性理论。本文将讨论量子计算的特点、量子计算对经典计算复杂性的克服及其哲学意义。

1 算法与计算复杂性的涵义

算法是对数据运算的描述,它是解一类问题的方法,或者是某种指令集。一个算法是一个有限规则的集合。计算复杂性是衡量算法效率的一种指标。现有的计算复杂性理论主要是针对经典计算而言的。计算复杂性分为时间复杂性和空间复杂性。

计算复杂性是算法所求解问题规模的某个函数。通常用一个自然数n来度量问题规模的大小。对于大小为n的问题,如果计算它最多需要时间为f(n),则这一问题类的时间复杂性为f(n)。算法的渐进时间复杂度T(n)=O(f(n)),其中T(n)是算法所耗费的时间。当问题的规模n趋向无穷大时,T(n)的数量级称为渐进时间复杂度,符号"O"表示T(n)的数量级。如果求解一个问题需要的运算次数是问题规模n的指数函数,则称该问题具有指数时间复杂性。如果所需的运算次数是n的多项式函数,则称它具有多项式时间复杂性。时间复杂性函数T(n)=O(p(n))((p(n))是多项式)的算法,称为多项式时间算法。

空间复杂性是指计算机中运行时所占用的存储空间大小。一个算法的空间复杂性h(n)也是问题规模n的函数。时间复杂性的减小通常是以空间复杂性的增大为代价的;空间复杂性的减小也往往导致时间复杂性的增大。

不同的算法具有不同的时间复杂性函数。对于多项式时间复杂性函数,工作量随问题规模n增长而增长的速度都比较平缓,但对于指数时间复杂性函数,这种增长到后来就非常剧烈[1]。研究表明,提高计算机速度,对计算机的算法复杂性改善较小。多项式时间算法被看作是"好的"算法。

在经典计算复杂性理论中,计算问题分为三类:P类、NP类、NPC类。具有多项式时间复杂性的问题类称为P类问题,这一类问题是大量存在的。NP类问题是能够写出其算法,但对它们已知的最好的算法不能用多项式来表示。NP类有一些具有特殊性质的问题,它们的计算复杂性具有等效性,如果它们当中的一个问题能用多项式时间解决,则其余的问题也都能用多项式时间求解,这样的问题我们称

收稿日期:2006-09-04

基金项目:广东省哲学社会科学"十五"规划项目"量子信息的哲学研究"(编号03104B07);教育部社科研究2006年度项目"量子控制论的哲学研究"(编号06JA720011)

作者简介:吴国林(1963-),四川营山人,哲学博士,教授,副主任,硕士生导师,研究方向:量子信息哲学、技术哲学与系统哲学等;黄灵玉(1980-),女,华南理工大学科技哲学硕士研究生,研究方向:自然科学的哲学问题。

之为 NP—完全问题类, 记作 NPC 类。一般认为, P 类问题是可以有效解决的; NP 类问题不能有效解决。

2 量子计算的基本特点

从物理学来看, 计算机就是一个物理系统。量子计算机就是一个量子力学系统, 量子计算过程是量子力学系统的量子态的演化过程。经典物理中不同的物理态可以迭加形成存在于量子计算机中, 量子态之间的纠缠在不同的量子比特之间建立了量子"信道"。计算过程可归结为制备物理态, 演化物理态, 最后对物理态实施测量。[2] 经典计算的理论事实上是建立在对编码态以及计算过程的经典物理理解的基础上。而量子计算则建立在对编码态以及计算过程的量子力学理解的基础上。量子算法、量子编码、量子逻辑网络是实现量子计算的三个关键问题, 目前已取得了重大突破。相对于经典计算, 量子计算主要具有以下特点:

(1) 量子存储器具有巨大的存储能力　量子计算机最基本存储单元是量子比特。一个量子比特是一个双态系统, 且是两个线性独立的态。两个独立的基本量子态常用狄拉克符号记为: $|0\rangle$ 和 $|1\rangle$。量子比特是两态量子系统的任意叠加态。比如 $|\psi\rangle = C_0|0\rangle + C_1|1\rangle$, 且 $|C_0|^2 + |C_1|^2 = 1$, 其中系数 C_0 与 C_1 为复数。

量子寄存器就是量子比特的集合。对于 n 个量子位的系统, 其中一个状态可表示为:

$$|a\rangle = |a_{n-1}\rangle |a_{n-2}\rangle \cdots |a_1\rangle |a_0\rangle,$$

$$a = 2^{n-1}a_{n-1} + 2_{n-2}a_{n-2} + \cdots + 2^1 a + 2^0 a_0,$$

其中 $a_i = \begin{cases} 1 \\ 0 \end{cases}$　$i = (n-1), (n-2), \cdots, 2, 1, 0.$

比如, 5 的二进制为 101, 其量子寄存器表示的量子状态为:

$$|\Psi\rangle = |1\rangle|0\rangle|1\rangle = |2^2 \times 1 + 2^1 \times 0 + 2^0 \times 1\rangle = |4 + 1\rangle = |5\rangle$$

对于 n 位量子寄存器, 可以存储的基态的脚标为: $N = 0, 1, 2, \cdots, (2^n - 1)$, 即有 2^n 个基态。最一般的态就是希尔伯特空间中的一个矢量, 即: $|\Psi\rangle = \sum_{N=0}^{2^{n-1}} C_N |N\rangle$, 它描述了可存储的各种可能的、不同的态的同时存在, 这是量子寄存器不同于经典寄存器的特征。

按照经典信息论, 对于一个二值系统 $(0, 1)$, 若取二值之一的概率是 1/2, 则给出这个系统的取值是 0 或 1 的信息量就是 1 比特。对于 n 个二值系统, n 位二进制数共有 2^n 个, 每个都等几率地出现, 于是指定其中一个的信息量就是 n 比特。换言之, 一个经典比特可以制备在两个逻辑态 0 或 1 中的一个态上, 而不能同时存储 0 和 1。但是, 一个量子比特可以制备在两个逻辑态 0 和 1 的相干叠加态, 即是说, 它可以同时存储 0 和 1 两个状态。可见, 量子存储器具有巨大的存储量。对于有 n 个量子比特的量子存储器, 同一时刻存储 2^n 个数的迭加态, 而在经典情况下, 同一时刻只能存储 2^n 个数中的一个。从拓扑来看, 一个经典比特的拓扑不过是两个点, 而一个量子比特的拓扑却是一个球面。在测量之前, 量子比特确实比经典比特承载了更多的信息[3]。

(2) 量子计算具有平行性　量子计算的平行性由量子算法的并行性决定的。当我们把代表几个数的相干迭加态制备在一个量子寄存器之中, 我们就可以对其进行运算。量子力学中的所有运算是幺正变换和线性变换, 因此, 可以保持态的迭加性。幺正变换还是局域变换, 即只对一定的量子位起作用。

例如, 设有一逻辑门 U 产生以下作用:

$$U|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\quad U|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

又设 3 位量子寄存器初始状态都处于 $|0\rangle$, 对每一位实行量子逻辑门 U 的演化, 于是有:

$$|\Psi\rangle = U \otimes U \otimes U |000\rangle = U|0\rangle\, U|0\rangle\, U|0\rangle$$

$$= \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

可见, 每一个量子算符操作同时变换两个量子态, 而这三个量子算符是同时作用的, 因此, 3 个量子幺正变换就是一次并行处理, 共得到 8 个量子态。n 次操作得到 2 的 n 次方个数的寄存器的态。而经典运算中, n 次操作只得到包含一个数值的寄存器的态。

因此, 量子计算机对 n 个量子存储器实行一次操作, 即同时对所存储的 2^n 个数据进行数学运算, 等效于经典计算机重复实施 2^n 次操作, 或者等效于采用 2^n 个不同的处理器进行并行操作。随着 n 的增加, 量子存储器存储数据的能力将指数上升。如果将寄存器制备为若干数的相干迭加态, 然后进行线性、幺正运算, 则计算的每一步同时对迭加态中的所有数进行, 这就是量子并行计算。正如尼尔逊与昌所说:"量子并行性是许多量子算法的一个基本特征, 简言之, 量子并行性使量子计算机可以同时计算函数 $f(x)$ 在许多不同的 x 处的值。"[4] 量子计算还具有随机性[5], 量子计算机是真正意义上的随机计

算机。而经典计算不是真正的随机性,而是伪随机性。

(3) 量子计算具有全局性　我们简要讨论 Deutsch 问题,认识量子计算的整体性。[6]设有一个黑盒,它实现把一个比特信息 x(x=0,1) 变到一比特信息 f(x) 的函数运算,即 f:x→f(x),定义域和值域都可用一个比特来荷载。我们无法知道黑盒子在干什么,但是它很复杂。函数 f 有以下 4 种可能:

$$\left.\begin{matrix} f_1(x)=x \\ f_2(x)=\bar{x} \end{matrix}\right\}\text{平衡变换型,}\quad \left.\begin{matrix} f_3(x)=0 \\ f_4(x)=1 \end{matrix}\right\}\text{常数变换型}$$

我们现在并不需要知道 f 是这 4 种可能中的哪一个,而只需要知道 f 是平衡型还是常数型即可,这就是 Deutsch 问题。

如果这个黑盒子是经典的,那么,只能运算经典比特。为此,我们需运行它两次,分别算出 f(0) 和 f(1),从而能得知 f 是平衡型还是常数型,且能够判断 f 是这 4 个函数中的哪一个。但是,我们只需要知道它是属于平衡型还是常数型。可见,我们计算函数 f 两次实际上给出了多余的信息,浪费了时间这一宝贵的资源。

如果黑盒是量子的,那么,我们只需对量子黑盒进行运算。对量子黑盒执行一个二量子比特的幺正变换,对量子黑盒采用迭加的量子态输入,只需要运行一次,就可以判断出 f 函数属于平衡型还是常数型。

量子计算机之所以能通过一次运算就给出 Deutsch 问题的答案,是因为它不仅能运算 f(0) 和 f(1),而且它能对 $|0\rangle$ 和 $|1\rangle$ 的任意叠加态进行运算,然后从中取出有关函数 f 的整体信息(既依赖于 f(0) 又依赖于 f(1) 的信息,如 f 是平衡类还是常数类)。

量子计算线路选择的并行性不同于经典计算线路选择的并行性,正如尼尔逊与昌指出,差别在于经典计算机上的"选择总是互相排斥的",而在量子计算机上"选择却可能通过相互干涉,而给出函数 f(x) 的某些全局性质"。"许多量子算法设计的本质在于,精心选择函数和最终变换,以便有效地确定有关函数的有用全局信息,而经典计算机无法快速得到"。[7]可见,量子计算具有全局性特点。

(4) 某些量子算法具有加速能力　被广泛应用的 RSA 公钥系统基于数论,其安全性建立在用经典计算机进行因数分解是困难的这一基础上,因为对 RSA 来说,逆向解密过程是一个与因数分解密切相关的问题。因数分解问题是指,一个 n 位整数 N,它等于两个素数和相乘的积,其中 N 为已知,由给定的数 N 去求这两个未知的素数因子 n_1 和 n_2。在经典计算机上进行因子分解,是依次用 2, 3, 4, …, $\sqrt{N}$ 作为除数去除 N,直至把能整除 N 的那些素数找出来。使用这种算法,计算的时间复杂度为 $O(2^{n/2})$(n 为输入量的位数),显见,这一算法具有指数时间复杂性。

1994 年,AT &T 公司的肖尔(Peter Shor)发现了肖尔算法,这个算法被称为"Shor 大数因子化"的量子算法。用肖尔量子算法进行因子分解的思想是,利用数论中的一些定理,把求数 N 的因子问题简化成求一个周期函数 f(x) 的周期 r 问题,即有 f(x)=f(x+r) 成立,然后利用傅立叶变换找出函数的周期。由于量子计算中的输入态和输出态处于量子纠缠之中,对余因子函数的输出态进行测量并得不到它的周期,但是可利用分立付里叶变换,不测量输出态,而测量输入态,以求得周期,于是就可以实现因子分解。

在经典计算机中,复杂性产生在求周期之中,求周期 r 的计算所需要的时间以 N 的位数 n 的指数函数方式增长。使用肖尔量子算法,关键采用了量子傅立叶变换(QFT)求周期 r。肖尔证明,基于 2^n 的量子傅立叶变换仅用 $n(n+1)/2$ 个量子门就可实现。求一个 n 位大数的两个质因子的 Shor 算法的时间复杂度为 $O(n^2(\lg n)(\lg\lg n))$,这是 n 的多项式。从而使肖尔的量子算法是一个多项式算法,是一个有效算法。

肖尔量子算法充分利用了量子的相位的相干性、相消性与量子计算的并行性,从而具有指数加速的特点,克服了经典计算复杂性。比如,对于十进制 60 位的数进行因子分解,如果用运算速度约为 10^{12} 次/秒的经典巨型计算机进行经典计算,需要的运算次数是 10^{30}次,耗费的时间为 10^{17}秒,这大约相当于宇宙的寿命;在采用量子算法的情况下,需要作的运算次数约为 $L^2\approx 4\times 10^4$,以同样的运算速度,只需 10^{-8}秒即可完成。肖尔算法对因子分解是有效的,如果多量子位的量子计算机能真正产生,那么破解 RSA 公钥系统将是很容易的。这说明量子计算相对经典计算的巨大优越性。这一算法的实际应用,将会使现行的计算机上使用的公共安全加密系统的安全性受到极大威胁。目前一个推广了的 Shor 算法已经在核磁共振中得到实验实现。

1997 年,格罗夫(Grover)发现了具有广泛用途的量子搜寻算法。它适用于解决如下问题:从 N 个未分类的客体中寻找出某个特定的客体。我们知道,经典算法只能是一个接一个搜寻,平均而讲,这

种算法需要寻找 N/2 次, 找到的几率为 1/2, 但是, 用 Grover 的量子搜寻算法仅需要 $\sqrt{N}$ 次。例如, 要从 100 万个电话号码中寻找出特定的号码, 经典方法平均需要找 50 万次, 其正确的几率为 1/2。如果用格罗夫的量子算法, 只需要 1000(即 $\sqrt{N}$) 次, 获得正确答案的几率为 1/2, 但若再多重复操作几次, 那么找到所需电话号码的几率接近于 1。[8]

总之, 目前已构造出来的一些量子算法已显示出超越经典计算机的强大能力。有的问题是指数加速(如肖尔算法), 而大量的问题是方根加速(如格罗夫算法), 从而可以节省大量的运算资源(如时间、记忆单元等)。但也有一些问题(如迭代问题、宇称问题等)则没有量子加速。

3 哲学意义

在我们看来, 量子算法的哲学意义表现在以下方面:

(1) 关于物理学与数学的关系　从历史来看, 数学总是走在物理学的前面, 物理学利用和依靠数学。似乎抽象的数学与经典层次的物理学没有多大的联系。量子算法与量子计算利用了量子力学的各种基本性质。比如, 量子相干性、迭加性、并行性、纠缠性、测量坍塌性等, 实现了数学与物理学的结合, 数学的经验性又在更高层次显现出来了, 数学深刻揭示了客观物质世界的本质。量子力学所提示的微观物理系统的经验性质, 促进了计算数学和计算机科学的发展, 也为解决计算复杂性提供了新的有力工具。事实上, 原来的 EPR 论证仅是作为一个佯谬, 是在量子力学的前提下从数学角度推演出来的, 而不是作为一个真正的物理过程, 但随后的一系列物理实验严格证明了 EPR 关联是微观客体的最基本的性质, 量子算法与量子计算正是以 EPR 关联——量子纠缠作为其关键运行机制。量子力学真正帮助数学去改进和突破原有的数学理论限制。因此, 建立在原有数学基础上的经典计算复杂性理论必然要作重大的调整。

(2) 量子算法与量子计算对波函数实在性的启示　量子力学中波函数(几率幅)究竟有没有物理意义, 一直存在争论。玻尔和海森堡认为, 波函数代表几率波, 几率波具有物理实在性, 它具有潜在性。目前正统的观点仍是玻恩的几率波解释, 即是说波并不像经典波那样代表什么实在的物理量的波动, 它只不过是关于粒子的各种物理量的几率分布的数学描述而已, 几率波解释只是将波的振幅的平方与各种物理量的测量值之间建立起了几率的关系。玻恩的波函数与微观实在并没有直接的联系。

如果说有关波函数的论争是在量子纠缠的客观实在性并没有得到认识之前做出的, 那么, 我们认为, 当量子纠缠确认为一种客观性关联, 并且作为量子算法和量子计算的根本性基础, 有关波函数的实在性论争应当告一段落, 波函数就是微观实在与量子信息的统一, 波函数表达的几率波的实在性质不同于经典力学的粒子和波的实在性质。如果我们不承认量子系统的波函数的实在性, 那么, 量子计算和量子算法就如同是在虚无飘渺的神话中变戏法。从量子计算与量子算法来看, 波函数(或几率幅)与算符都具有物理实在的意义, 波函数描述了微观物质(量子系统)的状态和运动(演化)性质, 微观客体的运动具有可逆性, 而算符描述了微观物质相互作用的性质, 测量仪器对量子系统的作用就等效于一个力学量算法作用在波函数上。

量子计算充分利用了微观物质的新性质。量子信息的存储与量子计算深刻表明, 微观客体既在这里, 又在那里, 这是量子并行计算的根本基础, 这充分体现了亦此亦彼的辩证逻辑。而经典信息存储与经典计算却不是这样, 却是严格的形式逻辑。量子计算所体现的辩证逻辑通过形式逻辑的运算而显现出来。

(3) 某些量子算法具有克服计算复杂性的能力　计算复杂性是由算法的复杂性决定的。计算都有一个物理的操作运行过程, 完成这一过程需要最起码的运行时间和计算空间。时间复杂性与空间复杂性的存在告诉我们, 时间和空间是计算最基本的物理限制因素, 计算时间与空间都是有限的, 且与人类活动的合理的时间与空间尺度密切相关, 如果超出这一合理时空尺度, 计算就是不现实的, 也是不可能的。比如, 计算时间高达几年或几十年, 其计算就不现实, 而且还不能保证在这计算期间是否不出现新的问题。

不仅时间与空间的现实合理尺度构成了计算复杂性, 而且丘奇-图灵(Church-Turing)论题深刻揭示了存在不可计算问题, 或者说不存在任何一种算法实现的问题。丘奇－图灵论题的表述是: 直观可计算的函数类就是图灵机以及任何与图灵机等价的计算模型可计算的函数类。不可计算问题的存在, 意味着世界本身是复杂的, 其复杂性远远超过了时间复杂性与空间复杂性, 因为时间复杂性与空间复杂性表明人类理性可能把握的, 只是其运行时间与所占空间超过了人类运行它的合理尺度, 但是, 不可计算问题从根本上否定了人类对某些问题的任何可计算性。我们认为, 目前有关计算复杂性的定义是操

作性和现象性的, 并没有揭示计算复杂性的本质。因为从经典计算理论来看, 只有多项式时间的算法可计算的, 而指数时间算法是不可能克服的。复杂程度与算法有关[9]。Shor算法与Grover算法等表明, 经典计算复杂性分类对于量子力学失去绝对性, 量子计算机有可能把NP问题转化为易解的P类问题。但目前, 仍不能肯定这种推论的正确性。

数学世界是一个具有高度自主性、客观性的世界。一个问题是否有解, 是由数学的客观性决定的。原来有的计算问题没有经典算法解, 而现在却有量子算法解, 这说明该计算问题是认识复杂性, 而不是客观复杂性。经典计算的指数复杂性, 是一个认识复杂性问题, 而不是客观复杂性。

为什么量子算法能克服经典算法所不能克服的某些复杂性呢? 我们认为, 关键在于量子计算机是一个复杂系统, 量子计算所具有的复杂程度不低于求解问题的复杂程度, 即以复杂性克服复杂性。当然, 如果量子计算的复杂程度低于问题的复杂程度, 那么, 量子计算也无法求解问题。

从定性来看, 经典算法具有有限性和离散性, 经典计算机的计算是逐次计算和部分性计算, 而计算问题具有无限性和整体性, 因此, 必然存在经典计算机无法完成的计算问题。而量子计算机是一个复杂系统, 其计算具有并行性与整体性或全局性, 量子计算机可能克服经典计算的复杂性。

量子计算是一个复杂系统, 其原因在于: 第一, 量子计算的物理基础是量子系统, 量子系统具有不确定性。诺贝尔物理学奖获得者盖尔曼曾指出: "许多人熟知海森堡不确定性原理, 该原理否定了同时准确地测量粒子间的位置和动量的可能性。……而量子力学所要求的附加不确定性却很少被人们提起。" "由于不能进行完全准确的测量, 因而, 混沌行为不但导致了量子力学原理中的不确定性, 而且引起了经典层次的明显的不确定性。"[10]量子算法往往要利用量子态之间的量子纠缠这一重要性质, 处于量子纠缠的单个量子态不具有可分离性, 或者其量子态是不确定的。

第二, 量子计算机需要有大量的量子存储器(如寄存器等)来存储信息, 而存储量子信息的量子态具有不确定性。

第三, 量子计算具有非线性特点。量子计算输出的是经典结果, 它是几率性的东西, 是波函数绝对值的平方后的东西, 因此计算机的结果是非线性的, 或者说, 量子计算机的经典输出与量子输入之间是非线性关系。

每一个算符是线性的, 多个算符同时作用就会产生非线性。当多个算符同时作用在几个量子比特上, 必然产生非线性。比如, n个量子逻辑门作用在n个量子比特的量子寄存器上, 就会产生包括2^n个值的寄存器的态, 这就是量子系统的非线性特征。量子计算机可以处于量子迭加态, 在一个硬件上同时进行不同路径的量子并行计算。

第四, 从量子系统的要素来看, 量子系统的要素具有复杂性, 因为量子系统没有办法确定其要素, 波函数仅仅是给出了量子系统的状态, 是一个状态函数, 没有更多的信息。或者说, 如果把一个可能的量子态看作为量子系统的一个要素, 那么, 经过多个算符的作用之后, 量子系统的要素将会指数增加。

参考文献

〔1〕顾小丰, 孙世新, 卢光辉. 计算复杂性[M]. 北京: 机械工业出版社, 2005. 13.

〔2〕李承祖等编著. 量子通信和量子计算[M]. 长沙: 国防科技大学出版社, 2000. 148.

〔3〕龙桂鲁, 肖丽. 核磁共振量子计算机与平行量子计算[A]. 载曾谨言等主编. 量子力学新进展(第三辑)[C]. 北京: 清华大学出版社, 2003. 114.

〔4〕〔7〕M Nielson, I Chuang. 量子计算和量子信息(一)[M]. 赵千川译. 北京: 清华大学出版社, 2004. 29, 32.

〔5〕J Rarity, P Tapster. Quantum Rantum-number Generation and Key Sharing. [J] **Mod. Opt.** 1994. (41): 2435—2444.

〔6〕吴盛俊, 周锦东, 张永德. 量子算法简介[J]. 大学物理, 1999(12): 1—5.

〔8〕D. Bouwmeester, A Ekert and A Zeilinger. **The Physics of Quantum Information**[M]. Berlin: Springer-Verlag, 2000, 413.

〔9〕赵瑞清, 孙宗智. 计算复杂性概论[M]. 北京: 气象出版社, 1989. 引言, 2.

〔10〕盖尔曼. 夸克与美洲豹[M]. 长沙: 湖南科学技术出版社, 1999. 27.

Quantum Complexity, Quantum Computation And Its Philosophical Implications

WU Guo-lin, HUANG Ling-yu

(School of Politics and Public Management, South China University of Technology, Guangzhou 510640, China)

Abstract: Quantum computers have much more capacity than classical ones. Quantum computations are of parallelism and wholeness. Some quantum arithmetic can be of acceleration. Quantum computations bring us new philosophical implications such as the relationship between mathematics and physics, the reality of wave—function, and capacity of solving computation complexity.

Key words: quantum computation; quantum arithmetic; computation complexity

(本文责任编辑 费多益)