量子计算及量子算法研究进展①

王　蕴，黄德才，俞攸红

(浙江工业大学 计算机学院，杭州 310023)

摘　要：量子相干性和量子纠缠等特性为量子计算带来了完全不同于经典计算的独特运算方式，量子计算表现出的并行性更是令经典运算望尘莫及。Shor 算法的提出完全展示了量子算法在解决某些经典问题时的优势，接踵而至的 Grover 搜索算法进一步诠释了量子计算的威力。此后，算法“量子化”在国际上掀起了研究的热潮，尤其在量子智能算法方面取得了不错的成果。文章首先介绍量子计算的发展现状和基本原理；然后列举三种典型的量子算法，展示量子计算的优越性；最后介绍该领域的研究进展。

关键词：量子算法；优化算法；量子计算；量子位；shor 算法

Current Research in Quantum Computation and Algorithm

WANG Yun, HUANG De-Cai, YU You-Hong

(College of Computer Science, Zhejiang University of Technology, Hangzhou 310023, China)

Abstract: According to quantum mechanics, quantum state has many advantages of the coherence and entanglement and the inner parallelism of quantum algorithm is totally different from the classical algorithm. Shor’s algorithm shows the advantage of quantum algorithm in solving some classical Non-polynomial problems, then Grover’s search algorithm further proves this point. And this brought more and more research on quantum algorithm in many countries and they have got great achievements especially on quantum intelligent algorithm. In this paper, the development and fundamental principles of quantum computing are generalized, then three typical quantum algorithms is introduced, and the superiority of quantum computer is explained. Finally, current research of quantum computation are introduced.

Keywords: quantum algorithm; optimization algorithm; quantum computing; qubit; shor’s algorithm

1　引言

随着社会的进步和经济的发展，人类在信息量处理速度方面的需求越来越高。自世界上第一台计算机问世以来，信息量的处理已经由最初的每秒千次运算发展到现在的每秒亿次级运算，然而，计算机性能的提升速度仍然满足不了人类社会在信息处理速度方面的需求。十九世纪初提出并建立的量子力学理论为计算机的革命性发展带来了新的曙光，量子独有的相干性和纠缠性等特性为量子计算带来了完全不同于经典计算的独特运算方式。经过近一个世纪的发展，世界上首台通用编程量子计算机于 2009 年面世[1]。这一量子计算机由美国国家标准技术研究院研制，可处理两个量子比特的数据，并可以在进一步改进后应用于密码破译等方面，相关的论文发表在《自然.物理学(Nature Physics)》上。与此同时发展起来的还有量子计算科学、量子信息科学以及量子控制理论等以量子力学理论为基础的相关学科。

2　量子计算

量子计算是由美国物理学家费曼（R.P.Feynman）生前认真研究量子力学理论之后，于 1982 年提出的，并由此构建了实现量子计算的机器——量子计算机。然而，由于量子态的测不准原则以及量子系统容易受噪声干扰，导致量子运算很容易出错，因此，量子计

① 基金项目:国家自然科学基金(10774131)

收稿时间:2010-09-14;收到修改稿时间:2010-11-19

算理论始终停留在“原则上可行”状态。直到 1994 年，美国计算机专家 Shor 证明了量子计算机能快速分解大因数，并完成了第一套量子算法编码，量子计算以及量子计算机的研究才进入实验时代。

2.1 量子位

与经典计算中使用比特（bit）作为信息的基本存储单元不同，量子计算中信息的基本单位是量子位或量子比特（qubit）。经典比特具有 0 和 1 两种状态，并利用 0 和 1 构成的比特串进行编码来表征不同的信息。为达到量子计算的目的，通常量子比特用两个量子态|0>和|1>表示（其中“| >”是量子力学中用来表示量子状态的符号，称为 Dirac 记号），然后用|0>和|1>构成的量子比特进行编码。根据量子力学原理，量子比特与经典比特的不同之处在于：一个量子比特除了可以像经典比特一样处于|0>和|1>这样的状态之外，还可以处于既非|0>又非|1>的状态上，即它可以处于由这两个态所组成的线性组合这样的中间状态上。这个中间状态称为叠加态（Superposition），一般用如下式子表示：

$$|\psi>=\alpha|0>+\beta|1> \tag{1}$$

其中 α 和 β 均为复数且满足条件 $|\alpha|^2+|\beta|^2=1$。也就是说，当有两个量子比特时，它们可以处于的量子态就是 00,01,10,11 这四个状态的叠加态，即 $|\psi_2>=a|00>+b|01>+c|10>+d|11>$，其中 a,b,c,d 满足$|a|^2+|b|^2+|c|^2+|d|^2=1$。当 a,b,c,d 中有三项为 0 时，量子比特又退化成与经典比特对应的状态。

量子叠加态是决定量子计算不同于经典计算的关键特性之一，也是量子并行计算的理论基础。以两比特可以表示的信息量为例，经典计算中可以用 00,01,10,11 分别表示四种不同的信息。传统存储器每次只能记录这四个状态中的一个，但量子存储器却可以在同一时刻以量子叠加态的形式存储这四个不同的状态，这就意味着对于相同位数的寄存器，量子计算机可以记录的信息量是传统计算机的指数倍。换句话说，对于一个 n 量子位的寄存器，它可以同时存储 2n 个不同的数字，并且这 2^n 个不同数字是用同一个量子态表示的，这个量子态的一般形式为：

$$|\psi>=\sum_{x=0}^{2^n-1}c^n|x> \tag{2}$$

如果对式（2）进行一次计算，相当于对 2^n 个数字同时进行计算，这种计算效果就是所谓的量子并行计算。量子并行计算体现了量子计算最重要的优越性，它的运算速度和信息处理能力是经典计算机所无法比拟的。

2.2 量子逻辑门

与经典逻辑运算不同，在量子世界里，信息的基本操作元件是量子逻辑门（简称量子门），量子逻辑门由幺正矩阵或者幺正矩阵的组合构成，通过对量子态实施幺正操控实现对信息的逻辑变换。因此，量子信息的处理过程也就是对经过编码的量子态进行幺正变换或者说操控的过程[2]。量子逻辑门按照输入比特的个数不同可以分为单比特、两比特以及三比特逻辑门等。例如，若一个幺正操作 P(θ)作用在量子态|0>和|1>上后，结果为：

$$\begin{cases}|0>\xrightarrow{P(\theta)}|0>\\ |1>\xrightarrow{P(\theta)}e^{i\theta}|1>\end{cases} \tag{3}$$

那么这个幺正操作就是一个单比特逻辑门，简称单比特门。记$|0>=\begin{bmatrix}1\\0\end{bmatrix}$，$|1>=\begin{bmatrix}0\\1\end{bmatrix}$，则单比特门 P(θ)可以用幺正矩阵 $P(\theta)=\begin{bmatrix}1&0\\0&e^{i\theta}\end{bmatrix}$ 表示。常用的单比特量子门有 Hadamard 门、Pauli-X 门、Pauli-Y 门、Pauli-Z 门等，其矩阵表示如表 1 所示[3]。

表 1 单比特量子逻辑门及其线路记号表示

名称	说明	名称	说明
Hadamard	$\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}$	Pauli-X	$\begin{bmatrix}0&1\\1&0\end{bmatrix}$
Pauli-Y	$\begin{bmatrix}0&-i\\i&0\end{bmatrix}$	Pauli-Z	$\begin{bmatrix}1&0\\0&-1\end{bmatrix}$
Phase	$\begin{bmatrix}1&0\\0&-1\end{bmatrix}$	$\pi/8$	$\begin{bmatrix}1&0\\0&e^{i\pi/4}\end{bmatrix}$

所谓量子计算，可以简单的理解为在量子计算机上利用量子态的物理特性进行信息处理的方法。量子并行性是量子计算区别于经典计算的主要特征。它是一种与经典计算截然不同的新型计算，在运算速度和信息处理能力方面均表现出了极大的优越性，具有经典计算不可比拟的并行性，量子计算的成功运用将使计算技术进入一种前所未有的新境界。

3 量子算法

量子算法作为量子计算科学的重要部分，在过

去的十几年中得到了广泛的发展并取得了一系列惊人的成就。1989 年，Deutsch 首次提出了 Deutsch 量子算法[4]，用于解决 n 比特 Deutsch 问题。该算法的提出第一次很好的展示了量子计算机的并行性，而且也为量子计算的研究工作带来了某种启示：量子计算机在解决某些问题的时候其效率确实有可能远远超过经典计算机。1994 年，Shor 提出大数质因子分解量子算法[5,6]并实现了该算法的量子编码。大数质因子分解问题在传统计算机上至今仍然是 NP 难题，Shor 算法证明了该问题利用量子计算机可以在多项式时间内完成，量子计算的威力由此可见一斑。此后，Grover 算法、量子智能算法等量子算法相继被提出，量子算法的研究工作也得到了各国研究者的关注。

3.1 Shor 大数质因子分解算法

Shor 于 1994 年提出的大数质因子分解量子算法吸引了众多研究者的目光。这是因为，大数质因子分解的难度确保了 RSA 公钥密码体系的安全，该问题至今仍属于 NP 难题，在经典计算机上需要指数时间才能完成。但是 Shor 算法表明，在量子计算条件下，这一问题就可以在多项式时间内得到解决。这就意味着目前广泛应用于政府、军事以及金融机构等重要方面的 RSA 公钥密码体系的安全性可能面临着致命的威胁，仅这一点就足以引起人们对量子算法研究的极大关注。

Shor 算法的基本思想是：首先利用量子并行性特点通过一步计算获得所有的函数值，并利用测量函数得到相关联的函数自变量的叠加态，然后对其进行快速傅里叶变换（QFFT）[7]。其实质为：利用数论相关知识将大数质因子分解问题转化为利用量子快速傅里叶变换求函数的周期问题[8]。其数学描述如下：为寻求某一大数 N 的两个素数因子 p、q，首先随机选择一个与 N 互质的自然数 a（a<N），并构造如下函数：

$$f(x)=a^x(\mathrm{mod}\,N) \qquad (4)$$

上式称为 x 的以 N 为模的同余式，即表示 N 整除 f(x) 和 ax 的余数相等。显然，式（4）是周期函数，通过 QFFT 可在多项式时间内求得函数的周期。然后利用数论相关知识很快得到 N 的一个因子。

Shor 算法证明了大数质因子分解问题可以在多项式时间内解决，量子算法在解决一些经典算法无法解决的问题时确实显示出了极大的优越性。另外，Shor 算法在量子计算机上的实现一直是一个国际难题。2007 年 12 月，中国科技大学潘建伟小组在国际上“首次利用光子比特、也是首次用真正的纯态量子系统”[9]实验演示了 Shor 算法，并验证了量子加速的根本原因。该项研究成果发表在物理学国际权威期刊《物理评论快报(Physical Review Letters)》上。

Shor 算法本身已经相当成熟，对其改进和优化的空间不大。目前的改进工作主要是通过对同余式函数（式 4）中与 N 互质的自然数选择的限制[10]，使得算法成功的概率提高。Shor 算法是目前为止已经提出的最好的量子算法，该算法不但具有传统算法无法比拟的优势，而且其巧妙的理论构思以及表现出的实际应用价值，都是十分宝贵的。Shor 算法及其模拟实现，对量子通信和量子密码学的发展都具有极其重要的参考价值。

3.2 Grover 数据库搜索算法

对于无序数据库，搜索的规模随着数据库规模的增长而成线性增长。这一问题在经典算法中需要 O(N) 时间才能完成整个搜索过程。1996 年 Grover 提出量子搜索算法[11]，将搜索问题完成的时间缩小到步，对经典问题起到了二次加速的作用。

Grover 算法适宜于解决在无序数据库中搜索某一个特定数据的问题。在经典计算中，对待这类问题只能一个一个的搜索数据库中的数据，直到找到为止，通常需要 N/2 次查询才能以 1/2 的概率找到需要的那一个数据。而 Grover 算法利用量子并行性，每一次查询可以同时检查所有的数据，并使用黑箱（Oracle）技术对目标数据进行标识，这样重复次后，就可以以 1/2 概率找到。再多重复操作几次，就可以以接近于 1 的概率找到那个特定数据。该算法并没有像 Shor 算法一样实现问题的指数加速，然而搜索算法的广泛应用性却很好的弥补了这一点。现实中有许多问题，如最短路径问题、图的着色问题、排序问题及密码的穷举攻击问题等，都可以利用 Grover 算法进行求解。事实上，目前 Grover 算法已经在核磁共振和光学系统中得到实现。另外，由于在求解过程中，Grover 算法的实现简单而且没有使用问题的特殊结构信息，因此它实际上为这类问题的解决提供了一种框架，属于通用算法[12,13]。

Grover 算法是目前最经典的量子算法之一，然而它也存在着某些缺陷。比如：当要搜索的目标数目超过数据库中记录总数的 1/4 时，Grover 算法搜索成功

的概率迅速下降；当目标数目超过数据库记录的一半时，算法几乎失效[14]。针对这一问题，各国学者进行了大量的研究改进工作，并且取得了很多不错的研究成果。对 Grover 算法的改进研究也成为了目前量子算法方面的一个热门研究领域。

3.3 量子智能算法

自 Shor 算法和 Grover 算法提出以后，量子计算方法表现出的独特计算方式以及在信息处理方面展现的巨大潜力引起了研究者的广泛关注。而智能算法向来是算法研究领域的一个热点，量子智能计算将量子理论原理与智能计算相结合，利用量子并行计算特性很好的弥补了智能算法中的某些不足之处，如：加快算法的收敛速度及避免早熟现象等。

目前已有的量子智能算法研究包括：量子进化算法、量子免疫计算、量子退火计算、量子神经网络和量子聚类算法等。其中，量子进化算法和量子神经网络成为目前学术研究的热点并取得了相当不错的成绩。

量子进化算法[15]建立在量子态矢量的基础上，是一种新的基于量子理论的进化算法。该算法采用量子位编码来表示染色体，使得传统表示方法下很大数量的个体仅需一个小种群的量子个体就可以表示。另外采用量子门实现染色体的更新操作，提高了计算的并行性和全局搜索能力。这些特点使得量子进化算法具有种群规模小、全局寻优能力强和计算时间短等特点。然而，量子进化算法的研究领域还主要集中于单目标、确定性的函数优化问题或者特殊类型的组合优化问题，在多目标、不确定优化领域的研究还不够[16]。另外，目前量子进化算法的应用研究领域也很有限，量子进化算法的研究还不够成熟，很多理论和应用的研究还需要深化和推广，进一步研究的空间还很大。

量子神经网络是将量子理论与神经网络相结合的一种尝试。越来越多研究人员发现，量子理论在大脑神经系统中可能扮演着一种至关重要的角色，将神经网络和量子理论相结合会更好的模拟人脑的信息处理过程。目前的研究工作主要集中在一下三个方面[14]：(1)通过传统神经网络模型来研究量子计算中的问题；(2)充分利用量子计算超高速、超并行、指数级存储容量的特点，来改进传统神经网络的结构和性能；(3)通过引入量子理论中的概念和思想，构造新的神经网络模型和算法。

经过十几年的发展，量子神经网络的研究取得了一系列成果，与传统神经网络相比，量子神经网络在结构和学习方面存在着不同并具有如下优势：（1）信息的高速处理；（2）记忆容量和回忆速度的指数级增长；（3）快速学习和一次学习的能力；（4）消除灾变性失忆等。由此可见，充分考虑量子理论在神经网络中的应用必将为人工神经网络的发展提供新思路和途径。

4 结语

量子计算和量子算法理论的基本框架已经成型，各方面研究也均取得了日新月异的进步，但最终要实现具有一定实用价值的量子计算，还存在着许多需要解决的问题。其中作为量子计算物理上支持的量子计算机系统的构造就是目前亟待解决的问题之一。不过最新一期的美国《科学》杂志刊登了英国研究小组在量子计算机研究领域的新进展，文章声称这一进展可能使量子计算机面世的时间提前到 10 年以内。我们有理由相信，随着更多的专家和学者加入该研究领域，量子计算的研究一定会得到突飞猛进的发展，人类将进入一个神奇而高效的量子计算时代。

参考文献

1 Hanneke D, Home JP, Jost JD, Amini JM, Leibfrid D, Wineland DJ. Realization of a programmable two-qubit quantum processor. Nature Physics, 2010,(6):13–16.

2 Steane A. Quantum computing. Rep. Prog. Phys.,1998.

3 Ekert A, Hayden P, Inamori H. Basic concepts in quantum computation. Coherent Atomic Matter Waves, 2001, 72: 661–701.

4 Deutsch D. Quantum computational networks. Mathematical and Physical Sciences. London: Proc. the Royal Society of London, 1989, A425:73–90.

5 Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. Proc. 35thAnnual Symposium on Foundations of Computer Science. Los Alamitos: IEEE Computer Society Press, 1994,11:124–134.

6 Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comp., 1997, 26:1484-1509.

7 苏晓琴,郭光灿.量子通信与量子计算.量子电子学报, 2004,

(下转第 237 页)

但由于用户少，维护一个云数据中心也是一个挑战。

这些只是我国云存储发展处于起步阶段面临的问题，随着更多的厂商的加入及用户的使用此问题便会迎刃而解。

5 结语

云计算是互联网发展的必然产物，它的出现也为互联网带来了更丰富的应用。云数据存储技术及数据管理技术是云计算中的核心领域，主要解决了在“云”这个大环境中的数据存储及管理模式。本文主要讨论了云存储的概念、优势及架构，分析了 GFS、HDFS 数据存储技术以及 BigTable、HBase 数据管理系统。虽然目前云存储处于起步阶段，也面临很多困难，但随着更多企业及学术界对云存储的研究，云存储技术会给我们的生活带来更多的便捷，云存储技术也会更加地成熟。

参考文献

1 Ghemawat S, Gobioff H, Leung ST. The Google file system. Michael L. Scott, ed. Proc. of the 19th ACM Symposium on Operating Systems Principles. New York: ACM Press, 2003: 29–43.

2 Chang F, Dean J, et al. Bigtable:A Distributed Storage System for Structured Data. ACM Trans. on Computer Systems, 2008,26(2):1–26.

3 中国云计算网.什么是云存储. (2008-11-17)[2010-08-25]. http://www.cloudcomputing-china.cn/Article/luilan/200811/215.html

4 Borthakur D. The Hadoop Distributed File System: Architecture and Design. (2008-09-02) [2010-08-25].http://hadoop.apache.org/common/docs/r0.16.0/hdfs_design.html

5 Hbase Development Team.HBase: Bigtable-like structured storage for Hadoop HDFS.(2010-08-10)[2010-08-25]. http://wiki.apache.org/hadoop/Hbase.

6 分布式基础学习.(2009-2-22)[2010-8-25]. http://www.cnblogs.com/duguguiyu/archive/2009/02/22/1396034.html.

7 White T. Hadoop:The Definitive Guide. California: O’Reilly Media,Inc. 2009:12–14.

8 Caibinbupt. Hadoop 源代码分析(重读 GFS 的文章). (2009-01-29)[2010-8-25].http://caibinbupt.javaeye.com/blog/318949.

9 Burrows M. The chubby lock service for looselycoupled distributed systems. Brian Bershad,ed. Proc. of the 7th USENIX Symposium on Operating Systems Design and Implementation. New York: ACM Press, 2006:30–40.

10 吴吉义,傅建庆,张明西,等.云数据管理研究综述.电信科学,2010,26(5):34–41.

11 李煜民,章才能,谢杰.云计算环境下的数据存储.电脑知识与技术,2010,6(5):1032–1034.

(上接第 231 页)

21(6):706–718.

8 Li CF Guo GC. Progress in quantum information research. Progress in Physics, 2000,20(4): 407–431 (in Chinese).

9 首次在国际上实现量子分解算法.中国科学院院刊,2008,23(1):76–76.

10 彭卫丰,孙力.SHOR 量子算法的优化及应用研究.计算机应用与软件,2009,26(5):239–246.

11 Grover Lov K. A fast quantum mechanical algorithm for database search. Proc. of the 28th Annual ACM Symposium on the Theory of Computing, 1996.

12 Grover LK. A Framework for Fast Quantum Mechanical Algorithms. Proc. of the 30th Annual ACM Symposium on Theory of Computing, 1998.

13 孙吉贵,何雨果.量子搜索算法.软件学报,2003,14(3):334–344.

14 李士勇,李盼池.量子计算与量子优化算法.哈尔滨:哈尔滨工业大学出版社,2009.

15 Han KH, Kim J H. Quantum-inspired evolutionary algorithm for a class of combinatorial optimization. IEEE Trans on Evolutionary Computation, 2002,6(6): 580–593.

16 王凌.量子进化算法研究进展.控制与决策,2008,23(12): 1322–1326.