# 量子算法与量子衍生算法

张 毅[1),2)] 卢 凯[1),2)] 高颖慧[3)]

[1)](国防科技大学并行与分布式国家重点实验室 长沙 410073)

[2)](国防科学技术大学计算机学院 长沙 410073)

[3)](国防科学技术大学电子科学与工程学院 长沙 410073)

**摘 要** 随着经典计算发展日趋缓慢,量子计算正逐渐成为研究领域的关注热点.该文简要介绍了量子计算的基本原理.接着,从当前量子计算领域中的两个活跃研究方向——量子算法和量子衍生技术研究出发对整个量子算法领域主要发展脉络进行梳理并总结目前量子计算研究的发展规律.最后,该文针对这两个方向提出了若干量子计算领域的发展趋势.通过对量子计算研究领域的综述和展望,对后续量子计算研究发展具有一定的指导意义.

**关键词** 量子算法;量子衍生技术;量子计算

**中图法分类号** TP301 **DOI号** 10.3724/SP.J.1016.2013.01835

# Quantum Algorithms and Quantum-Inspired Algorithms

ZHANG Yi[1),2)] LU Kai[1),2)] GAO Ying-Hui[3)]

[1)](*National Laboratory for Parallel and Distributed Processing, National University of Defense Technology, Changsha* 410073)

[2)](*College of Computer, National University of Defense Technology, Changsha* 410073)

[3)](*College of Electronic Science and Engineering, National University of Defense Technology, Changsha* 410073)

**Abstract** With the decreasing development of the classical computation, quantum computation becomes the increasing hot topic recently. In this paper, the fundamental theory of quantum computation is briefly introduced firstly. Then, we give the state of the art of quantum computation and research principles in this field from two different research directions (quantum algorithms and quantum-inspired algorithms). At last, some trends of quantum computation in the future research are given. Through the review and prospect of the whole field, this paper could give a significant guide for the future development of quantum computation.

**Keywords** quantum algorithm; quantum-inspired algorithm; quantum computation

## 1 引 言

20世纪微电子技术的迅速发展,大大提高了电子计算机的集成度,计算性能、存储能力、通信速度的飞速提升,为现代社会的信息化发展打下了重要的物质基础.但是随着技术的发展,经典的基于电子传输的微电子技术发展已经遇到瓶颈,晶体管的集成密度和传输线宽已经发展到了极致,传统集成电路制作工艺的极限迫使经典计算的计算速度不可能一直按照"摩尔定律"[1]持续发展,经典计算已逐渐进入了发展的困境[2].

量子计算作为一种新型的计算理论模型,正逐渐成为信息研究领域关注的焦点.利用量子机制进

收稿日期:2012-07-30;最终修改稿收到日期:2012-11-20.本课题得到国家"八六三"高技术研究发展计划天河新一代高性能计算机系统研制项目(2012AA01A301、2012AA010901)、国家自然科学基金(61103082、61003075)、国防科技大学优秀研究生创新项目(B120601)以及湖南省优秀研究生创新项目(CX2012A002)资助.**张 毅**,男,1987年生,博士研究生,主要研究方向为量子计算、图像处理.E-mail:zhangyinudt@nudt.edu.cn.**卢 凯**,男,1973年生,博士,教授,中国计算机学会(CCF)会员,主要研究领域为高性能并行计算.**高颖慧**,女,博士,副教授,主要研究方向为量子计算、图像处理.

行信息处理已成为突破经典计算极限的一条重要的探索途径.

简单地说,量子计算机就是利用微观粒子状态来进行存储和处理信息的计算工具[3].其基本原理就是通过物理手段制备可供操控的量子态,并利用量子态的叠加性和相干性等量子力学相关特性进行信息的运算、保存和处理操作.

如何利用现有的物理手段制备出稳定实用的量子态一直是量子计算研究领域的难题,因此至今仍未有实用的量子计算机出现.虽然目前人们已尝试利用核磁共振[4]、离子阱[5]、量子点[6]以及光量子[7]等物理操控手段来制备和控制量子态,但均尚未成熟.然而有关量子计算理论的研究却一直蓬勃发展,目前主要有两个比较活跃的发展方向:(1)量子算法[8]——它是指运行在量子计算机上,利用量子力学原理解决实际问题的计算方法.虽然目前量子计算机的研制滞后,但如何利用这种未来的新型计算工具解决实际问题的理论研究却备受关注.目前已有若干量子算法的研究成功地取得了相对经典算法在计算性能等方面的重大理论突破.(2)量子衍生技术[9]——它是利用量子计算原理对经典信息处理算法进行量子化改进,运行在经典计算机上的计算方法.由于引入量子计算的优良性能够带来信息处理能力的显著提高,量子衍生技术也成为量子计算研究中的一个活跃方向.

本文将首先介绍量子计算基本原理并着重从量子算法和量子衍生技术两个方向综述发展现状.通过对其进行系统的分类和梳理,总结发展规律,进而展望量子计算研究的发展趋势和发展方向.本文的综述工作对量子计算领域的后续发展研究具有指导意义.

## 2 量子计算基本原理

经典计算机是通过硅芯片上微型晶体管电位的高低来表达二进制信息,从而进行信息数据的处理和储存.每个时刻每个电位只能处理和保存一个数据,非 0 即 1.多个电位共同作用,才能完成一次复杂的运算过程.

而根据量子论原理[3],单个量子能够在同一时刻处于多个(一般以两个为例)正交态的叠加,例如氢原子中电子的基态和第一激发态,圆偏振光的左旋和右旋等.通常一位量子信息可表示为式(1)的形式,其中$|0\rangle$和$|1\rangle$分别表示两个相互正交的标准状态.当对该量子比特进行测量时,量子状态将会以$|a|^2$的概率坍缩到$|0\rangle$态,以$|b|^2$的概率坍缩到$|1\rangle$态.

$$|\varphi\rangle=a|0\rangle+b|1\rangle\ (a,b\in\mathbb{C},\ |a|^2+|b|^2=1) \tag{1}$$

量子态保存在量子寄存器中,与经典计算不同的是,量子寄存器可同时保存多个正交态的叠加.一般来说,$n$ 位量子寄存器可以同时保存和处理 $2^n$ 个 $n$ 位正交态,这样利用正交态来表征信息,就可以实现多个信息的同时存储和处理.量子计算的另一重要特性是量子寄存器内的量子比特可以相互纠缠[10].量子纠缠是指两个或多个量子系统之间具有非经典的强关联作用,对其中某个子系统的局域操作会影响到整体状态,影响主要体现在对其余子系统的测量结果会发生变化.

由量子态的相干叠加原理知,针对量子态中所有叠加分量的变换能在同一时刻一次性完成,并按一定的概率幅叠加起来得到结果,因此量子计算可以实现非线性的高度并行计算.相比于目前传统的多线程[11]、GPU(Graphics Processing Units)[12]等经典并行计算方式,量子计算所提供的才是一种真正意义上的更为强大的并行计算能力.

## 3 量子计算研究现状

量子计算利用量子力学原理进行信息处理,是利用量子并行计算能力的重要技术.本节将主要从量子算法和量子衍生技术两个方向讨论量子计算理论的研究现状并总结目前该领域的一些发展规律.

### 3.1 量子计算理论发展脉络

早在 20 世纪初,量子力学就已经成为物理研究领域的重点.直到 1982 年,Feynman[13]提出利用量子计算模拟量子力学过程的思想.在 1985 年,Deutsch[14]首次提出了量子图灵机的概念,主要是希望利用量子力学的特性来进行信息处理以获得计算性能的提升.这个阶段可以看作是量子计算理论研究的起源阶段,人们主要关注于构建量子物理特性与信息计算之间的联系.从量子力学基本原理出发,量子计算理论研究有两个不同的发展方向:量子算法和量子衍生技术.

#### 3.1.1 量子算法

为了验证 Feynman 设想的重要意义,研究者相继提出了量子 Fourier 变换[15]、量子黑盒加速[16]以及量子随机漫步[17]等基本量子工具,证明了将量子

机制用于信号处理以及科学计算等工作时能够取得相对于经典计算更为高效的性能优势(比如量子 Fourier 变换的计算复杂度相比于经典 Fourier 变换有指数级的降低).这个阶段虽然已取得了惊人的研究成果,但开发的量子工具比较初级,无法用来解决实际问题,故量子计算并未引人瞩目.

1994 年,AT&T 公司的 Shor 基于量子 Fourier 变换提出了大数质因子分解算法[18].该量子算法可以在多项式时间内破解 RSA(R. Rivest, A. Shamiv, L. Adleman)保密体制,这使得依赖该密钥机制的电子银行、网络等在理论上已不再安全.1996 年,贝尔实验室的 Grover 基于量子黑盒加速工具提出了针对乱序数据库的量子搜索算法可破译 DES 密码体系[19].算法针对一个具有 $N$ 个记录的数据库,将记录均匀相干地叠加在量子态中,通过 $\sqrt{N}$ 步基本的幺正变换可以把其中某一个表征搜索结果记录的基矢概率幅逐渐放大为 1,从而使得在针对结果状态进行测量时将以很大的概率测得所要搜索的结果的数据索引.因此算法取得了相比于经典搜索二次方的加速比.这两个算法的提出震惊了整个信息领域,使人们认识到了量子计算巨大的优越性,促使了更多的研究者开始关注量子算法的研究.这两个具有里程碑意义的算法也成为目前整个量子算法研究领域的核心.随后,基于量子随机漫步方法又提出的对集合中的两个复杂元素甄别的量子算法[20],其与 Shor 算法、Grover 算法都利用已有的量子工具提出了应用于实际问题的算法,具有重大意义.

近十年来,虽然关注量子算法设计的研究者越来越多,但几乎没有再出现新颖的量子工具,这也直接导致了具有核心作用的量子算法的匮乏.目前的量子算法的研究主要围绕着现有的几种核心量子算法展开深入的讨论.比如针对 Grover 算法在特定情况下的失效问题进行改进的研究[21-22]以及改进 Grover 算法以完成更复杂的数据查询统计工作[23-25]等.另外基于 Grover 算法延拓的应用层量子算法也大量涌现,目前已有 Graph 搜索算法[26]、计算几何算法[27]和动态规划算法[28]等都基于 Grover 算法提出了相应的量子算法以及利用量子 Fourier 变换等进行量子图像处理的研究[29-30],与对应的经典算法相比,在计算性能方面取得了理论上的重大提升.此外利用量子随机漫步进行图形同构性判定也是近年来的一个重要研究方向.利用量子元素甄别算法的思想判断两幅图形是否同构可以在多项式时间内完成这个经典计算中著名的 NP(Non-deterministic Polynomial)难题[31-32].

从近十年的量子算法创新来看,如何利用未来的量子计算机解决实际问题以得到经典计算机无法达到的良好性能已成为目前量子算法发展的主要方向.

3.1.2　量子衍生技术

量子计算的另一重要发展方向是量子衍生技术[33],它指的是以量子信息学原理对经典信息处理技术进行改进,所得到的在现有电子计算机硬件系统上实现的带有量子信息学特性的高性能信息处理技术,其高性能主要体现在良好的非线性处理能力上.

1995 年,Kak[34]提出量子神经计算的概念,从此开始了量子衍生技术的研究.此后,量子衍生技术主要与人工智能、信号处理以及图像处理等具体学科相结合发展.

将量子信息学引入人工智能技术,相继出现了量子衍生神经网络、量子衍生遗传算法以及量子衍生群智能技术等研究.Menneer 等人[35]将量子信息学中的多体观点应用到单层人工神经网络,提出了量子衍生神经网络,并证明了其在处理分类问题的有效性.Kouda 等人[36]将量子位引进神经元定义,提出了量子位神经网络,仿真实验表明该神经网络具有更好的学习能力.1996 年,Narayanan 等人[37]将量子叠加态原理引进遗传算法,提出了量子衍生遗传算法.2000 年,Han 等人[38]采用量子比特编码染色体,以量子门对染色体进行更新,提出了具有更强并行搜索能力的量子遗传算法.Sun 等人[39]针对粒子群优化算法的参数多、易收敛于局部极值等问题,于 2004 年提出了量子粒子群优化算法 QPSO(Quantum-behaved Particle Swarm Optimization).Shuai 等人[40]将量子纠缠机理和 Von Neumann 熵理论引进群智能技术中,定义了一个性能优良的可用于高维大数据集聚类的群智能实现模式——通用量子粒子模型 GQPM(General Quantum Particle Model).近年来,量子衍生人工智能技术越来越受关注,研究成果层出不穷,其实用价值也在实践中得到了充分验证.

将量子信息学与具体领域相结合,就出现了相应领域的量子衍生技术研究.Eldar 等人[41]将量子态叠加原理和坍缩测量机制引进信号处理基本流程中,设计了一种量子衍生信号处理算法生成机制,并成功开发了一些实用的量子衍生信号处理技术.Xie

等人[42]将数学形态学中的腐蚀、膨胀、开和闭算子利用量子机制进行表示，从而开发了量子衍生形态学理论，为自适应滤波等应用提供新的手段. Tseng 等人[43]将量子信息学引入数字图像处理领域，从而设计出完整的量子图像处理算法.

图 1 展示了量子计算理论研究的发展脉络. 随着时间的发展，整个量子计算理论研究领域不断地延伸发展. 从量子计算发展的整个 30 年来看，从量子物理特性出发，目前量子计算领域朝量子算法和量子衍生信息处理技术两个方向迅猛发展. 在量子算法领域，目前虽然可用的量子工具仍然很少，量子算法能解决的实际问题也仍然很有限，但经典计算可能出现的极限以及现存的量子算法理论上的巨大的性能提高促使量子算法设计仍是众多研究者关注和创新的热点. 而在量子衍生信息处理方向，与经典的人工智能技术以及具体领域相结合设计量子衍生算法，目前已有大量研究工作并在很多应用中取得了性能提升.

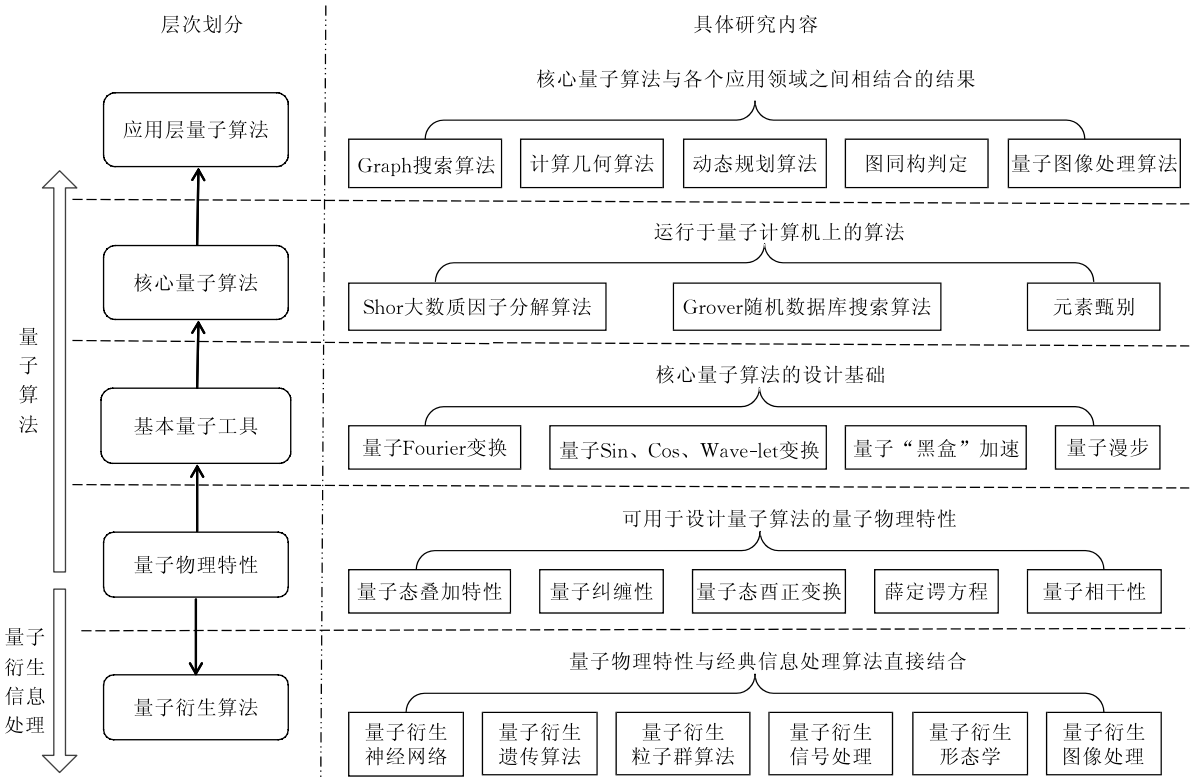


图 1 量子计算理论研究发展脉络图

### 3.2 量子计算发展规律

量子计算领域发展了近 30 年，总体来看，在量子算法和量子衍生技术两个研究方向呈现出以下发展规律.

(1) 量子算法设计的总体思路基本确定.

为了利用量子特性进行信息处理，量子算法首先需要将经典信息量子化，比如将可并行处理的数据以叠加的方式存放在量子态中，然后通过量子幺正变换等方式对信息进行处理. 为了得到算法预期的结果，量子演化过程需要将表征结果的态矢在整个叠加态中出现的概率调节得足够大. 这样，利用量子测量的手段，在计算终态中就可以以很大的概率得到算法所希望得到的结果[44]. 这就是整个量子算法设计的主要过程，目前主要的量子算法都遵循这个设计过程，从而获得了相对于经典计算在计算性能方面的极大提升. 图 2 给出了量子算法设计的基本过程.

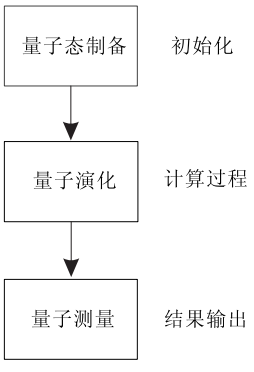


图 2 量子算法设计的基本框架

(2) 量子算法的适用范围还很有限.

虽然目前已有很多实际问题都已开发了相应的

快速量子算法，但这些已有的量子算法所处理的问题主要局限于 SIMD(Single Instruction Multiple Data)性质较好的算法(比如在经典计算中的穷举问题)以及可分解的算法(比如信号处理中的 Fourier 变换等问题)，而对于例如需用递归、分治等思想进行处理的问题目前还没有取得重大突破的量子算法研究出现[44]. 主要原因是目前仅有的几种量子工具无法在处理这类问题上取得优势. 因此，我们认为至少到目前为止，量子计算还远没有发展到取代经典计算的程度，其适用范围仍然十分有限.

(3) 量子核心算法创新困难.

量子核心算法利用了已有的量子工具并延伸出相应的应用层算法，可以说其支撑了整个量子算法脉络的发展. 因此，对于新的核心算法的探索从未停止，但却鲜有成果. 主要的原因是没有新的量子工具出现. Shor 指出由于经典计算的算法设计创新思维无法为量子计算创新带来启示[45]，人们不知道该如何寻找一个崭新的角度利用量子机制来服务于信息处理，从而使得很难能再出现像 Shor 算法[18] 和 Grover 算法[19] 这样核心量子算法出现.

(4) 量子算法设计的主要贡献在于能够突破部分经典计算极限.

之所以量子计算如此备受青睐，主要在于当经典计算遇到极限或性能瓶颈时，量子算法可能提供一种快速有效的实现方案. 目前，针对一些熟知的 NP 难题已经开发出了相应的多项式计算复杂度的量子算法[18] 以及一些高复杂度的计算问题也能够通过采用量子计算得到复杂度的巨大降低[19]. 因此，如何寻找到一个合适的经典计算难解问题并设计出相应的快速量子算法，是目前量子算法研究领域的主要动机和创新思路.

(5) 量子算法的验证仍以模拟为主.

虽然国内外部分研究机构在量子计算机研制方面取得了一定的成果，并已经出现了若干将量子算法在小规模的量子计算机模型上进行实验展示的研究工作[46-47]. 但从整个量子算法领域的发展来看，目前绝大部分的量子算法设计由于规模较大，仍然只能利用经典计算机进行模拟的手段来进行算法验证. 虽然量子算法研究通过构建量子线路模型[48] 等手段能够分析算法所带来的性能提升，但无法得到算法运行的实测结果，这也是经典算法设计和量子算法设计的差异之一. 在量子计算机真正实现并普遍适用于科学研究之前，量子算法的验证工作仍只能以模拟手段为主.

(6) 量子衍生算法研究逐渐活跃.

量子衍生算法研究对一些经典信息处理技术进行改进，并可以利用现有经典计算机对某些非线性问题实现带有量子特性的高性能信息处理，因此量子衍生信息处理是目前很多研究领域提升性能的一种重要手段，该方向的研究近年在信息处理领域逐渐活跃.

## 4　量子计算发展趋势

当前量子计算仍然是信息科学研究领域的重点和热点，越来越多的研究者正在着力于新的量子计算的研究探索中. 通过对量子计算发展脉络的梳理以及发展规律的总结，我们认为未来量子计算领域将有以下发展趋势.

(1) 量子计算所针对的问题领域将逐渐扩大，其带来的优势将更加多样化.

随着应用层量子算法设计和量子衍生信息处理成为当前量子计算发展的重要方向，目前量子计算在很多科学领域已有相应的应用. 由于量子计算巨大的并行计算能力，未来势必有更多的信息科学研究需要借助量子计算的高度并行能力来解决实际问题，这也有利于人们对量子计算的适用性等问题有更深刻的认识. 计算性能的提升是目前量子算法的主要设计目标，但量子机制能够被利用以提升哪些科学计算的处理性能等问题将会得到探索.

(2) 量子核心算法可能在 P 类问题中找到突破.

由于量子核心算法在整个量子计算中处于重要地位，因此量子核心算法的探索将仍就是未来量子计算研究的核心问题. Shor[45] 指出针对 P 类问题设计量子算法可能是一种可行的突破性探索. 虽然 P 类问题在经典计算机中已有很多成熟的优秀算法，但这并不意味着针对这类问题的量子算法没有意义. 相反，P 类问题的量子算法的设计不仅仅能够为这类问题提供多项式时间的性能加速，同时新的算法设计思路可能为其他类问题的量子算法设计带来灵感.

(3) 量子计算将与经典计算并存.

目前量子计算多采用量子线路模型[48]、簇态量子模型[49] 及绝热量子模型[50] 等针对特殊问题进行算法设计，而经典计算则采用传统的编程模型针对通用的信息处理问题进行求解. 所以量子计算技术和经典计算技术的适用领域各不相同，研究方法也

不同.目前由于量子计算机实现困难、操控复杂,同等规模的系统将需要更多的资源,故在一些量子计算无法取得巨大的计算优势的计算问题的处理上(例如小规模计算问题或串行计算问题等),经典计算相比量子计算更有优势.

另外,量子计算机的复杂操控需要借助于经典计算机的控制实现,因此即便量子计算机已经成熟到了实用阶段,量子计算仍然无法完全取代经典计算.

因此,只要量子计算机实现仍需要大量的计算资源或是经典计算机的辅助,量子计算将无法完全取代经典计算,两者将相辅相成,共同服务于未来世界的信息处理.

(4)量子计算仍将向量子算法和量子衍生技术两个方向快速发展.

到目前为止,成熟的量子工具和量子核心算法仍很缺乏,而且由于人们对量子世界的未知使得在短期内也很难有大量的工具层算法出现.因此将量子信息处理思想应用于具体科学领域,尤其是高性能计算需求高的应用领域,从而设计出具有具体领域特色的量子算法可能是未来一段时间量子计算的主要发展方向.目前在信号处理领域以及图像处理领域等都已经出现了基于量子信息处理的系统的研究,从信息预处理到信息分析已出现了基本完整的量子处理流程[41,43].因此我们认为在未来一段时间内,应用层量子算法的研究仍将继续占据量子算法研究发展的主流,会有越来越多的实际问题利用现有的量子工具找到合适的快速量子求解算法.同时量子衍生信息处理由于其可以在现有经典计算机上运行,其深入发展也将为更多实际问题的求解提供新思路.

(5)量子算法将成为未来计算体系的计算核心,而量子算法的外延设计有待研究.

有研究指出,人类所能接受和理解的信息是经典信息.这就意味着即便我们在未来设计出成熟的量子计算机,它只能相当于经典计算机中的"CPU",而我们仍需要根据计算核心的改变设计相应的"外设".直观地讲,即是如何将经典信息转化为量子信息从而使得量子计算机可以进行量子算法的运行以及如何将量子算法所得到的结果信息正确地转化为经典信息反馈给人们等问题.目前在多数量子算法中并没有针对这些内容进行深入讨论,但这些问题必须在量子计算机使用之前得到妥善解决.

(6)研究模式的创新将可能带来量子计算发展的飞跃发展.

量子线路模型[48]一直是量子计算研究的主流模式.而近年来,单向量子模型[49]和绝热量子模型[50]的出现为量子计算研究带来了新思路.最近又出现一个量子算法模式——对偶量子模型[51]可以允许在量子算法的设计中使用非酉算符.而 Gudder 证明[52],任意有界线性算符都可以在对偶量子计算中实现.这大大增加量子算法设计的灵活性,可以为今后的量子算法设计提供一条新的途径.

## 5 总 结

随着经典计算的缺陷日益显著,量子计算作为一种新型计算模型正越来越受到更多的研究者的关注.本文首先介绍了量子计算的基本原理以及其区别于经典计算的独特属性.接着,通过对量子计算30年的发展进行综述和总结,梳理出了量子计算的发展脉络.最后,本文总结了量子计算发展的一般规律并展望了未来的发展趋势.

总体来说,量子计算已经越来越多地与实际应用领域相结合,并呈现出多样化的研究趋势.虽然可用的量子计算机仍然尚未研制成熟,但这并不影响量子计算领域研究的蓬勃发展,在未来一段时间内,如何设计量子算法来解决信息科学领域难题以及如何借用量子信息处理思想在现有计算机上设计高效的量子衍生算法将仍然是科研领域的热点之一.

**致 谢** 感谢所有为本文提出宝贵意见的审稿专家.感谢国防科技大学理学院刘伟涛老师对文章修改给予的帮助,在此致以衷心的感谢!

## 参 考 文 献

[1] Schaller R R. Moore's law: Past, present and future. IEEE Spectrum, 1997, 34(6): 52-59

[2] Yang X, Wang Z, Xue J, et al. The reliability wall for exascale supercomputing. IEEE Transactions on Computers, 2012, 61(6): 767-779

[3] Nielsen M A, Chuang I L. Quantum computation and quantum information. Cambridge: Cambridge University Press, 2000

[4] Weitekamp, Daniel Paul. Time-domain multiple-quantum NMR. Lawrence Berkeley Laboratory, CA (USA), No. LBL-10593, 1982

[5] Haas F, Garcia L G, Goedert J, et al. Quantum ion-acoustic waves. Physics of Plasmas, 2003, 10(10): 3858-3866

[6] Imamog A, Awschalom D D, Burkard G, et al. Quantum information processing using quantum dot spins and cavity QED. Physical Review Letters, 1999, 83(20): 4204

[7] van Enk S J, Cirac J I, Zoller P. Ideal quantum communication over noisy channels: A quantum optical implementation. Physical Review Letters, 1997, 78(22): 4293-4296

[8] Ekert A, Jozsa R. Quantum algorithms: Entanglement—enhanced information processing. Philosophical Transactions A, 1998, 356(1743): 1769

[9] Han K H, Park K H, Lee C H, et al. Parallel quantum-inspired genetic algorithm for combinatorial optimization proble//Proceedings of the 2001 Congress on Evolutionary Computation. Seoul, Korea, 2001, 2: 1422-1429

[10] Horodecki R, Horodecki P, Horodecki M, et al. Quantum entanglement. Reviews of Modern Physics, 2009, 81(2): 865

[11] Armand F, Herrmann F, Lipkis J, et al. Multi-threaded processes in CHORUS/MIX//Proceedings of EEUG Conference. Munich, Germany, 1990: 1-13

[12] Fan Z, Qiu F, Kaufman A, et al. GPU cluster for high performance computing//Proceedings of the 2004 ACM/IEEE Conference on Supercomputing. Pittsburgh, PA, USA, 2004: 47

[13] Feynman R P. Simulating physics with computers. International Journal of Theoretical Physics, 1982, 21(6): 467-488

[14] Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer//Proceedings of the Royal Society of London. UK. Mathematical and Physical Sciences, 1985, 400(1818): 97-117

[15] Gamache R R, Davies R W. Theoretical calculations of N2-broadened halfwidths using quantum Fourier transform theory. Applied Optics, 1983, 22(24): 4013-4019

[16] Mermin N D. Quantum mysteries refined. American Journal of Physics, 1994, 62(10): 880-886

[17] Aharonov Y, Davidovich L, Zagury N. Quantum random walks. Physical Review A, 1993, 48(2): 1687-1690

[18] Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring//Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Santa Fe, NM, 1994: 124-134

[19] Grover L K. A fast quantum mechanical algorithm for database search//Proceedings of the 28th Annual ACM Symposium on Theory of Computing. Philadelphia PA, USA, 1996: 212-219

[20] Ambainis A. Quantum walk algorithm for element distinctness. SIAM Journal on Computing, 2007, 37(1): 210-239

[21] Long G L. Grover algorithm with zero theoretical failure rate. Physical Review A, 2001, 64(2): 022307

[22] Long G L, Li Y, Xiao L, et al. Phase matching in quantum searching and the improved grover algorithm. Nuclear Physics Review, 2004, 21(2): 114-116

[23] Durr C, Hoyer P. A quantum algorithm for finding the minimum. Cornell. arXiv preprint quant-ph/9607014, 1996

[24] Coffey M W, Prezkuta Z. A quantum algorithm for finding the modal value. Quantum Information Processing, 2008, 7(1): 51-54

[25] Li H S, Qingxin Z, Lan S, et al. The quantum search algorithms for all solutions. International Journal of Theoretical Physics, 2013, 52(5): 1893-1907

[26] Dürr C, Heiligman M, Høyer P, et al. Quantum query complexity of some graph problems. Automata, Languages and Programming. Springer Berlin Heidelberg, 2004: 481-493

[27] Furrow B. A panoply of quantum algorithms. Quantum Information & Computation, 2008, 8(8): 834-859

[28] Baritompa W P, Bulger D W, Wood G R. Grover's quantum algorithm applied to global optimization. SIAM Journal on Optimization, 2005, 15(4): 1170-1184

[29] Zhang W W, Gao F, Liu B, et al. A watermark strategy for quantum images based on quantum fourier transform. Quantum Information Processing, 2013, 12(2): 793-803

[30] Pang C Y, Zhou Z W, Guo G C. Quantum discrete cosine transform for image compression. Cornell. arXiv preprint quant-ph/0601043, 2006

[31] Emms D, Wilson R C, Hancock E R. Graph matching using the interference of discrete-time quantum walks. Image and Vision Computing, 2009, 27(7): 934-949

[32] Douglas B L, Wang J B. A classical approach to the graph isomorphism problem using quantum walks. Journal of Physics A: Mathematical and Theoretical, 2008, 41(7): 075303

[33] Manju A, Nigam M J. Applications of quantum inspired computational intelligence: A survey. Artificial Intelligence Review, 2012: 1-78

[34] Kak S C. Quantum neural computing. Advances in Imaging and Electron Physics, 1995, 9(4): 259-313

[35] Menneer T, Narayanan A. Quantum-inspired neural networks. University of Exeter, Technical Report R329, 1995

[36] Kouda N, Matsui N, Nishimura H, et al. Qubit neural network and its learning efficiency. Neural Computing & Applications, 2005, 14(2): 114-121

[37] Narayanan A, Moore M. Quantum-inspired genetic algorithms//Proceedings of IEEE International Conference on Evolutionary Computation. Nagoya, Japan, 1996: 61-66

[38] Han K H, Kim J H. Genetic quantum algorithm and its application to combinatorial optimization problem//Proceedings of the 2000 Congress on Evolutionary Computation. La Jolla, CA, USA, 2000, 2: 1354-1360

[39] Sun J, Feng B, Xu W. Particle swarm optimization with particles having quantum behavior//Proceedings of the Congress on Evolutionary Computation. Portland, OR, USA, 2004, 1: 325-331

[40] Shuai D, Liu Y, Shuai Q, et al. Self-organizing data clustering based on quantum entanglement model//Proceedings of the First International Multi-Symposiums on Computer and Computational Sciences. Hangzhou, China, 2006, 2: 716-723

[41] Eldar Y C, Oppenheim A V. Quantum signal processing. IEEE Signal Processing Magazine, 2002, 19(6): 12-32

[42] Xie Ke-Fu, Luo An, Zhou Xin-Yi. Morphological method inspired by quantum for edge detection of image. Computer Engineering and Applications, 2007, 43(11): 87-89 (in Chinese)
(谢可夫, 罗安, 周心一. 量子衍生形态学图像边缘检测方法. 计算机工程与应用, 2007, 43(11): 87-89)

[43] Tseng C C, Hwang T M. Quantum digital image processing algorithms//Proceedings of the 16th IPPR Conference on Computer Vision, Graphics and Image Processing. 2003: 827-834

[44] Galindo A, Martin-Delgado M A. Information and computation: Classical and quantum aspects. Reviews of Modern Physics, 2002, 74(2): 347

[45] Shor P W. Why haven't more quantum algorithms been found? Journal of the ACM, 2003, 50(1): 87-90

[46] Vandersypen L M K, Steffen M, Breyta G, et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature, 2001, 414(6866): 883-887

[47] Chuang I L, Gershenfeld N, Kubinec M. Experimental implementation of fast quantum searching. Physical Review Letters, 1998, 80(15): 3408

[48] Lloyd S. Almost any quantum logic gate is universal. Physical Review Letters, 1995, 75(2): 346

[49] Raussendorf R, Briegel H J. A one-way quantum computer. Physical Review Letters, 2001, 86(22): 5188-5191

[50] Averin D V. Adiabatic quantum computation with Cooper pairs. Solid State Communications, 1998, 105(10): 659-664

[51] Long G L. Duality quantum computing and duality quantum information processing. International Journal of Theoretical Physics, 2011, 50(4): 1305-1318

[52] Gudder S. Mathematical theory of duality quantum computers. Quantum Information Processing, 2007, 6(1): 37-48

**ZHANG Yi**, born in 1987, Ph. D. candidate. His research interests focus on quantum computation & image processing.

**LU Kai**, born in 1973, professor. His research interests focus on high performance computing.

**GAO Ying-Hui**, associate professor. His research interests include quantum computation & image processing.

**Background**

Recently, quantum computation has become an increasing hot topic as the decreasing development of the classical computation.

In this paper, firstly, the fundamental theory of quantum computation is briefly introduced by comparing with classical computation. And then the authors demonstrate the whole state of the art of quantum computation and some research principles in this field. Quantum computation includes two different research orientations: (1) quantum algorithms, which would utilize the future quantum computer to solve problems and (2) quantum-inspired information processing, which can enhance the classical algorithms and work on the classical computers. At last, some future research trends of quantum computation are discussed. Through the review and prospect of the whole field in this paper, the authors hope to make a significant guide for the future development of quantum computation.

The work in this paper is supported in part by the National High-Tech R&D Program of China (863 Program) under Grants 2012AA01A301 and 2012AA010901. And it is partially supported by National Science Foundation (NSF) China 61103082, 61003075. Moreover, it is a part of Innovation Fund Sponsor Project of Excellent Postgraduate Student of National University of Defense Technology (B120601). As a review of quantum computation, the work in this paper will be the fundamental work of these projects. Through the research of the state of the art of quantum computation, the authors find most of the researches on quantum computation focus on the combination between quantum mechanics and actual problems. And it means researchers cannot stop wondering how to utilize the future quantum computer to serve our life. Hence they would try to explore some novel and significant study or design for some actual fields such as digital image processing.

The group has much experience and researches on high performance computation and image processing, especially the high performance computation algorithms based on GPU (graphics processing units). Similar with the SIMD (single instruction multiple data) theory of GPU, quantum computation could show an unbelievable speedup of classical computation. As a novel kind of parallel tool, quantum computation will be the further research orientation of our group.