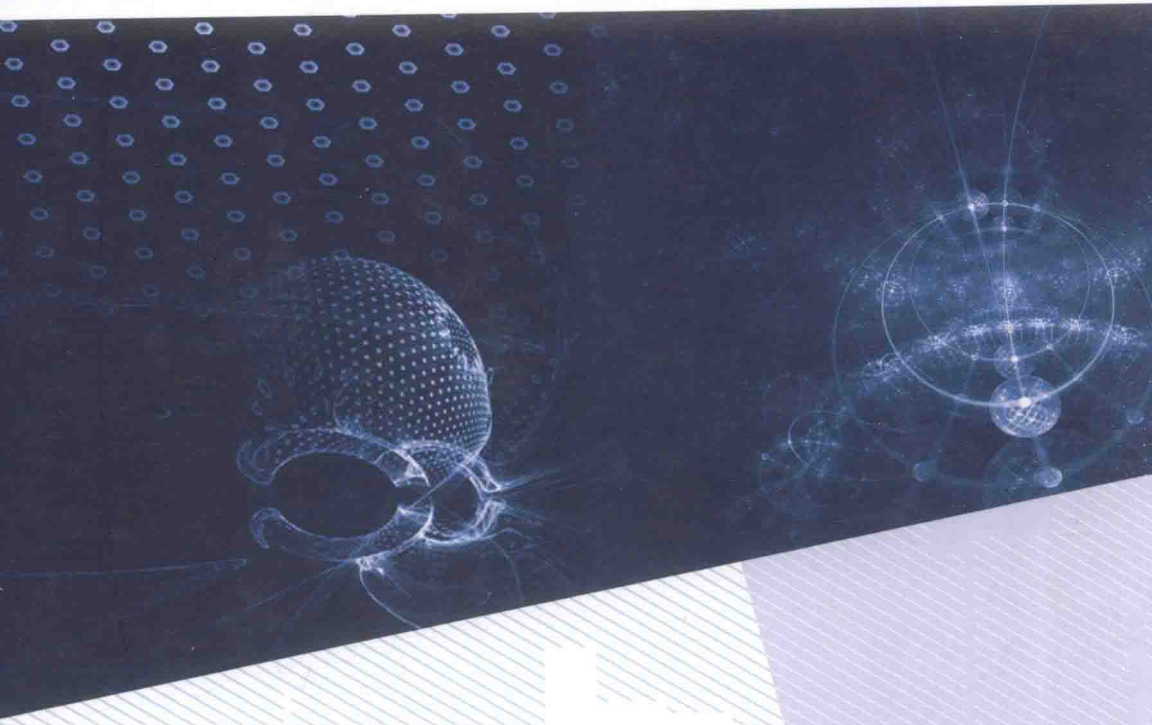
量子计算、优化与学习

焦李成 李阳阳 刘 芳 马文萍 尚荣华 著



科学出版社

量子计算、优化与学习

焦李成 李阳阳 刘 芳 马文萍 尚荣华 著

科学出版社

北京

内 容 简 介

本书对近年来量子计算智能领域常见理论及技术进行较为全面的阐述和总结，并结合作者多年的研究成果，对相关理论及技术在应用领域的实践情况进行展示和报告。全书从优化和学习两个方面展开，主要内容包含：量子计算物理基础、量子搜索与优化、量子学习、量子进化组播路由、量子粒子群优化、量子进化聚类、基于核熵成分分析的量子聚类、量子粒子群数据分类、量子进化聚类图像分割、量子免疫克隆聚类 SAR 图像分割与变化检测、量子粒子群医学图像分割和量子聚类社区检测等。

本书可作为计算机科学、信息科学、人工智能、自动化技术等领域及交叉领域中从事量子计算、进化算法、机器学习及相关应用研究的技术人员的参考书，也可作为相关专业高年级本科生和研究生的教材。

图书在版编目(CIP)数据

量子计算、优化与学习/焦李成等著. —北京: 科学出版社, 2017. 3

ISBN 978-7-03-052346-4

Ⅰ. ①量… Ⅱ. ①焦… Ⅲ. ①量子力学-信息技术 Ⅳ. ①TP387②O413.1

中国版本图书馆 CIP 数据核字 (2017) 第 053214 号

责任编辑: 宋无汗 杨 丹 / 责任校对: 刘亚琦

责任印制: 张 倩 / 封面设计: 陈 敬

科学出版社 出版

北京东黄城根北街 16 号

邮政编码: 100717

http://www.sciencep.com

北京通州皇家印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2017 年 3 月第 一 版 开本: 720×1000 1/16

2017 年 3 月第一次印刷 印张: 19 1/4

字数: 390 000

定价: 130.00 元

(如有印装质量问题, 我社负责调换)

前　言

作为20世纪最具革命性的理论成果，量子力学改变了人们对物质结构及其相互作用的认识，推动人类社会生产中的方方面面发生着深刻变化。同样，作为当下最活跃的技术领域，信息技术正在飞速发展，并催生了一大批智能化的技术和产品，改变着人类的生活和思维习惯。虽然量子力学和信息技术这两个领域的出发点不同，但随着相关理论和技术的不断更新，越来越多的研究成果表明，这两个看似毫无关联的领域，正逐渐碰撞出火花。

从20世纪90年代开始直至目前的一些研究成果均表明：人脑信息处理的过程可能与量子现象有关。英国牛津大学Penrose教授对量子理论和人脑意识的研究证明了人体内的某些细胞对单个量子敏感，因此大脑中可能存在量子力学效应；1994年美国亚利桑那大学Hameroff教授指出：在神经元细胞内架的微管之中或周围，意识是作为一个宏观量子态由量子级事件相干的一个临界极突现出来的；1996年 Perus 博士提出：量子波函数的坍缩十分类似于人脑记忆中的神经模式重构现象。所有研究结果均表明：量子系统是所有物理过程的微观系统基础，同样也应该是生物和心理过程的基础，量子系统具有和生物神经网络相似的动力学特征。

同时，国内的诸多学者在量子信息、量子通信等信息科学和量子力学的交叉领域内取得杰出成果。2003年，中国科技大学潘建伟教授所在的实验室实现了自由传播光子的隐形传态，使得量子隐形传态能应用在更加广泛的量子通信和量子计算中；2004年，在首次实现五光子纠缠的基础上，实现了一种更新颖的量子隐形传态，即终端开放的量子隐形传态，为奠定分布式量子信息处理的基础作出了贡献；2006年，首次实现了两光子复合系统量子隐形传态；2008年，首次实现了光子比特与原子比特间的量子隐形传态。2016年8月16日，中国发射世界首颗量子科学实验卫星，为量子信息、量子通信等领域的发展奠定基石。

从1996年开始，在国家“973”计划项目(2013CB329402、2006CB705707)，国家“863”计划项目(863-306-ZT06-1、863-317-03-99、2002AA135080、2006AA01Z107、2008AA01Z125和2009AA12Z210)，国家自然科学基金创新研究群体科学基金项目(61621005)，国家自然科学基金重点项目(60133010、60703107、60703108、60872548和60803098)及面上项目(61272279、61473215、61371201、61373111、61303032、61271301、61203303、61522311、61573267、61473215、61571342、61572383、61501353、61502369、61271302、61272282、61202176、

61573267、61473215、61573015、60073053、60372045 和 60575037)，国家部委科技项目资助项目(XADZ2008159 和 51307040103)，高等学校学科创新引智计划(“111”计划)项目(B07048)，国家自然科学基金重大研究计划项目(91438201 和 91438103)，教育部“长江学者和创新团队发展计划”项目(IRT_15R53 和 IRT0645)，陕西省自然科学基金项目(2007F32 和 2009JQ8015)，国家教育部高等学校博士点基金项目(20070701022 和 200807010003)，中国博士后科学基金特别资助项目(200801426),中国博士后科学基金资助项目(20080431228 和 20090451369)及教育部重点科研项目(02073)的资助下，我们对量子智能计算理论、算法及应用进行了较为系统的研究，尤其对量子优化、量子学习、量子粒子群优化及其应用、量子聚类及其应用方法等进行了较为深入的探讨。

鉴于量子智能信息处理技术展现的广阔前景，以及对社会各个方面产生的重要影响，本书作者在该领域进行了深入而有成效的研究工作。在十多年的探索研究中，取得了一些成果，并在广泛的应用领域进行了尝试。从量子智能信息处理的角度，对很多复杂问题提出了新颖的解决思路和方法。本书结合国内外的发展动态，集合了当前量子智能信息处理的相关内容，不仅包含量子计算、智能信息处理以及交叉领域的基础理论介绍，更加入了许多最新技术在不同领域的应用工作解析。

本书是西安电子科技大学智能感知与图像理解教育部重点实验室，智能感知与计算教育部国际联合实验室，国家“111”计划创新引智基地，国家“2011”信息感知协同创新中心，“大数据智能感知与计算”陕西省 2011 协同创新中心及智能信息处理研究所近十年集体智慧的结晶。特别感谢保铮院士多年来的悉心培养和指导；感谢中国科技大学陈国良院士和 IEEE 计算智能学会副主席、英国伯明翰大学姚新教授、英国埃塞克斯大学张青富教授、英国诺丁汉大学屈嵘教授的指导和帮助；感谢国家自然科学基金委信息科学部的大力支持；感谢西安电子科技大学田捷教授、高新波教授、石光明教授、梁继民教授的帮助；感谢王洋、王东、陆高、白小玉、梁晓旭、周林浩、柴英特、冉坤、卢玉静、陈正寒、徐娜娜、侯小菊等智能感知与图像理解教育部重点实验室全体成员付出的辛勤劳动。

感谢作者家人的大力支持和理解。

由于作者水平有限，书中不妥之处在所难免，恳请读者批评指正。

作　者

2016 年 10 月 28 日

目　录

第 1 章　量子计算物理基础

1.1　量 子 算 法

随着电路集成度的不断提高，量子效应开始影响电子的正常运动，经典计算机硬件的发展面临瓶颈，摩尔定律将会失效。作为突破当前计算极限的重要技术之一，量子计算成为世界各国紧密跟踪的前沿学科之一。自诺贝尔物理学奖获得者 Richard Philips Feynman 提出量子计算的概念后，相关的研究被不断推进。量子计算的并行性、指数级存储容量和指数加速特征展示了其强大的运算能力[1,2]。

1994 年 Shor[3]提出了分解大数质因子的量子算法，并吸引了众多研究者的目光。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(non-deterministic polynomial, 非确定多项式)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，这一问题可以在多项式时间内得到解决。它仅需几分钟就可以完成用 1600 台经典计算机需要 250 天才能完成的 RSA-129 问题（一种公钥密码系统），使当前公认为最安全的、经典计算机不能破译的公钥密码系统 RSA 可以被量子计算机容易地破译。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。Shor 算法的基本思想是:首先利用量子并行性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。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。

1996 年，Grover 提出 Grover 量子搜索算法，该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，对待这类问题只能逐个搜索数据库中的数据，直到找到为止，算法的时间复杂度为 $O(N)$。而 Grover 量子搜索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，并使用黑箱技术对目标数据进行标识，成功地将时间复杂度降低到 $O(\sqrt{N})$。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，可以利用 Grover 量子搜索算法进行求解。用 Grover 量子搜索算法，可以仅用 2 亿步代替经典计算机的大约 3.5×10^{16} 步，破译广泛使用的 56 位数据编码标准 DES(一种被用于保护银行间和其他方面金融事务的标准)。

自 Shor 算法和 Grover 量子搜索算法提出以后，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。以这两种算法为基础，产生了大量的讨论并有很多改进的算法被提出。Grover 量子搜索算法提出不久后有研究者提出量子态不必翻转，只需旋转一个适当的角度便可以获得与 Grover 量子搜索算法等同的效果[4]。Long 等[5]提出了量子搜索的相位匹配条件。Grover 量子搜索算法在搜索过程中没有使用具体问题的特殊结构信息，为了在搜索中利用问题的结构信息，Hogg[6]提出了基于结构的搜索算法——约束满足算法。为了能使 Grover 量子搜索算法在连续变量的全局优化问题中运用，Bulger 等[7]给出了一种用 Grover 量子搜索算法实现纯适应的搜索 (pure adaptive search, PAS) 算法，称为 Grover 适应搜索。

同时量子算法对算法设计领域产生着深刻影响。如何将量子计算强大的存储和计算优势引入到现有的算法体系中，成为广泛关注的焦点。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地弥补了智能算法中的某些不足，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有(包括但不限于以下算法)：量子退火算法、量子进化算法、量子神经网络、量子贝叶斯网络、量子小波变换、量子聚类算法等。这些算法的共同点都是应用了量子计算的机制或是受到量子机制的启发，按照某种符合量子力学行为特点的方式进行算法设计，有鲜明的量子计算的特点，或多或少延续了量子计算的优势。但是，由于量子计算设备的发展相对滞后，目前看来，这些算法并未能在真正的量子计算机上运行检验。但是通过模拟量子计算的过程，与传统的智能算法比较，这些量子智能算法广泛地展现出了较强的竞争力。

从算法功用的角度，本书将智能算法分为两大类：一类以优化为目的，称为智能优化算法；另一类以学习为目的，称为智能学习算法。以此为基础，本书将量子退火算法、量子进化算法等统称为量子优化算法；将量子神经网络、量子贝叶斯网络、量子小波变换、量子聚类算法等统称为量子学习算法。并将在第 2 章和第 3 章对这两类算法进行简单介绍。

1.2　量子系统中的叠加、相干与坍缩

在经典数字计算机中，信息被编码为位链(bit)，1bit 信息就是两种可能情况中的一种：0 或 1，假或真，对或错。例如，电容器的板极间的电压可以代表 1bit 信息：带电的电容表示 1，而放电的电容表示 0。不同于经典计算模式，在量子世界中，微观粒子的状态是不可确定的，系统以不同的概率处于不同状态的叠加之中。

量子系统中，态的叠加定义为：已知系统的两个态$|A\rangle$和$|B\rangle$，如果存在这样一种系统态$|R\rangle$，使得在其上的测量，有一定概率获得$|A\rangle$，一定概率获得$|B\rangle$，除

此之外没有其他的结果，那么$|R\rangle$称为$|A\rangle$与$|B\rangle$的叠加，记为

$$|R\rangle = c_1|A\rangle + c_2|B\rangle \tag{1-1}$$

式中，c_1和c_2称为概率幅，且$c_1^2 + c_2^2 = 1$，c_1^2和c_2^2分别为取得状态$|A\rangle$和$|B\rangle$的概率。

由态的叠加定义可得如下推论。

推论 1：一个态与自己叠加的结果仍是原来的态。

推论 2：若$|R\rangle$上还有别的测量结果，则$|R\rangle$无法只由$|A\rangle$和$|B\rangle$叠加而成。

态$|A\rangle$和$|B\rangle$的加和与数乘满足如下运算规则。

乘法结合律：$c_1(c_2|A\rangle) = (c_1c_2)|A\rangle = c_1c_2|A\rangle$

乘法分配律：$(c_1 + c_2)|A\rangle = c_1|A\rangle + c_2|A\rangle$

加法交换律：$|A\rangle + |B\rangle = |B\rangle + |A\rangle$

加法结合律：$|A\rangle + (|B\rangle + |C\rangle) = (|A\rangle + |B\rangle) + |C\rangle$

加法分配律：$c(|A\rangle + |B\rangle) = c|A\rangle + c|B\rangle$

对于量子寄存器，每一个量子位是一个双态系统。例如，半自旋或两能级原子：自旋向上表示$|0\rangle$，向下表示$|1\rangle$，以$|\phi_i\rangle$表示一个量子位的状态，则$|\phi_i\rangle$可以由状态$|0\rangle$和$|1\rangle$叠加表示为

$$|\phi_i\rangle = c_0^i|0\rangle + c_1^i|1\rangle \tag{1-2}$$

式中，c_0^i 和 c_1^i分别为状态$|\phi_i\rangle$处于基态$|0\rangle$和$|1\rangle$的概率幅，即该量子位以概率$(c_0^i)^2$和$(c_1^i)^2$处于状态$|0\rangle$和$|1\rangle$，并且$(c_0^i)^2 + (c_1^i)^2 = 1$。

更进一步，设 n 位量子比特的系统所处的状态为$|\phi\rangle$，则$|\phi\rangle$可以表示为

$$|\phi\rangle = |\phi_0\rangle \otimes |\phi_1\rangle \otimes \cdots \otimes |\phi_{n-1}\rangle \tag{1-3}$$

式中，$\otimes$表示各个状态的张量积。将式(1-2)代入式(1-3)，可得

$$\begin{aligned} |\phi\rangle = {} & (c_0^0|0\rangle + c_1^0|1\rangle) \otimes (c_0^1|0\rangle + c_1^1|1\rangle) \otimes \cdots \\ & \otimes (c_0^{n-1}|0\rangle + c_1^{n-1}|1\rangle) \\ = {} & (c_0^0 c_0^1 \cdots c_0^{n-1})|00\cdots0\rangle + (c_0^0 c_0^1 \cdots c_1^{n-1})|00\cdots1\rangle + \cdots \\ & + (c_1^0 c_1^1 \cdots c_1^{n-1})|00\cdots1\rangle \\ = {} & \sum_{i=0}^{2^n-1} c_i|\phi_i\rangle \end{aligned} \tag{1-4}$$

式中，n 位量子比特系统所处的状态$|\phi\rangle$由2^n个基态的叠加组成，且处于每一个基态的概率为c_i^2，易得$\sum_{i=0}^{2^n-1} c_i^2 = 1$。

相干与坍缩是与态的叠加紧密相关的概念，一个量子系统如果处于其基态的线性叠加中，那么此量子系统是相干的。当一个相干的系统和它周围的环境发生相互作用（测量）时，线性叠加就会消失，由此所引起的相干损失就叫做坍缩。以式(1-4)为例，系统坍缩到某个基态$|\phi_i\rangle$的概率由$|c_i|^2$决定。

1.3　量子态的干涉

干涉是一种常见的现象，是由于相位关系而产生的波的幅度增强或减弱的现象[8]。量子计算的一个主要原理为：使构成叠加态的各个基态通过量子门的作用发生干涉，从而改变它们之间的相对相位。

以叠加态式(1-5)为例，将式(1-6) Handamard 门算子$\hat{H}$代入，可得式(1-7)：

$$|\phi\rangle=\frac{2}{\sqrt{5}}|0\rangle+\frac{1}{\sqrt{5}}|1\rangle=\frac{1}{\sqrt{5}}\begin{pmatrix}2\\1\end{pmatrix} \tag{1-5}$$

$$\hat{H}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix} \tag{1-6}$$

$$\begin{aligned}|\phi'\rangle&=\hat{H}|\phi\rangle\\&=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\frac{1}{\sqrt{5}}\begin{pmatrix}2\\1\end{pmatrix}\\&=\begin{pmatrix}\frac{3}{\sqrt{10}}\\\frac{1}{\sqrt{10}}\end{pmatrix}\\&=\frac{3}{\sqrt{10}}|0\rangle+\frac{1}{\sqrt{10}}|1\rangle\end{aligned} \tag{1-7}$$

可以看出，基态$|0\rangle$的概率幅增大，而$|1\rangle$的概率幅减小。

对于单个量子位的变换，除了上述的 Handamard 门算子，还有一些常用的变换算子，如式(1-8)～式(1-10)等。其中，$\hat{I}$实现了恒等变换，即$|0\rangle\to|0\rangle$，$|1\rangle\to|1\rangle$，$\hat{X}$实现了求非变换，即$|0\rangle\to|1\rangle$，$|1\rangle\to|0\rangle$，$\hat{Z}$实现了相位移动，即$|0\rangle\to|0\rangle$，$|1\rangle\to-|1\rangle$。

$$\hat{I}=\begin{pmatrix}1&0\\0&1\end{pmatrix} \tag{1-8}$$

$$\hat{X}=\begin{pmatrix}0&1\\1&0\end{pmatrix} \tag{1-9}$$

$$\hat{Z}=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \tag{1-10}$$

在量子状态空间上，任何幺正变换都是合法的变换；反之，任何量子门 $\hat{U}$ 必须满足幺正限制，即 $\hat{U}^{+}\hat{U}=I$。其中，$\hat{U}^{+}$ 为 $\hat{U}$ 的共轭转置矩阵，I 为单位矩阵。容易验证，以上提及的各个量子门均满足幺正限制。

1.4　量子态的纠缠

从计算角度来看，纠缠态是指发生相互作用的两个子系统中所存在的一些态，它们不能表示为两个子系统态的张量积，而是表现为子系统中态的某种纠缠形式[8]。在数学上，纠缠可以使用密度矩阵来表示。量子状态 $|\phi\rangle$ 的密度矩阵 ρ_{ϕ} 定义为

$$\rho_{\phi}=|\phi\rangle\langle\phi| \tag{1-11}$$

以下以三个量子态为例。

(1) $|\phi_1\rangle=\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|01\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\\0\\0\end{pmatrix}$，相应的密度矩阵为

$$\begin{aligned}\rho_1=|\phi_1\rangle\langle\phi_1|&=\frac{1}{2}\begin{pmatrix}1&1&0&0\\1&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\\&=\frac{1}{\sqrt{2}}\left(\begin{pmatrix}1&0\\0&0\end{pmatrix}\otimes\begin{pmatrix}1&1\\1&1\end{pmatrix}\right)\end{aligned} \tag{1-12}$$

(2) $|\phi_2\rangle=\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$，相应的密度矩阵为

$$\rho_2=|\phi_2\rangle\langle\phi_2|=\frac{1}{2}\begin{pmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{pmatrix} \tag{1-13}$$

(3) $|\phi_3\rangle=\frac{1}{\sqrt{3}}|00\rangle+\frac{1}{\sqrt{3}}|01\rangle+\frac{1}{\sqrt{3}}|11\rangle$，相应的密度矩阵为

$$\rho_3=|\phi_3\rangle\langle\phi_3|=\frac{1}{3}\begin{pmatrix}1&1&0&1\\1&1&0&1\\0&0&0&0\\1&1&0&1\end{pmatrix}$$

$$=\frac{1}{\sqrt{3}}\left(\begin{pmatrix}1&1\\1&1\end{pmatrix}\otimes\begin{pmatrix}0&0\\0&1\end{pmatrix}\oplus\begin{pmatrix}1&1&0&1\\1&0&0&0\\0&0&0&0\\1&0&0&0\end{pmatrix}\right) \tag{1-14}$$

如上所述，$|\phi_1\rangle$ 可以分解为两个子系统的态的张量积，因此 $|\phi_1\rangle$ 不处于纠缠态。而 $|\phi_2\rangle$ 和 $|\phi_3\rangle$ 都无法分解为子系统态的张量积，因此它们处于纠缠态。其中，$|\phi_2\rangle$ 因为无法分解，其纠缠程度最高，$|\phi_3\rangle$ 处于部分纠缠状态。

1.5　量子计算的并行性

在经典计算机中，信息的处理是通过逻辑门进行的。量子寄存器中的量子态则是通过量子门的作用进行演化，量子门的作用与逻辑电路门类似，在指定基态的条件下，量子门可以由作用于希尔伯特空间中向量的矩阵 $\hat{U}_f$ 描述。由于量子门的线性约束，量子门对希尔伯特空间中量子状态的作用将同时作用于所有基态上，对应到 n 位量子计算机模型中，相当于同时对 2^n 个数进行运算，这就是量子并行性。量子并行性是量子计算的一个基本特性，可以简单理解为，量子的并行计算可以同时计算一个函数 $f(x)$ 的很多个不同 x 处的函数值。以式(1-15)为例：

$$|\phi\rangle=\frac{1}{\sqrt{2^n}}\left(|00\cdots0\rangle+|00\cdots1\rangle+\cdots+|11\cdots1\rangle\right)$$

$$=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}x \tag{1-15}$$

该叠加态可以看做是在 0～2^n–1 的所有整数的一个叠加态，由 $\hat{U}_f$ 的线性性质可得

$$\hat{U}_f\left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x,0\rangle\right)=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}\hat{U}_f|x,0\rangle$$

$$=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x,f(x)\oplus0\rangle$$

$$=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x,f(x)\rangle \tag{1-16}$$

其中$f(x)$即是所要计算的函数。由于n个量子位允许同时对2^n个状态进行处理，量子门的一次操作，即可计算2^n个位置的函数值。

参 考 文 献

[1] DEUTSCH D, JOZSA R. Rapid solution of problems by quantum computation[J]. Proceedings of the Royal Society A Mathematical Physical & Engineering Sciences, 1992, 439(439): 553-558.

[2] BARENCO A, DEUTSCH D, EKERT A, et al. Conditional quantum dynamics and logic gates[J]. Physical Review Letters, 1995, 74(20):4083-4086.

[3] SHOR P W. Algorithms for quantum computation: Discrete logarithms and factoring[C]// Symposium on Foundations of Computer Science. IEEE Computer Society, 1994: 124-134.

[4] GROVER L K. Quantum computers can search rapidly by using almost any transformation[J]. Physical Review Letters, 1998, 80(19): 4329.

[5] LONG G L, LI Y S, ZHANG W L, et al. Phase matching in quantum searching[J]. Physics Letters A, 1999, 262(1): 27-34.

[6] HOGG T. Quantum search heuristics[J]. Physical Review A, 2000, 61(5): 052311.

[7] BULGER D, BARITOMPA W P, WOOD G R. Implementing pure adaptive search with Grover's quantum algorithm[J]. Journal of Optimization Theory and Applications, 2003, 116(3): 517-529.

[8] 周日贵. 量子信息处理技术及算法设计[M]. 北京：科学出版社, 2013.

第 2 章　量子搜索与优化

2.1　Grover 搜索算法

本节首先介绍 Grover 搜索算法。考虑从 N 个数据中搜索某一个特定数据的问题，经典计算机上实现的时间复杂度为 $O(N)$，而在量子计算机上，Grover 搜索算法将该问题的时间复杂度降低到 $O(\sqrt{N})$，起到了对经典搜索算法的二次加速作用，显著提高了搜索效率。

Grover 搜索算法主要是通过变换量子基态的概率幅，使求解结果对应的量子基态的概率幅达到最大，同时，不满足条件的基态的概率幅不断减小。然后，对量子态进行观测时，就会以较大概率获得所要搜索的基态，即搜索成功。具体过程如下。

步骤 1：制备等概率幅叠加态 $|s\rangle$ 如下：

$$|s\rangle=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle \tag{2-1}$$

其中 n 代表所用的量子系统中的量子位的个数。该叠加态可以由 $H^{(n)}=H\otimes H\otimes\cdots\otimes H$ 对 n 位的初始态 $|00\cdots0\rangle$ 作用得到，H 为 Handamard 门算子。

步骤 2：利用黑箱算子 O 检验每个元素是否为搜索问题的解，该算子可以使目标态 $|a\rangle$ 的相位反转，任何与目标态正交的态的符号保持不变，即 $O|a\rangle=-|a\rangle$，如果 $\langle a|v\rangle=0$，则 $O|v\rangle=|v\rangle$。

步骤 3：构造幺正变换 U_s 如下：

$$U_s=2|s\rangle\langle s|-I \tag{2-2}$$

设 c_x 是当下基态 $|x\rangle$ 的概率幅，对于叠加态 $|\phi\rangle=\sum_{x=0}^{2^n-1}c_x|x\rangle$，用 U_s 对其进行变换，可得

$$\begin{aligned}U_s|\phi\rangle&=2|s\rangle\langle s|\phi\rangle-|\phi\rangle\\&=2|s\rangle\sqrt{N}\langle c_x\rangle-|\phi\rangle\\&=\sum_{x=0}^{2^n-1}\left(2\langle c_x\rangle-c_x\right)|x\rangle\end{aligned} \tag{2-3}$$