量子计算算法介绍*

龙桂鲁†

(清华大学原子分子与纳米科学重点实验室　清华大学物理系　北京　100084)

摘　要　量子计算机利用量子力学原理进行计算,具有量子并行计算的优势,能够超越经典计算.1990年中期,量子算法取得突破,舒尔(Shor)构造了大数质因子的量子算法,葛洛沃(Grover)构造了无序数据库的量子搜索算法,引起了人们对量子计算的重视,极大地推动了量子计算的研究.文章简单介绍了几个典型的量子算法以及量子算法研究的一些新进展.

关键词　量子算法,舒尔(Shor)算法,葛洛沃(Grover)算法,量子计算机

Introduction to quantum algorithms

Long　Gui-Lu†

(*Key Laboratory for Atomic and Molecular Nanosciences and Department of Physics, Tsinghua University, Beijing* 100084, *China*)

Abstract　Quantum information is an interdisciplinary science involving quantum mechanics, information theory, and computer science. It is of strategic importance and has far-reaching influence. Born in the late 1970s, it has developed very fast since the mid-1990s. Quantum information science includes quantum computing, quantum communication, and so on. The combination of different branches of science has led to many new research topics in science and technology, and many remarkable achievements have been made. This paper will introduce the basics of quantum information science, including some very important quantum algorithms such as Shor's algorithm and Grover's algorithm. The former factorizes an integer in polynomial steps, while the latter finds a marked item with a square-root increase in speed compared to classical algorithms. Other recent studies of quantum algorithms will also be reviewed.

Keywords　quantum algorithms, Shor algorithm, Grover algorithm, quantum computer

1　引言

量子计算机由两条不同的路线发展出来.一条路线是发展可逆计算机,可逆计算机可以由计算结果反逆推出输入,因为可逆计算机可以大大减少热耗.班尼奥夫(Benioff)首先利用量子力学原理构造了可逆的量子计算机[1].量子计算机发展的另一条路线是科学研究的需求,费曼(Feynman)指出,对一个量子力学体系进行模拟,需要的计算资源是体系大小的指数函数,经典计算机是无法满足模拟需要的.对量子体系的模拟,必须使用以量子力学原理进行计算的量子计算机[2].

早期量子计算机的研究非常少.1994年,舒尔(Shor)构造了大数质因子分解的量子算法[3],可以用多项式的复杂度进行大数质因子分解.1996年,葛洛沃(Grover)给出了一个量子搜索算法[4],可以平方根地加速无序数据库的搜索.这些算法显示出量子计算机具有超越经典计算机的强大功能,引起了学术界和西方国家的国防安全部门的重视,极大地推动了量子计算机研究的发展.从此量子计算机的研究成为国际上的持续的前沿研究领域.

*　国家自然科学基金(批准号:10775076)、国家重点基础研究发展计划(批准号:2006CB921106)资助项目

2010－10－19收到

†　Email:gllong@tsinghua.edu.cn

我们在本文中简单介绍量子计算的基本知识,重点介绍几个重要的量子算法,并简单介绍最近的相关发展.如需要比较详细系统的阅读,请参考文献[5—7],一些近期量子信息的进展可以参考文献[8—11].

2 量子幺正操作和量子逻辑门

根据量子力学理论,孤立量子系统态矢量随时间的动力学演化遵从 Schrödinger 方程:

$$\mathrm{i}\hbar\frac{\partial|\psi(t)\rangle}{\partial t}=\hat{H}|\psi(t)\rangle\ . \tag{1}$$

同时,在量子力学中,孤立系统的态$|\psi(t)\rangle$随时间的演化还可以通过演化算符$U(t,t_0)$来描述:

$$|\psi(t)\rangle=U(t,t_0)|\psi(t_0)\rangle\ . \tag{2}$$

当哈密顿量$\hat{H}$不显含时间时,利用初始条件$U(t,t_0)=1$,可求得演化算符为

$$U(t,t_0)=\mathrm{e}^{-\frac{\mathrm{i}}{\hbar}\hat{H}(t-t_0)}. \tag{3}$$

在量子力学中,如果算符A满足如下关系,则称之为幺正算符,

$$AA^{\dagger}=A^{\dagger}A=I\quad , \tag{4}$$

其中I为单位矩阵.显然,由于$\hat{H}$是厄米算符,演化算符$U(t,t_0)$满足幺正算符的要求,即

$$UU^{+}=U^{+}U=I\quad , \tag{5}$$

因此,幺正算符$U(t,t_0)$对应的变化通常被称为幺正变换或幺正操作.演化算符的幺正性使得量子信息过程有如下一些特殊的性质:(1)保几率性,即量子态的归一化性质不随时间的改变而改变,量子系统的总几率保持不变;(2)可逆性,即量子信息处理中的所有逻辑操作都是可逆的.

在量子信息处理过程中,系统的幺正演化通过量子逻辑门来完成,根据作用的量子位数目,量子逻辑门被分为单量子比特门、二量子比特门和多量子比特门.常见的单量子比特门主要有U_I,U_x,U_y,U_z和 Walsh-Hadamard 门H.在基矢$\{|0\rangle=\begin{pmatrix}1\\0\end{pmatrix},|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}\}$下,几个常见的单量子比特门的矩阵可表示为

$$U_I=I=\begin{pmatrix}1&0\\0&1\end{pmatrix}\quad , \tag{6}$$

$$U_x=\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix}\quad , \tag{7}$$

$$U_y=-\mathrm{i}\sigma_y=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\quad , \tag{8}$$

$$U_z=\sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\quad , \tag{9}$$

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\quad . \tag{10}$$

量子控制非门(CNOT 门)是最常用的二比特量子门之一,其中的两个量子比特分别为控制比特与目标比特.当控制比特为$|0\rangle$时,它不改变目标位;当控制比特为$|1\rangle$时,它将目标位翻转.CNOT 门的矩阵表示为

$$\mathrm{CNOT}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\quad . \tag{11}$$

英国科学家道亦奇(Deutsch)证明了任意的酉变换都可以用一组有限数目的简单酉变换的组合来构造,这些简单的酉变换称为基本逻辑门[12].巴兰克(Barenco)、班尼特(Bennett)、克里夫(Cleve)、狄文琴佐(Divincenzo)、马国鲁斯(Magolus)、舒尔等在 1995 年给出了利用单量子比特旋转门和 CNOT 门构造任意酉变换的一般方法,并给出了 4 个比特下的具体结果[13],任意数目的体系中的分解解析表达式在文献[14]中给出.如何使用最少的基本逻辑门来实现一个给定的酉变换,是一个重要的量子计算问题,目前已经有许多这方面的研究.

3 量子并行性与量子算法

量子并行计算贯穿于量子算法之中,使得量子算法与经典算法相比,以更高的效率得到所期望的计算结果.量子并行性是指,如果将量子计算过程中实施某个函数$f(x)$的幺正操作U_f,U_f作用在量子寄存器的输入叠加态上,则它将对每个基矢进行作用,并将所有结果进行线性叠加,产生一个输出叠加态.因此,只需要应用一次U_f就可以同时计算出不同x值对应的函数$f(x)$.

$$U_f\sum_i|i\rangle|0\rangle=\sum_i|i\rangle|f(i)\rangle\quad . \tag{12}$$

量子计算机是服从量子力学规律的新型计算模型,通常,我们需要用量子计算机模拟量子物理系统

随时间的演化:$U=e^{iHt}$,从而完成某一计算任务,这就需要给出具体的算法,即给出量子逻辑门序列来实现这个幺正操作.量子算法的任务是将一系列量子逻辑门组织起来,实现对量子计算机状态的幺正操作,使量子计算机按照设计者的意愿随时间演化,达到预期的输出状态.

量子算法目前可以归为以下几个种类:(1)模拟量子力学体系性质的量子仿真.从理论上说,量子计算机对此类问题具有指数化的加速;(2)基于葛洛沃量子搜索算法的量子振幅放大类算法.量子振幅放大算法即放大所需要的输出值的振幅.它的基本思想是对量子态进行幺正变换,从而放大所需要的输出值,使得在测量的时候可以很大的概率得到该结果,例如,这类算法包括了葛洛沃搜索算法及其改进和推广算法[4,15,16];(3)相位估计量子算法.舒尔算法就属于这一类算法.它的思想是通过量子酉变换,估算特定态的相位,而这个相位与本征值成正比;(4)"相对黑盒"指数加速的量子算法.这类算法是一些特别设定问题的算法,在这些问题中,量子算法显示出明显的优越性,如道亦奇算法等.

4 量子仿真

假设体系S是我们需要研究的体系,而量子计算机体系是P,量子仿真的任务就是要在量子计算机中仿真体系S的动力学演化等性质.在经典计算机上进行仿真往往需要进行很多的简化,如在原子核结构理论的计算中,通常只能取价核子,并且局限在轻核和中等质量的原子核中.

而利用量子计算则可以不采用这些简化.如果体系S和量子计算机体系P之间存在着可逆的映射ϕ,$|\psi_S(0)\rangle=\phi|\psi_P(0)\rangle$,则我们可以先在量子计算机中研究P体系的演化,$|\psi_P(T)\rangle=V_P(T)|\psi_P(0)\rangle$,然后再通过逆映射,仿真所需要研究的体系S的演化,$|\psi_S(T)=\phi^{-1}|\psi_S(T)\rangle$[17].而对应于量子计算机的演化$V_P$可以利用最基本的量子门进行构造.

量子仿真可能会成为量子计算机的一个最大的应用方向.根据一般的估计,具有几千个以上数目的量子比特的量子计算机在较短的时间内实现可能比较困难,但是只要能够有几十个量子比特的量子计算机,就可以做相当多的实际量子体系的仿真.量子仿真的研究已经成为当前的热点研究方向之一,例如已经演示了量子体系的三体相互作用[18]、四体相互作用[19]、氢分子的结合能[20,21]等.

5 "相对黑盒"指数加速的量子算法

量子黑盒是执行某种计算任务的幺正操作.它可以作为量子计算的一段子程序,当量子黑盒的输入为量子叠加态时,与输入为经典态时相比,它可以实现计算的指数加速,对应的算法称为"相对黑盒"指数加速的量子算法.

"相对黑盒"指数加速的量子算法的一个典型代表是Deutsch-Jozsa问题及其算法[22].在要求精确解的时候,Deutsch-Jozsa问题的经典解没有多项式算法,量子算法具有指数加速的优势.Deutsch-Jozsa问题是指:假设有一个n位输入的量子黑盒,它的计算函数为

$$f\{0,1\}^n\to 0,1\ , \tag{13}$$

如果对所有的输入x,$f(x)$都是0或者1,称$f(x)$是常数函数;如果对一半的输入x,$f(x)=0$,对另一半的输入x,$f(x)=1$,则称f是对称函数.Deutsch-Jozsa问题希望判定f是否为常数函数.

如果利用经典态作为输入,共需2^n+1次计算来解决此问题.而利用量子叠加态作为输入,则只需要运行一次量子黑盒,就可以得到肯定的结果.过程如下:首先,利用1个辅助量子位,将$n+1$量子位的Walsh-Hadamard变换$H^{\otimes(n+1)}$作用在$|0\rangle^n|1\rangle$态上,得到输入态

$$H^{\otimes(n+1)}|0\rangle^n|1\rangle=\left(\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\ . \tag{14}$$

然后进行U_f操作,得到

$$U_f H^{\otimes(n+1)}|0\rangle^n|1\rangle=\left(\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\ . \tag{15}$$

再对前n个输入量子位进行$H^{\otimes n}$操作,得到

$$\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle\ . \tag{16}$$

此时测量前n个量子位,如果测得$|00\cdots0\rangle$态时,说明$f(x)$是常数函数;如果测得的状态不是$|00\cdots0\rangle$态时,说明$f(x)$是对称函数.可见,相对于经典算法的2^n+1次计算,Deutsch-Jozsa量子算法只需一次黑盒计算就解决问题,它实现了"相对黑盒"的指数加速.

6 舒尔大数质因子分解算法

舒尔大数质因子分解算法[3]是一个典型的实现指数加速的量子算法.根据经典计算复杂性理论,分解大数质因子属于 NP 困难问题(即没有多项式算法的问题,但不是 NPC 问题),而在量子计算机上利用舒尔大数质因子分解算法,可以在多项式时间解决这一问题,实现了计算的指数加速.

找两个质数的乘积是一个很容易进行的运算.可是如果反过来,把一个乘积分解成两个质数的乘积,则相对于前者是一个麻烦得多的问题.一般情况下,一个大数 N,我们要将其分解,约需要计算 $\sqrt{N}=2^{\frac{1}{2}\log_2 N}$ 步.计算的步数与大数的位数成指数增长关系.一个 600 位的大数,使用目前最快的计算机,居然要用比整个宇宙的年龄还要长的时间才能分解出.目前广泛使用的 RSA 密钥系统的基础即是假定不存在快的大数分解算法.而使得 RSA 密钥系统受到巨大挑战,同时也推动了人类对量子计算机的研究.在量子计算机上实现舒尔的大数分解算法,分解一个 L 位的大数,计算步数下降为 $O(L^3)$.

假定要分解的大数为 N,舒尔算法的过程如下:

(1) 随机选取 $a(a<N$ 并与 N 互质),用量子算法求函数 $f(x)=a^x \bmod N$ 的周期 T.

(2) 若 T 为奇数,则返回 1,重新选取 a;若 T 为偶数,则取 $y=a^{T/2}$.

(3) 求得 y 后,用欧几里德辗转相除法求得 $y-1$,$y+1$ 与 N 的最大公约数 n_1,n_2,则可以找到质因子.

以上算法的关键在于求得函数 $f(x)=a^x \bmod N$ 的周期 T,这是量子计算机体现其优越性的地方.以上算法在经典计算机上进行时,需要使用比量子计算机指数多的物理资源,同时计算步骤也是呈指数增加的.

7 相位估计算法[23, 24]

假设酉算符 U 有一个本征矢量 $|u\rangle$,相应的本征值是 $e^{2\pi i\phi}$,ϕ 是未知的.相位估计算法的目的就是要将相位 ϕ 估算出来.这个算法可以用于构造许多其他量子算法.

算法的输入:(1) 一个能够运行受控 U^j 运算的系统,j 是一个任意的整数;(2) U 的一个具有本征值 $e^{2\pi i\phi_u}$ 的本征矢量 $|u\rangle$;(3) $t=n+\log(2+\frac{1}{2\epsilon})$ 个量子比特,将这些量子比特初始化到 $|0\rangle$ 上.

算法的输出:相位 ϕ_u 的 n 比特近似 $\widetilde{\phi_u}$.

算法的运行时间:$O(t^2)$ 个运算以及调用一次受控 U^j 运算,能够以 $1-\epsilon$ 的成功概率得到近似相位.

具体的过程是:

(1) 准备初始态 $|0\rangle|u\rangle$;

(2) 制备叠加态 $\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|u\rangle$;

(3) 调用受控 U^j 运算,得到 $\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle U^j|u\rangle=\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}e^{2\pi ij\phi_u}|j\rangle|u\rangle$;

(4) 做一次逆向傅里叶变换,得到 $|\widetilde{\phi_u}|u\rangle$;

(5) 测量第一个存储器,得到 $\widetilde{\phi_u}$.

相位估计算法可以用于其他的量子算法,例如,求周期函数的周期,量子时钟同步算法等.通过递推的方法,可以使用有限的比特数目,得到任意高精度的相位估计,这就是改进的递推相位估计算法[25],每一次递推给出相位的一个新的有效比特值.实验上递推相位估计算法是在 2007 年演示的[26].

8 葛洛沃量子搜索算法

1996 年,葛洛沃提出了非结构化数据库的量子搜索算法,又称为葛洛沃算法[3].该算法的时间复杂度为 $O(\sqrt{N})$,与经典算法的平均复杂度为 $O(N)$ 相比,葛洛沃量子搜索算法实现了计算的平方加速.

葛洛沃量子搜索算法要解决的问题是:在 n 个量子比特的非结构化数据库中,有 $N=2^n$ 个量子基态 $|i\rangle$,$i=1, 2, \cdots, N$,其中只有一个目标态 $|\tau\rangle$ 满足某一量子黑盒的查询函数 $C(i)=1$,其他量子态都使得查询函数 $C(i)=0$.量子搜索算法是以尽可能大的概率将目标态 $|\tau\rangle$ 找到.

葛洛沃搜索算法包括以下步骤:

(1) 数据库初始化.首先,n 量子比特的寄存器处在 $|0\rangle$ 态上,实施 n 量子比特的 Walsh-Hadamard 操作 $W=H^{\otimes n}$,此时数据库被初始化为一个平均叠加态

$$|\varphi_0\rangle=W|0\rangle=\sqrt{\frac{1}{N}}\sum_i|i\rangle=\sin\beta|\tau\rangle+\cos\beta|c\rangle, \tag{17}$$

其中

$$|c\rangle=\sqrt{\frac{1}{N-1}}\sum_{i\neq\tau}|i\rangle,\ \beta=\arcsin\left(\sqrt{\frac{1}{N}}\right). \quad (18)$$

(2) 进行葛洛沃搜索迭代 $O(\sqrt{N})$ 次,然后对 n 量子比特状态进行测量,以一定概率得到目标量子态 $|\tau\rangle$. 葛洛沃搜索迭代包括 4 个子步骤.

步骤 1:反转目标态 $|\tau\rangle$ 的相位,而其他态保持不变,这个作用可以表示为

$$I_\tau=I-2|\tau\rangle\langle\tau| \quad . \quad (19)$$

对目标态 $|\tau\rangle$ 的相位反转是通过查询函数 $C(x)$ 来完成的,如果基态 x 满足 $C(x)=1$,则对 x 态附加一个相位 π;否则保持 x 态不变.

步骤 2:进行 n 量子比特的 Walsh-Hadamard 变换,$W=H^{\otimes n}$.

步骤 3:反转除 $|0\rangle$ 态之外的所有基态的相位,而保持 $|0\rangle$ 态不变,这个作用可以表示为

$$-I_0=-I+2|0\rangle\langle 0| \quad . \quad (20)$$

步骤 4:进行 n 量子比特的 Walsh-Hadamard 变换,$W=H^{\otimes n}$.

步骤 2 至步骤 4 的过程,相当于对平均量子态进行了一个反转,将这个操作称为扩散操作,记为 D. 扩散操作 $D=-WI_0W$,D 在以 $|i\rangle(i=1,2,\cdots,N)$ 为基矢的 Hilbert 空间当中的矩阵元为

$$D_{ij}=\begin{cases}\dfrac{2}{N}, & i\neq j\\ \dfrac{2}{N}-1, & i=j\end{cases} \quad . \quad (21)$$

通过分析发现,扩散操作 D 还可以表示为

$$D=-WI_0W=W(2|0\rangle\langle 0|-I)W=2|\psi\rangle\langle\psi|-I, \quad (22)$$

其中 $|\psi\rangle$ 就是 n 量子比特系统的初态. 我们用 G 来表示葛洛沃搜索迭代的操作,则

$$G=-WI_0WI_\tau=(2|\psi\rangle\langle\psi|-I)(I-2|\tau\rangle\langle\tau|) \quad , \quad (23)$$

可以从一种更直观的几何可视化角度去理解葛洛沃量子搜索算法,即在以 $|\tau\rangle$ 态和 $|c\rangle$ 态为基矢的二维 Hilbert 空间中,葛洛沃迭代操作 G 可以表示为

$$G=\begin{bmatrix}\cos 2\beta & \sin 2\beta\\ -\sin 2\beta & \cos\beta\end{bmatrix} \quad . \quad (24)$$

I_τ 可以看作是使态在二维平面内绕 $|c\rangle$ 态做镜面反射的操作;$2|\psi\rangle\langle\psi|-I$ 可以看作是使态在二维平面内绕 $|\psi\rangle$ 态做镜面反射的操作. 单个葛洛沃搜索迭代 G 的整体作用可以看作是在二维平面内沿逆时针方向旋转 2β 角度. 因此,在连续 j 次搜索迭代之后,数据库的量子态变为

$$|\psi_j\rangle=\cos[(2j+1)\beta]|c\rangle+\sin[(2j+1)\beta]|\tau\rangle \quad . \quad (25)$$

如果要以尽可能大的概率搜索到目标态 $|\tau\rangle$,则需要尽可能满足条件 $\sin[(2j+1)\beta]=1$,因此最佳的搜索迭代步数是

$$j_{\mathrm{op}}=\begin{cases}j_m & \text{当 } j_m \text{ 为整数时}\\ \mathrm{INT}[j_m]+1 & \text{当 } j_m \text{ 不为整数时}\end{cases}, \quad (26)$$

其中

$$j_m=\frac{\pi}{4\beta}-\frac{1}{2} \quad , \quad (27)$$

INT[ ]表示对实数取整. 显然,$j_{\mathrm{op}}\approx\pi\sqrt{N}/4$. 由(25)式可知,对于某个特定的数据库,$(2j_{\mathrm{op}}+1)\beta$ 不一定恰好等于 $\pi/2$,因此葛洛沃搜索算法的最大成功率不一定为 100%,它是一个随迭代步数 j 变换的周期性函数.

9 相位匹配与精确量子搜索算法

虽然葛洛沃算法的搜索成功率很大,但是它有缺陷. 它的搜索成功率只是在只有 4 个数据的时候才是 100%. 即使在数据库很大的时候,如果标记态的数量比较大,葛洛沃算法的成功率也会很低. 例如,如果标记态的数目是数据库的一半的时候,标准的葛洛沃算法就失败了.

葛洛沃等人曾认为,如果将葛洛沃算法中的两个相位取反,换成任意角度的转动,搜索算法依然可以成功. 后来证明,葛洛沃的这个判断是错误的. 在一般的相位转动下,两个转动的角度,也就是两个相位必须满足相位匹配条件[28—30]. 一般相位转动下的量子搜索算法的搜索操作(或者叫做搜索引擎)是

$$\begin{aligned}&G=-UR_0U^{-1}R_\tau,\\ &R_0=I+(\mathrm{e}^{\mathrm{i}\theta}-1)|0\rangle\langle 0|,\\ &R\tau=I+(\mathrm{e}^{\mathrm{i}\phi}-1)\sum_k|\tau_k\rangle\langle\tau_k| \quad ,\end{aligned} \quad (28)$$

其中 θ 和 ϕ 为两个相位转角. 相位匹配条件和数据库的形式有关,对于均匀分布的初始态数据库,相位匹配条件为

$$\theta=\phi \quad . \quad (29)$$

而对于一般性的量子数据库,

$$|\psi_0\rangle=\sin\theta_0|\tau\rangle+\cos\theta_0\mathrm{e}^{\mathrm{i}\delta}|c\rangle \quad , \quad (30)$$

其相位匹配条件是

$$\begin{aligned}&\tan\frac{\theta}{2}[\cos 2\beta+\tan\theta_0\cos\delta\sin 2\beta]\\ &=\tan\frac{\phi}{2}[1-\tan\theta_0\sin\delta\sin 2\beta\tan\frac{\theta}{2}] \quad ,\end{aligned} \quad (31)$$

其中 $\sin\beta=\langle\tau|U|0\rangle$是搜索引擎中的幺正算符的矩阵元,对于标准的 Hadmard 算符,其值就是 $1/\sqrt{N}$.

相位匹配条件是量子搜索算法成功的必要条件.而葛洛沃算法的成功率不是 100% 的主要原因是,用一个固定的 180 度转动对任意的数据库进行搜索,这种粗糙的相位转动选择导致了搜索成功率的降低.2001 年构建的改进葛洛沃算法,可以精确地给出标记态[16].对于含有 1 个目标态的 N 条目非结构化量子数据库,该算法经过数次搜索迭代,可以以 100% 的成功率将目标态搜索到.其算法过程如下:对于 N 个基态的平均叠加态的数据库,

$$|\psi_0\rangle=\sqrt{\frac{1}{N}}(|0\rangle+|1\rangle+\cdots+|\tau\rangle+\cdots+|N-1\rangle). \tag{32}$$

搜索引擎为

$$\begin{aligned} L&=-WR_0WR_\tau \quad ,\\ R_\tau&=I+(e^{i\phi}-1)\,|\tau\rangle\langle\tau| \quad ,\\ R_0&=I+(e^{i\phi}-1)\,|0\rangle\langle 0| \quad , \end{aligned} \tag{33}$$

其中

$$\phi=2\arcsin\left(\sin\left(\frac{\pi}{4J_L+6}\right)\sqrt{N}\right),J_L\geq J_{op}. \tag{34}$$

需要特别指出,这里的角度不是唯一的.这里有一个最小的搜索次数 j_{op},比这个数大的任意整数都可以.在以$|\tau\rangle$态和$|c\rangle$态为基矢张开的二维 Hilbert 空间中,搜索迭代 L 可以表示为矩阵形式:

$$\begin{aligned} L&=-WR_0WR\tau\\ &=\begin{bmatrix} -e^{i\phi}(1+(e^{i\phi}-1)\sin^2\beta)-(e^{i\phi}-1)\sin\beta\cos\beta\\ -e^{i\phi}(e^{i\phi}-1)\sin\beta\cos\beta-e^{i\phi}+(e^{i\phi}-1)\sin^2\beta \end{bmatrix}, \end{aligned} \tag{35}$$

对形如(34)式的初始数据库进行 j_{op} 次的搜索迭代 L,然后对其测量,将会以 100% 的成功率找到目标态.在此算法中,经过 j_{op} 次搜索迭代后,量子寄存器态矢量变为

$$L^{j_{op}}|\psi_0\rangle=e^{i\left[j_{op}(\pi+\phi)+\frac{\pi-\phi}{2}\right]}|\tau\rangle \quad , \tag{36}$$

其中 $e^{i\left[j_{op}(\pi+\phi)+\frac{\pi-\phi}{2}\right]}$是一个没有物理效应的整体相位.因此该算法可以以 100% 的成功率搜索到目标态$|\tau\rangle$.

10 定点搜索算法

最近与葛洛沃算法有关的一个发展是定点量子搜索算法[31,32].在葛洛沃算法中,搜索成功的概率是搜索次数的三角函数,错过了最佳搜索次数之后,搜索成功的概率随着搜索次数的增加反而减少.葛洛沃定点搜索算法解决了这一问题.给定初始态是均匀量子力学叠加态,即

$$|\psi_0\rangle=\sqrt{\frac{1}{N}}\sum_{j=0}^{N-1}|j\rangle \quad . \tag{37}$$

第一次搜索的时候是采用标准的葛洛沃算符 $S_0=HR_0HR\tau$,在搜索的第二步中,将 S_0 来代替上一步中的 H,即 $S_1=S_0R_0S_0^{-1}R_\tau$.一般情况下,第 j 步搜索的算符为 $S_j=S_{j-1}R_0S_{j-1}^{-1}R_\tau$.而这里 I_0 和 R_τ 都是 $\pi/3$的相位转动.可以证明,在这样的算法中,随着搜索次数的增加,量子计算机的状态波函数越来越接近目标态,是一个定点搜索算法.但是这个算法所需要的步骤是 $O(3^n)$,比经典搜索算法需要的步骤还多.这个算法在空间资源上比经典算法节约,只需要 n 个量子比特即可,而在经典计算机中所需要的比特数目至少是 $n2^n$ 个比特.

11 结束语

舒尔算法和葛洛沃算法极大地推动了量子计算机的研究.如何从物理上实现量子计算机是当前和今后一段时间内的重要科学问题,这也是一个巨大的科学研究挑战.随着这一目标的逐渐实现,量子算法的研究会越来越重要,并且成为量子计算研究的主要内容.具有大数量比特的量子计算机在短时间内尚不能研制,而十几个甚至几十个比特的量子计算机有可能在近期研制成功.而这一规模的量子计算机可以进行相当多的量子体系的量子仿真研究.

参考文献

[1] Benioff P. J. Stat. Phys., 1980, 22(5):563

[2] Feymnman R P. Int. Journal of Theor. Phys., 1982, 21(6): 467

[3] Shor P. Algorithms for quantum computaion: discrete logarithm factoring. In:Proc. 35th Annual Symposium on computer Science, IEEE, 1994:181—182

[4] Grover L. A fast quantum mechanical algorithm for database search. In:Proc. 28th Annual ACM Symposium on Theory of Computing. ACM, New York, 1996. 212—219

[5] Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000

[6] 李承祖,黄明球,陈平行等. 量子通信和量子计算. 长沙:国防科技大学出版社,2001[Li C Z, Huang M Q, Chen P X *et al*. Quantum Commuication and Quantum Computation. Changsha: National Defence Univerdsity Press, 2001 (in Chinese)]

[7] 张永德. 量子信息物理原理. 北京:科学出版社,2006[Zhang

Y D. Principles of Quantum Information Physics. Beijing: Science Press,2006(in Chinese)]

[8] 曾谨言,裴寿镛主编. 量子力学新进展(第一辑). 北京:北京大学出版社,2000[Zeng J Y, Pei S Y. eds. Recent Progress in Quantum Mechanics, Volume 1. Beijing: Peking University Press,2000(in Chinese)]

[9] 曾谨言,裴寿镛,龙桂鲁主编. 量子力学新进展(第二辑). 北京:北京大学出版社,2000[Zeng J Y, Pei S Y, Long G L. eds. Recent Progress in Quantum Mechanics, Volume 2. Beijing:Peking University Press,2001(in Chinese)]

[10] 曾谨言,龙桂鲁,裴寿镛主编. 量子力学新进展(第三辑). 北京:清华大学出版社,2003[Zeng J Y, Long G L, Pei S Y. eds. Recent Press in Quantum Mechanics, Volume 3. Beijing:Peking University Press,2003(in Chinese)]

[11] 龙桂鲁,曾谨言,裴寿镛主编. 量子力学新进展(第四辑). 北京:清华大学出版社,2006[Long G L, Zeng J Y, Pei S Y. eds. Recent Press in Quantum Mechanics, Volume 4. Beijing:Peking University Press,2006(in Chinese)]

[12] Deutsch D. Proc. Roy. Soc. London, Ser. A,1985, 400:97

[13] Barenco A, Bennett C H, Cleve R *et al*. Phys. Rev. A, 1995,52 :3457

[14] Liu Y, Long G L, Sun Y. Int. J. Quantum Information, 2008,6:447.

[15] Boyer M, Brassard G, Hoyer P *et al*. Fortschr. Phys. ,1998, 46:493

[16] Long G L. Phys. Rev. A, 2001, 64:022307

[17] Lloyd S. Science, 1996,273:1073

[18] Tseng C H. Somaroo S, Sharf Y *et al*. Phys. Rev. A,1999, 61: 012302.

[19] Liu W Z, Zhang J F, Long G L. Chinese Sci. Bull. ,2009, 54: 4262;doi: 10.1007/s11434-009-0502-y

[20] Lanyon B P *et al*. Nature Chemistry, 2009,2:106

[21] Du J F *et al*. Phys. Rev. Lett. , 2010,104:030502

[22] Deutsch D, Jozsa R. Proc. R. Soc. London, A, 1992,439: 553

[23] Kitaeve A Y, Quantum measurements and the Abelian stablizer problem. arxiv eprint quant-ph/9511026, 1995.

[24] Cleve R, Ekert A, Macchiavello C *et al*. proc. R. Soc. London, A,1998,454:339

[25] Dobšíček M, Johansson G, Shumeiko V *et al*. 2006 arXiv: quant-ph/0610214

[26] Liu X M, Luo J, Sun X P. Chinese Phys. Lett. , 2007,24: 3316

[27] Bennett C H. SIAM J. Comput. , 1989, 18(4):766

[28] Long G L, Tu C C, Li Y S *et al*. J. Phys. A, 2001, 34(4): 861

[29] Long G L, Zhang W L, Li Y S *et al*. Commu. Theor. Phys. , 1999, 32(3):335

[30] Long G L, Xiao L, Sun Y. Phys. Lett. A, 2002, 294 (3-4):143

[31] Grover L K. Phys. Rev. Lett. , 2005, 95:150501.

[32] Li D F. Front. Comput. Sci. China, 2008,2(2):138