量子搜索算法*

孙吉贵[1,2,3+], 何雨果[1]

[1](吉林大学 计算机科学与技术学院,吉林 长春 130012)
[2](吉林大学 符号计算与知识工程教育部重点实验室,吉林 长春 130012)
[3](复旦大学 智能信息处理开放实验室,上海 200433)

A Quantum Search Algorithm

SUN Ji-Gui[1,2,3+], HE Yu-Guo[1]

[1](College of Computer Science and Technology, Jilin University, Changchun 130012, China)
[2](Key Laboratory for Symbolic Computation and Knowledge Engineering, Jilin University, Changchun 130012, China)
[3](Open Laboratory for Intelligence Information Processing, Fudan University, Shanghai 200433, China)
+ Corresponding author: Phn: 86-431-5166478, E-mail: jgsun@public.cc.jl.cn
Received 2002-01-28; Accepted 2002-04-11

Sun JG, He YG. A quantum search algorithm. *Journal of Software*, 2003,14(3):334~344.

Abstract: In this paper, an important idea of devising a quantum algorithm is introduced, based on the description and analysis of two classes of quantum search algorithms, i.e. the unstructured search algorithms and structured search algorithms. Some qualities of Grover's search algorithm, which is the representation of the unstructured search algorithms are introduced and summarized, by analyzing its peculiar complexity, completeness, sensitivity to the errors in the mappings, and its advantages and disadvantages. On introducing structure-based search algorithm, the Tad Hogg's series of search algorithms are referred to. They can be summarized into one universal algorithm framework, which can be separated into two parts, i.e., the problem-independent mapping and phase rotation matrix. This paper places emphasis on analyzing one of the phase adaptation strategies, and interprets how it works and what can make it more efficient. Some other factors affect the algorithm are also discussed more generally. Finally, based on the comparison and analysis of classical search algorithm and the quantum one, the thoughts behind various quantum search algorithms are illustrated.

Key words: quantum search algorithm; geometric interpretation of Grover's iterative procedure; problem-independent mapping; phase for nogoods

摘 要: 结合 Grover 和 Tad Hogg 的算法框架,叙述了量子算法中非结构化和结构化的两类搜索算法的设计思想.在 Grover 算法中,结合复杂性、临界点、非单调性、完备性和鲁棒性分析总结了一些性质,分析了 Grover 算

* Supported by National Natural Science Foundation of China under Grant Nos.60073039, 60273080 (国家自然科学基金); the Science and Technology Development Program of Jilin Provience of China under Grant No.20020306 (吉林省科技发展计划); the Foundation of Innovation of Jilin University of China (吉林大学创新基金)

第一作者简介: 孙吉贵(1962－),男,辽宁庄河人,博士,教授,博士生导师,主要研究领域为人工智能,约束程序设计,决策支持系统.

法的优缺点.在 Tad Hogg 算法中对独立于问题的映射和相位调整分别作了介绍.重点分析了一种相位调整策略,解释该策略有效的原因和适用的场合,讨论了影响算法效率的因素.在上述论述的基础上对量子搜索算法与传统搜索算法进行了比较和分析,总结了隐藏在不同量子搜索算法背后的深刻思想.

关键词: 量子搜索算法;Grover 迭代的几何表示;独立于问题的映射;相位调整

中图法分类号: TP301 **文献标识码**: A

计算本质上是物理的.自然界中无处不存在计算.雪花的结晶、钟摆的摆动、蜂房的构造、水的流动等等都是“自然的计算”.从这些丰富多彩的计算中,人们也学到了不少东西.以计算智能为例,就有模拟退火、Hopfield 网络中的能量函数;遗传算法等借鉴了这种自然计算的思想.在未来,人们仍将不断地从自然的计算中获取灵感和启发.

计算最终是一个物理过程[1].计算装置的物理特性决定了什么是事实上可以计算的以及对于给定的问题所需消耗的包括时间在内的计算资源.量子系统具有独特的物理特性,如叠加性、相干性.Feynman 首先认识到这些量子特性可以用于计算,例如用来有效地模拟量子系统[2].这种思想在 David Deutsch 身上得到了进一步的发展.他提出了量子图灵机和通用量子计算机的最初的构想[3],随后又提出了量子计算网络[4].Andrew Chi-Chih Yao 进一步证明任意的在量子图灵机上是多项式时间可计算的函数一定存在一个相应的多项式大小的量子电路[5].这意味着,我们可以用更为自然的量子电路来描述和实现量子算法.1993 年,Bernstein 和 Vazirani 研究了量子计算复杂性理论,并首先给出了量子图灵机比经典的概率图灵机在计算效率上更为强大的证据[6].

1994 年,Peter W.Shor 在 Daniel Simon 所著论文[7]的基础上提出了离散对数问题和大整数质因子分解问题的量子算法,证明了这两个重要且复杂的问题属于 BQP 类[8,9].Shor 的算法极大地促进了量子计算的发展,他使人们第 1 次清楚地看到了量子计算独具优势的重要应用前景.从此,世界众多研究小组加入了该研究行列,量子计算机研究领域取得了许多重大进步.在算法方面也取得了一些成果,如 Jozsa 的因子分解算法[10]、Hogg 的约束满足问题算法[11~15]、Grover 数据库搜索算法[16]、求中数[17]和平均数的算法[18]等等.Shor 的另一个同样重要的工作是率先提出了量子纠错码[19],这使得容错的量子计算成为可能[20],从而避免重蹈模拟计算的覆辙.

Julia Wallace 在“a brief histroy of quantum computation”一文中指出:已知的量子算法根据其使用的方法可以分为 3 类.有一类问题,它的所有输出具有一个共同的属性(如函数周期),相应地,有一类量子算法适用于这种情况,例如,Shor 的算法[8,9].另一种算法通过不断作幺正变换来提高所希望要的解出现的可能性.例如,Grover 的算法[16].第 3 类算法是前两类算法的结合.如 Brassard,Hoyer 和 Tapp 的近似计数算法[21].关于 Shor 的大整数质因子分解算法国内已有文章介绍[22].本文旨在结合量子计算的一个重要应用领域——组合搜索,来分析并阐述第 2 类方法的思想.

本文第 1 节首先叙述了 Grover 算法,对算法进行了详细的讨论,给出了 Grover 算法的若干性质,并分析了算法的优缺点.第 2 节描述了 Hogg 算法框架,讨论、分析了算法中结构信息的利用、算法的效率等问题.第 3 节简要比较了量子搜索算法与传统搜索算法.第 4 节给出了简要的总结.

组合搜索问题是一类重要的问题,许多问题都与它相关.另一方面,它又是困难的问题,这是因为它的解空间随着问题的规模呈指数增长.它还具有这样的特征:虽然找到解很难,但解的检验却很容易.组合搜索问题的研究具有重要的理论和应用价值,它可以广泛地应用于规划、调度、约束满足、图着色、电路设计等领域.

下面,我们首先来讨论和分析 Grover 算法[16].该算法在量子计算中有着很重要的地位.它适合于对无序数据集进行搜索.后面探讨 Tad Hogg 的算法框架,它在利用问题结构信息的搜索中具有一定的代表性.

1 Grover 的搜索算法

Grover 的算法对应于一类重要的应用,即从给定的集合中找到一个元素 X,该元素满足 $C(X)$为真.

1.1 算法叙述

(1) 初始化: $\left(\overbrace{\frac{1}{\sqrt{N}},\frac{1}{\sqrt{N}},\ldots,\frac{1}{\sqrt{N}}}^{N}\right)$.

设 n 为量子比特数, $N=2^n$.也就是说,初始时所有基矢(一组正交归一完备的矢量,取通常意义上的那一组,即(1,0,0…)(0,1,0…)…)的振幅(一个事件的概率 p 是由一个复数α决定的,$p=|\alpha|^2$ (这里,| |为取模).我们称α为概率振幅,简称振幅.α=〈终止条件|初始条件〉)相等.这可以通过 Walsh-Hadamard 变换作用在|000…0>上来实现.共需 $O(\log N)$步.Walsh-Hadamard 变换的定义为

$$H:|0\rangle\rightarrow\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\qquad |1\rangle\rightarrow\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle).$$

$$W_1=H,\ldots,W_{n+1}=H\otimes W_n,$$

故 $W_{ij}=2^{-n/2}(-1)^{\bar{i}\cdot\bar{j}}$.其中 $\bar{i}$ 是i的二进制表示. $\bar{i}\cdot\bar{j}$ 是 $\bar{i}$ 和 $\bar{j}$ 的按位与,即它们共同的1的个数.

(2) 进行 Grover 迭代(Grover iterate 简称 G:$G=DU_f$ =WRW U_f)

反复执行下述(a),(b)$O(\sqrt{N})$次(确定循环多少次是重要的,有关讨论参见文献[23]).

(a) 选择性旋转变换 U_f (相当于对解集作标记):

设 S 为输入中的一个基矢:当 $C(S)$=1 时,把矢量 S 旋转 180°;当 $C(S)$=0 时,不变.

(b) 用变换 D 作用在各输入分量上.D 定义如下: $D_{ij}=\frac{2}{N}$ if $i\neq j, D_{ii}=-1+\frac{2}{N}$.

D 可以表示成 WRW.其中 W 是 Walsh-Hadamard 变换矩阵.R 是条件相移矩阵(conditional phase shift matrix):

$$R_{ij}=0 \text{ if } i\neq j;\ R_{ii}=1 \text{ if } i=0;R_{ii}=-1 \text{ if } i\neq 0.$$

该矩阵把除了|000…0〉以外的基矢的振幅相位取反.

(3) 对输出进行测量,观察结果为 Sv.若 $C(Sv)$=1,则得到结果,否则重新开始算法.

1.2 算法的讨论分析

步骤(2)中的(a)是通过一个选择性旋转变换 U_f 得到的,在变换中借助了一个附加量子比特 b:

$$U_f:|x,b\rangle\rightarrow|x,b\oplus C(x)\rangle,$$

其中$|b\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$.设$X_0=\{x|\,C(x)=0\}$,$X_1=\{x|\,C(x)=1\}$,初始状态为$|\phi_0\rangle=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$,则

$$\begin{aligned}U_f(|\phi_0,b\rangle)&=\frac{1}{\sqrt{2^{n+1}}}U_f\Big(\sum_{x\in X_0}|x,0\rangle+\sum_{x\in X_1}|x,0\rangle-\sum_{x\in X_0}|x,1\rangle-\sum_{x\in X_1}|x,1\rangle\Big)\\&=\frac{1}{\sqrt{2^{n+1}}}\Big(\sum_{x\in X_0}|x,0\oplus 0\rangle+\sum_{x\in X_1}|x,0\oplus 1\rangle-\sum_{x\in X_0}|x,1\oplus 0\rangle-\sum_{x\in X_1}|x,1\oplus 1\rangle\Big)\\&=\frac{1}{\sqrt{2^n}}\Big(\sum_{x\in X_0}|x\rangle-\sum_{x\in X_1}|x\rangle\Big)\otimes|b\rangle.\end{aligned}$$

于是,X_1 中的矢量的振幅相位旋转了 180°.如图 1 所示.

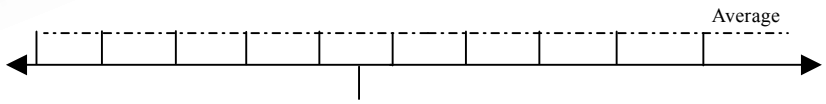


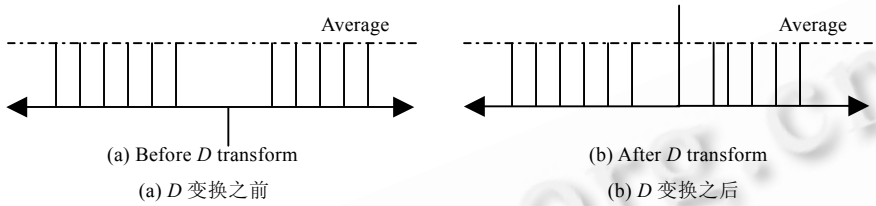
Fig.1 Inversion about average operation

图1 基于平均值的翻转

在步骤(2)(b)中, $D=-I+2P$ .I 是单位矩阵. $P_{ij}=\frac{1}{N}$;显然, $P^2=P$,所以 $D^2=I$;又 D 是实对称矩阵,故 D 是幺正的(若 $UU^+=U^+U=I$,其中 U^+ 是 U 的共轭转置矩阵,则 U 称为幺正变换矩阵.量子计算机中的变换为所有可

能的幺正变换). $P\bar{v}=T$,其中 $T_i=A=\frac{1}{N}\sum\bar{v}_i$,则有 $D\bar{v}=(-I+2P)\bar{v}=-\bar{v}+2P\bar{v}$.故 $D\bar{v}$ 的第 i 个元素为 $-\bar{v}_i+2A=A+(A-\bar{v}_i)$.因此,Grover 把这种变换叫做 the inversion about average.

设非目标矢量的振幅为 C,显然,开始时 C 大约为 $\frac{1}{\sqrt{N}}$,目标矢量的振幅是负数,则 A 大约等于 C,故非目标矢量的振幅在变换后基本不变.而目标矢量的振幅则变为正数,增长了近 $2C$,也就是约 $\frac{2}{\sqrt{N}}$.如图 2 所示.



(a) D 变换之前 (b) D 变换之后

Fig.2

图2

目标矢量的振幅大小增加了(为了叙述方便和流畅,后面提到的振幅若不特殊指出,均指振幅的大小),非目标矢量的振幅就相应地有所减少.在下一次循环中,A 变小.故目标矢量的增幅不断减少,直至某个极小值.此后,继续循环,目标矢量的振幅非但没有增加,反而减小,故循环次数的确定对该算法意义重大.

为了简化分析,可以引入 Grover 迭代的几何表示[24].如图 3 所示.

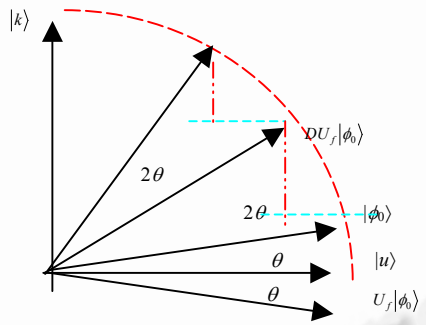


Fig.3 Geometric interpretation of Grover's iterative procedure

图3 Grover迭代的几何表示

现假设在 N 个解中存在 M 个可行解.我们可以把它们合并成两个正交基矢:

目标矢量的合并:$|k\rangle=\frac{1}{\sqrt{M}}\sum_{x\in X_1}|x\rangle$;非目标矢量的合并:$|u\rangle=\frac{1}{\sqrt{N-M}}\sum_{x\in X_0}|x\rangle$.

以这两个正交矢量为坐标轴构成了一个二维平面.由于在量子系统的演化过程中振幅都是实数,故量子系统的演化可以简化为在上述的二维欧氏空间中的演化.而这正是我们的直觉最能发挥效力的地方.

初始状态:

$$|\phi_0\rangle=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle=\frac{\sqrt{M}}{\sqrt{N}}\left(\frac{1}{\sqrt{M}}\sum_{x=X_1}|x\rangle\right)+\frac{\sqrt{N-M}}{\sqrt{N}}\left(\frac{1}{\sqrt{N-M}}\sum_{x=X_0}|x\rangle\right)=\sqrt{\frac{M}{N}}|k\rangle+\sqrt{\frac{N-M}{N}}|u\rangle.$$

U_f 对矢量作以$|u\rangle$为对称轴的旋转变换,使新矢量与原矢量关于$|u\rangle$对称.

类似地,D 对矢量作以矢量$|\phi_0\rangle$为对称轴的旋转变换,使新矢量与原矢量关于$|\phi_0\rangle$对称.故 $G=DU_f$ 相当于对矢量作了 2θ的旋转.$\theta=\sin^{-1}\sqrt{\frac{M}{N}}=\cos^{-1}\sqrt{\frac{N-M}{N}}$.

i 次迭代后:

$$(DU_f)^i|\phi_0\rangle=\sin((2i+1)\theta)|k\rangle+\cos((2i+1)\theta)|u\rangle. \quad (*)$$

性质 1. 目标矢量振幅大小是迭代次数的周期函数,其变化是非单调的.

当目标矢量振幅处在增长阶段时(如图 3 所示),Grover 迭代在增长目标矢量振幅的效率上是单调下降的,直到振幅增长到某个极大值(当 $N>>M$ 时接近 1).继续迭代,目标矢量振幅将逐渐变小.

设在某一时刻系统处于叠加态:

$$|Mid\rangle=\alpha|u\rangle+\beta|k\rangle=\alpha\left(\frac{1}{\sqrt{N-M}}\sum_{x=X_0}|x\rangle\right)+\beta\left(\frac{1}{\sqrt{M}}\sum_{x=X_1}|x\rangle\right),$$

则 $\alpha^2+\beta^2=1$.也就是说,Grover迭代实际上就是使单位矢量在上面的坐标系中以(0,0)为圆心,并以一固定的角速度逆时针旋转.由图可以清楚地看出,当迭代发生在第1象限中时,目标矢量振幅的增长是单调下降的.当然,严格证明也很容易.

性质 2. 目标矢量的振幅所能达到的最大值不小于 $\frac{N-M}{N}$.

这是因为只要在上述的坐标系中当前状态所对应的单位矢量与纵轴的夹角α大于θ,则迭代过程还可以继续进行.最终,当夹角α小于θ时, $\cos^2\alpha\geq\cos^2\theta=\frac{N-M}{N}$.当 $N>>M$ 时,算法可以通过很大的概率观测到解.

性质 3. 当迭代 $\mathrm{Round}\left(\frac{\arccos\sqrt{M/N}}{2\theta}\right)$ 时,解集的振幅总和达到最大值.我们称该迭代数为临界点(不一定是最佳停止时刻).其中,Round(x)表示四舍五入,不过,在这里,Round(0.5)=0.该性质由上述的图中很容易看出.

性质 4. 算法在临界点满足 $\frac{\pi}{8}\sqrt{\frac{N}{M}}-1<i<\frac{\pi}{4}\sqrt{\frac{N}{M}}$ .i 为迭代次数.

易知,当 $0<\theta<\pi/2$ 时,有 $2\sin\theta>\theta>\sin\theta=\sqrt{M/N}$,在式(*)中,满足:

$$\pi/2>(2i+1)\theta>(2i+1)\sin\theta=(2i+1)\sqrt{M/N},$$

故 $\frac{\pi}{4}\sqrt{\frac{N}{M}}-0.5<\frac{\pi}{4}\sqrt{\frac{N}{M}}$.因此,当解比较稠密时,算法很快就能使解集的振幅之和达到最大值.特别地,当 $M\geq\frac{N}{2}$ 时,i=0.此时无须作Grover迭代,直接测量即可.

又 $(4i+2)\sqrt{\frac{N}{M}}=(2i+1)\cdot2\sin\theta>(2i+1)\theta\geq\frac{\pi}{2}-\theta>\frac{\pi}{2}-2\sin\theta=\frac{\pi}{2}-2\sqrt{\frac{M}{N}}$,故 $\frac{\pi}{8}\sqrt{\frac{N}{M}}-1<i$.对 i 的估计可进一步精确,这里不再作进一步讨论了.

量子算法的复杂性分析有其特殊性.由于算法只能以某种概率得到解,故量子算法分析也必须紧密结合一定的概率进行.比如有一个重要的问题是:若解以概率 p 被检测到,我们该重复执行多少次才能以大于某个信念度 q 期望解至少出现 1 次? $(0<p,q<1)$ 假设需要 x 次,于是有 $1-(1-p)^x\geq q$.即 $x\geq\frac{\ln(1-q)}{\ln(1-p)}=c$. 故有:

性质 5. 若解的判定是容易的(在很多情况下是满足的,如组合搜索问题),只要 p 是不依赖于 N 的常数,则何时进行测量不会影响复杂性的阶.故一般迭代停止时刻的选择只能带来线性加速.平均地说,在成功前至少需要执行 $\frac{1}{p}$ 次(即求数学期望).

由性质 1 我们可以看出,在分析复杂性时要综合考虑单次执行的时间和执行的次数.这就是为什么 Grover 迭代不是越多越好的原因.即使振幅处在增长阶段,在算法执行的某一时刻开始,振幅的增长也极其缓慢,可能最多的时间花在了最少的振幅增长上.有关最佳停止时间(或最佳迭代次数)的分析可以参考文献[24].

性质 6. Grover算法是不完备的,不能确保问题是无解的.即当Grover的算法没有找到解时,在严格和绝对的意义上,它无法判断出到底是没有解还是因为一个小的概率没有检测出解.不过从概率的角度来看,当 $N>>M$ 时,Grover 的算法与完备算法是难以区分的.

有许多高效率的算法都是不完备的.如局部搜索算法 GSAT,WALK-SAT.在问题有解时表现出优良的性质,但却不能发现问题无解.那么,研究和设计这类算法又有多大的意义呢?我们认为很有意义.首先,对于难解问题

以及对于实时性要求高的问题,这类算法往往更有效.其次,在计算资源有闲置或不是瓶颈的情况下,这类算法的不足可以通过消耗更多的计算资源来弥补.如可以同时在两台独立的计算机上解决同一个问题.在一台上运行不完备但高速的算法,在另一台上运行完备的算法.这种思想同样适用于量子计算机和普通计算机的结合.

1.3 Grover算法的评价

优点:

(1) 由于没有使用具体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个普适的框架,是一种通用的算法[25].算法本身体现了一种重要的思想.

(2) 已经证明,对于无序数据集的搜索问题,如果忽略常系数,则 Grover 的算法属于最优的算法之一[23,26,27].

(3) Grover 算法的另一个重要优点是实现比较简单.算法中的 Walsh-Hadamard 变换和选择性旋转变换 U_f、条件相移矩阵的实现相对量子傅里叶变换来说要简单得多.一个幺正变换一般是通过基本的量子逻辑门来逼近的(极少数的由特殊的设备实现).因此量子逻辑门阵列的复杂性反映了算法的复杂性.这也涉及到量子算法设计的一个原则,即算法应尽量容易实现.例如,在 Grover 算法中 D 变换可由 $O(\log(N))$ 个基本量子逻辑门实现.Grover 算法在小规模的量子系统中得到了验证[28,29].在后面,我们把逻辑电路的规模及其实现的复杂性称为幺正变换的实现复杂性.

(4) 量子系统要与外界环境耦合,极不稳定,消相干是指数级的,因此量子力学计算机对外界扰动是极其敏感的.这样一来,在存在大量噪音的环境中要想使系统正常工作,就更需要考虑算法的鲁棒性.Grover 指出,对某些扰动,他的量子搜索算法可以具有一定的鲁棒性[30].龙桂鲁则指出,算法步骤(a)中目标矢量的旋转角度为 180°是算法具有某种鲁棒性的保证[31].另外,Grover 的算法还可以通过在一个原子上多个 Rydberg 态的叠加来实现.这种方法不需要利用纠缠态,据称具有良好的鲁棒性[32,33].

缺点:

(5) 从另一种意义上说,没有充分利用结构信息可能会影响算法的效率.普适性与效率是一对矛盾.因此,Grover 算法主要适合于无序、缺乏可利用的结构信息的问题.而在传统经典的搜索算法中,一般都充分利用结构信息.如在 DP 过程中的单元传播,对问题进行预处理对效率的提高是显著的.

(6) 从消相干的角度来看,Grover 算法的一次执行需要 $O\left(\sqrt{N/M}\right)$ 步.当数据库的规模较大时,要保持系统的相干是很困难的.在这方面,Brian M. Murphy 和 Tad Hogg 的算法可能更具优势.

(7) Grover 算法的致命缺点是需要预先知道问题有几个解.对于该算法来说,了解这个信息是关键的.从上面的分析可以清楚地看到,解的振幅的大小是算法执行次数的周期函数.因此,盲目的运行无法保证解以确定的大概率被检测到.针对 Grover 算法的这一不足,Michel Boyer 等人提出了重要的改进,仍然能够在 $O\left(\sqrt{N/M}\right)$ 步内找到解[23].

(8) 另外,与 Grover 的期望相背离的是,该算法并不适用于对数据库的搜索.这是因为,Grover 的算法需要作用在查询信息的叠加态上.这种信息一般不能通过算法的步骤(1)获得.而要由经典比特信息重建量子信息,需要 $O(N)$ 步.这样就把 Grover 算法带来的好处抵消了.除非我们能够改进存储系统,一次性地把数据信息提出到量子系统中.而且还有一个如何生成幺正变换矩阵及其实现复杂性的问题.

2 Tad Hogg 的基于结构的搜索算法

Tad Hogg 的算法与 Grover 的算法的主要区别在于利用了问题的结构信息.该算法有点类似于传统的回溯法(backtrack).其共同点在于:增量地扩充部分解(后来,Hogg 等人又提出了量子算法中的局域搜索算法[15],算法框架差不多,下面将只分析前一种增量算法).Hogg 设计出了一组组合搜索的算法(主要针对 CSP 来说)[11~15],这些算法虽然在如何处理冲突集振幅的相位上有点区别,但大体的框架是固定的.我们将在下面先介绍总体框架,然后再具体分析一种较简单的相位选择策略.

在组合搜索中有一类重要而困难的问题——约束满足问题(CSP).假设有 n 个变量 $V=\{v_1,v_2,\ldots,v_n\}$.每个变量可以取 b 个值,$X=\{x_1,x_2,\ldots,x_b\}$.也就是说是有限离散论域的.这里,假定 $b\geq 2$.要求找到对这 n 个变量的一个赋值,

这个赋值不违反问题中的约束.对于上述问题,存在一个格对应着这样的赋值空间 $V \times X$ (图 4 显示了这样的一个格结构.其中 $n=2,b=2$).对于该问题共有 b^n 个可能的赋值.随着问题规模的扩大,赋值空间将呈指数倍增长.CSP 是著名的 NP 完全的难题.

如图 4 所示,集合{1,2,3,4}中的元素都是对变量的赋值.1,2,3,4 分别对应于赋值 $x1=0$,$x1=1$,$x2=0$,$x2=1$(假设这里 $X=\{0,1\}$).

我们称一个集合 s 是“相容的”(good),若该集合中的元素不违反约束.我们把这样的集合称为“相容集”.否则叫做“冲突集”(nogood).称一个集合 s 是“完全的”(complete),若集合中共有 n 个元素.如果 $|s|<n$($|s|$表示 s 中元素的个数),则称 s 是“不完全的”(incomplete).显然,解是相容并且完全的.部分解是相容但不完全的.

格共有 nb 层,解层在 n 层.因此当 $b\geq 2$ 时,解层在格的较下面的固定位置.

Tad Hogg 的算法可以分为两部分.一部分是独立于问题的,实现振幅从格底向解层传播.另一部分则依赖于具体的问题,主要实现振幅的旋转(如果把振幅看做是复平面上的一个矢量的话).这一部分是基于结构搜索的灵魂.对问题结构信息的利用也体现在这里.其中第 1 部分基本上是固定的,仅与问题中变量的个数和值域的大小有关.第 2 部分实质上是一个通过决定振幅的相位变化来调整振幅的传播向解集集中的过程.

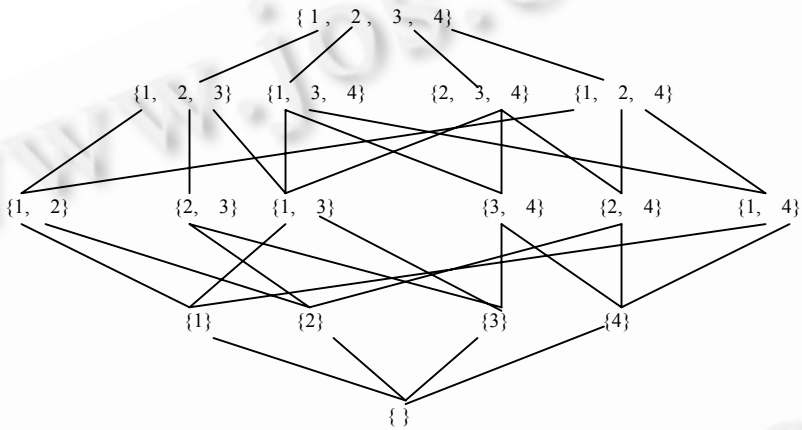


Fig.4 Structure of the set lattice when nb=4

图4 nb=4的格的结构

nb=4 的格的结构.{1,2,3,4}的子集以集合的大小分组形成格中的各层.集合与它的直接的超集(只相差一个元素)之间通过直线相连.格底的空集属于 0 层.

2.1 Tad Hogg搜索算法框架描述

设 $\psi_s^{(j)}$ 是 j 步后集合 s 的振幅.解层位置在 J 层.

步骤 1. 初始时,若 $s=\phi$,则 $\psi_s^{(0)}=1$,否则 $\psi_s^{(0)}=0$.

步骤 2. 令 j 从 1 到 J 重复执行下面过程:

$$\psi_r^{(j)}=\sum_s U_{rs}\rho_s\psi_s^{(j-1)}.$$

其中 ρ_s 使对应集合s的振幅相位发生变化.

该循环也可写成:

$$|\phi^{(J)}\rangle=UP^{(J)}\ldots UP^{(1)}|\phi^{(0)}\rangle=U^{(J)}P^{(J)}\ldots U^{(1)}P^{(1)}|\phi^{(0)}\rangle,$$

其中 $|\phi^{(0)}\rangle$和$|\phi^{(J)}\rangle$分别为初始时和传播终止时的量子态.

步骤 3. 测量.

2.2 算法讨论与分析

(1) 步骤 2 中 U 是 $U^{(1)},U^{(2)},\ldots,U^{(nb)}$的合并.$U$ 和 $U^{(i)}$ 是独立于问题的.U 负责格中所有集合振幅向上的传播.而 $U^{(i)}$ 仅负责从第 i 层到第 j 层的映射.显然,把 U 分解成 $U^{(i)}$ 是合适的.有利于减少映射实现时的复杂性.为了映

射的通用和简单,这里允许对同一个变量具有不同的赋值.

(2) 正如前面已经提到的,对于量子算法的实现需要考虑一个重要的问题,即映射中不可预测的错误对算法表现的影响.在 Hogg 的算法中,对这种错误最敏感的部分在映射 $U^{(i)}$.而 $P^{(i)}$ 的容错性相对较好.这是因为,与 $U^{(i)}$ 必须精确地把振幅向上传播有所不同,包含在 $P^{(i)}$ 中的相位选择策略本身对精度要求不高.

(3) 在Hogg的算法中,独立于问题的映射虽然缺乏个性,却是集中体现量子计算优点的地方.因为它允许同时搜索访问上层诸集合.而另一方面,即在充分利用问题特有的性质、结构方面,传统方法显得更加简单、灵活.

(4) 当映射不是幺正的时候,可以用奇异值分解(singular value decomposition)技术构造出最逼近原映射的幺正变换.但还可用另一种经典技术构造映射:即用 $WD^{(i)}W$ 来传播振幅.其中 W 是 Walsh-Hadamard 变换. $D^{(i)}$ 是一对角矩阵, $D_{rr}^{(i)}=e^{j\pi g(i,|r|)}$.其中 $|r|$ 表示 r 的二进制表示中 1 的个数.容易看出, $U^{(i)}$ 与具体的问题无关.

(5) $P^{(i)}$ 是依赖于问题的. $P^{(i)}$ 是对角矩阵,一般具有如下的形式:

$$P_{ss}^{(i)}=\rho_s^{(i)}=\mathrm{e}^{j\pi f(i,c(s))}.$$

其中 $j=\sqrt{-1}$,即 $P^{(i)}$ 是一个相移矩阵.例如, $P_{ss}^{(i)}=\sqrt{2}\cos\frac{\pi(2c(s)-1)}{4}=e^{j\pi f(i,c(s))}$, $f(i,c(s))=\frac{1-\sqrt{2}\cos\frac{\pi(2c(s)-1)}{4}}{2}$.

$c(s)$ 为赋值 s 下真值为 0 的子句的个数.它决定了 $P_{ss}^{(i)}$ 的取值,在相位调整中体现了对问题信息的利用.

在相位调整中,主要有以下几个策略:当 s 是相容集时, $\rho_s^{(i)}=1$ (Hogg 在文献[12]中作了些改进),否则,

(a) $\rho_s^{(i)}$ 取 $(0,2\pi]$ 中的任意值.

(b) $\rho_s^{(i)}=-1$.即相位取反.显然,当在与格中集合相连的所有子集中,相容集与冲突集数目大致相当时(如果有冲突集的话),该策略的效果最好(文献[11]中的例子可以证明这一点).

(c) $\rho_s^{(i)}=\mathrm{e}^{j\pi f(i,c(s))}$.该策略也适合于部分约束满足问题(partial constraint satisfaction problem)和最优化搜索等.

(6) 下面我们选择相位调整策略(a)来说明相位调整是如何可能影响振幅的再分配的.

设 s 在 i 层,并且 s 的 i–1 层上的子集都是冲突子集.设 s 只从 $C_i^{i-1}=i$ 个冲突子集 s_m (m=1,…,i)中获取振幅.假设各个子集的振幅大小相等,则

$$E(|\psi(s)|)=E(|(\sum_{m=1}^{i}|\psi(s_m)|e^{i\phi_m})|)=E(|\psi(s_i)|\cdot\left|\sum_{m=1}^{i}e^{i\phi_m}\right|)=|\psi(s_i)|\cdot\sqrt{i}\ ,\ \phi_m\in(0,2\pi].$$

注意,在推导中应用了这样一个结论:假设我们连续地走出 i 步,每步的方向是任意的,则平均地讲,我们离出发点的距离为 $\sqrt{i}$.

证明:当 $k=1$ 时,结论显然.假设当 $k=i$–1 时结论成立.设 $Ea=\sqrt{i-1}$,则 $E(\int_0^{\pi}(a^2+1-2a\cos(\pi-\theta))\cdot\frac{1}{\pi}\mathrm{d}\theta)=E(a^2+1)=i$.故当 $k=i$ 时结论也成立. □

显然,这个结论只有在重复次数较多时才有效.注意,该问题在二维平面上是无方向性的,即始点到终点的方向在二维平面上的分布是均匀的.理解这一点对理解以下性质是很重要的:

性质 7. 若 s 在 i 层,s 在 i–1 层上有 p 个冲突子集 s_m ($p\le i$ 且 $m=1,...,p$)且 s 只从 $C_i^{i-1}=i$ 个子集中获取振幅.假设各个子集的振幅大小相等,则 $E(|\psi(s)|)=|\psi(s_m)|\cdot\sqrt{p+(i-p)^2}$.

显然,当 $p=0$ 时, $E(|\psi(s)|)$ 取得最大值,当 $p=i$ 和 p=i–1 时取最小值.证明方法同上.

从个体的角度来看,在冲突集超集的子集中冲突集越多越好.从性质 7 可以看出,当 $0\le p<i$ 时, $E(|\psi(s)|)$ 是单调递减的.且当 $i\ge1$ 时, $\sqrt{i}/i$ 也是一个单调递减函数, $\lim_{i\to\infty}\sqrt{i}/i=0$.可以看出,当 i 较大时,冲突集的振幅向超集传播过程中的相对损失是很大的.相应地,解集的相对收益也随之增大.这里,假设冲突集的振幅都向上传播了.为了保证这一点,冲突集的振幅不仅向它的超集传播,还部分流向它的上层相容集.

但从整体的角度来看,冲突集向超集的传播应是均匀的(这是由同一层中冲突集的分布特征决定的).若大多数的传播都集中在某几个超集上,则其他冲突集的超集的振幅就不能有效地被消除,约束冲突不能有效地向上传播.其结果是有很大一部分振幅“流”到了解层中的冲突集上.

另外,冲突集在格中的位置越低越好,与解层的距离越远越好.这对所有的策略都是有利的.

因为约束冲突发现得越及时,振幅就越难向解层中的冲突集传播.

2.3 Hogg算法的效率

Hogg 算法的效率取决于两个因素:独立于问题的映射的实现复杂性以及振幅向解集集中的效率和程度.实际上主要体现在:① 解层的位置(对应着变量的数目)和冲突集的分布;② 对冲突集的相位调整策略.前者主要由问题本身决定的,后者是对算法进行改进和优化的关键所在.

约束的大小或元数(这里是指约束中包含的变量的个数)对算法的影响很大.显然,在一元约束的问题中,冲突集出现在第 1 层.这对相位调整是很有利的.若约束过大(与过约束不是一个概念),包含的变量太多,则冲突集的出现会过分接近解层,就会对相位调整策略提出很高的要求.在通常情况下,我们对问题的具体结构不会太清楚.故这种情况也会在很大程度上影响振幅向解集集中.在约束都是 n 元约束时,该算法一般是无效的.

上面讨论的是约束的个体性质对算法的影响.下面再讨论约束集合在整体上对算法的影响.

与自然现象相似,在约束问题中也存在相变(phase transitions)的情况.一般来说,约束较少、较弱时,解集较大,故解集的总体振幅也较大,这时,解容易被检测到.当约束较多、较强时,冲突集较多地集中在格的底部,或说大的部分解较少,故最终振幅更容易集中在解集上.在这两种情况之间,算法的效率相对较低.在某一点算法的效率达到最低,而且这一点一般是独立于各种算法,而与问题本身有关的.形成易-难-易的特征.问题的规模越大,相变也越明显.

相变是一种基本独立于许多算法的现象,它必定与问题中约束结构的统计学意义上的特性有关.一般在检测对比搜索算法的效率时,在相变临界点附近比较好.这是因为不同的搜索算法在相变区以外的地方一般效率都不错,难以区分搜索算法的优劣.Hogg 告诉我们,用量子算法解决约束满足问题,也可能存在相变的现象.

对一个算法来说,存在相变的现象并不是一件坏事.它说明算法可能充分利用了结构信息以提高效率.一个忽视结构信息的算法是不存在相变的.而且若相变情况相似,可能暗示着对相似结构信息的利用.对于量子计算来说,这一点尤其重要.因为目前的量子计算系统的规模还很小,只能用来测试一些很小的问题.而像 Hogg 那样的算法由于其效率与问题本身有关,因而分析其复杂性是很困难的.这样,利用相变的估计来研究其对结构信息的利用和效率就不失为一个可以考虑的途径.

3 量子搜索算法与传统搜索算法的比较

传统搜索算法主要是要克服由解空间过大而导致的需要搜索的路径过多的问题,因此经典搜索策略的核心特征为:设法减少实际搜索空间,当然同时也要考虑挖掘利用结构信息时付出的代价.而量子算法面临的主要问题是解集的振幅太小,因此量子搜索算法策略的核心是:如何迅速地使振幅向解集集中,同时考虑变换的实现复杂性和鲁棒性.也就是说,传统搜索算法考虑的是如何避免在无效路径上进行搜索,而对量子算法来说,搜索所有的路径不是困难所在.量子算法寻求的是如何减少、消除非解路径上的振幅,并把它转移到解路径上来.

打一个比方.搜索算法解决问题就像看一幅巨大的图画并从中找出目标来.传统的方法就好像一个近视的人,为了看清图,不得不离图很近,所以每次只能看到一个(或几个)点.因此为了在“有生之年”看到目标点,他不得不利用结构信息跳跃着选择注视点.而量子算法好像站在远处了望的人,他可以同时看到整幅图画.可惜他看到的只是一幅模糊的图画,为了看清目标,他不得不设法把目标的“颜色”加浓,同时使其他点的颜色变谈.从而使目标更清晰、更突出.这里,“颜色”的深浅就相当于振幅的大小.

4 结 语

虽然 Grover 的算法具有种种缺陷和不足,但它在量子算法早期发展中具有重要的意义.它为量子算法的设计提供了一种框架和思想,故与 Shor 的大整数质因子分解算法一样,是量子算法宝库中的明珠.

与 Grover 的算法相比,Hogg 的算法利用了问题的结构信息,若相位调整策略选择得当,则可能比 Grover 的算法更有效[34].要想对 Hogg 的算法的效率有更深入的了解,还有待于更好的复杂性分析技术的出现或进行规

模更大的试验.

量子计算技术对人工智能的发展有深远的影响.对于现在的人工智能来说,面临的两个主要问题是:(1) 缺乏统一的基本理论的指导,经验的成分较多.知识表示能力与自然语言理解能力还不够.(2) 人工智能面对的问题复杂,相应地,算法复杂性一般也很高.我们认为,对于后者,量子算法的研究可能会在很大程度上改变这种局面.

从软件技术的角度来看,目前的量子算法主要是直接针对量子比特进行设计的.量子算法的设计对设计者要求高,不利于推广(虽然已有了一些算法的框架).从目前的算法来看,大多简洁、精巧,观察问题的层次低.在这个领域,软件、算法的设计与传统的差别很大,很难借鉴传统已有的、成熟的软件设计思想.成熟的量子软件技术和方法学还有待发展.

虽然有种种不足,但纵观量子计算机发展的历史,我们发现,现在的量子计算机是通过克服一个个当初认为的"不可能"而走到今天的.是科学家们的勇敢和热情促使了这一切或者说一种令人憧憬的可能的发生.我们相信,凭借勇气和科学的态度、方法,量子计算技术能走得更远、更好.

References:

[1] Landauer R. Information is physical. Physics Today, 1991,44(5):23~29.

[2] Feynman R. Simulating physics with computers. International Journal of Theoretical Physics, 1982,21:467~488.

[3] Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer. Proceedings of the Royal Society of London (series A), 1985,400:97~117.

[4] Deutsch D. Quantum computational networks. Proceedings of the Royal Society of London (series A), 1989,425:73~90.

[5] Yao A. Quantum circuit complexity. In: Proceedings of the 34th Annual Symposium on Foundations of Computer Science. IEEE Computer Society Press, 1993. 352~361.

[6] Bernstein E, Vazirani U. Quantum complexity theory. In: Proceedings of the 25th ACM Symposium on Theory of Computating. 1993. 11~20.

[7] Simon DR. On the power of quantum computation. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science. IEEE Computer Society Press, 1994. 116~123.

[8] Shor PW. Algorithms for quantum omputation: discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Santa Fe: IEEE Computer Society Press, 1994. 124~134.

[9] Shor PW. Polynomial-Time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal of Computing, 1997,26(5):1484~1509.

[10] Jozsa R. Quantum algorithms and the Fourier transform. Proceedings of the Royal Society of London (series A), 1998,454:323~338.

[11] Hogg T. Quantum computing and phase transitions in combinatorial search. Journal of Artificial Intelligence Research, 1996, 4:91~128.

[12] Hogg T. A framework for structured quantum search. Physica D, 1998,120:102~116.

[13] Hogg T. Highly structured searches with quantum computers. Physical Review Letters, 1998,80:2473~2476.

[14] Hogg T. Solving highly constrained search problems with quantum computers. Journal of Artificial Intelligence Research, 1999,10: 39~66.

[15] Hogg T, Yanik M. Local search methods for quantum computers. Technical Report, 1998.

[16] Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on the Theory of Computing. 1996. 212~219.

[17] Grover LK. A fast quantum mechanical algorithm for estimating the median. Technical Report, quant-ph/9607024, 1996.

[18] Grover LK. Quantum Telecomputation. Technical Report, quant-ph/9704012, 1997.

[19] Shor PW. Scheme for reducing decoherence in quantum computer memory. Physical Review A, 1995,52(4):R2493.

[20] Shor PW. Fault-Tolerant quantum computation. In: Proceedings of the 37th Annual Symposium on Foundations of Computer Science. IEEE Computer Society Press, 1996. 56~65.

[21] Brassard G, Hoyer P, Tapp A. Quantum counting. In: Proceedings of the 25th ICALP. Lecture Notes in Computer Science, Vol 1443, Berlin: Springer-Verlag, 1998. 820~831.

[22] Zhang ZJ, Zhang ZL. Prime factorization in quantum computation. Physics, 2000,29(9):560~564 (in Chinese with English Abstract).

[23] Boyer M, Brassard G, Hoyer P, Tapp A. Tight bounds on quantum searching. In: Proceedings of the Workshop on Physics of Computation: PhysComp'96. IEEE Computer Society Press, 1996.

[24] Nielson MA, Chuang IL. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000.

[25] Grover LK. A framework for fast quantum mechanical algorithms. In: Proceedings of the 30th Annual ACM Symposium on Theory of Computing. 1998. 53~62.

[26] Bennett CH, Bernstein E, Brassard G, Vazirani U. Strengths and weaknesses of quantum computing. SIAM Journal on Computing, 1997,26(5):1510~1523.

[27] Zalka. Grover's quantum searching algorithm is optimal. Physical Review A, 1999,60:2746~2751.

[28] Jones JA, Mosca M, Hansen RH. Implementation of a quantum search algorithm on a quantum computer. Nature, 1998, 393:344~346.

[29] Chuang IL, Gershenfeld N, Kubinec M. Experimental implementation of fast quantum searching. Physical Review Letter, 1998,80(15):3408~3411.

[30] Grover LK. Quantum computers can search rapidly by using almost any transformation. Physical Review Letters, 1998,80(19): 4329~4332.

[31] Long GL, Zhang WL, Li YS, Niu Li. Arbitrary phase rotation of the marked state can not be used for Grover's quantum search algorithm. Commun.Theor.Phys., 1999,32:335~338.

[32] Ahn J, Weinacht TC, Bucksbaum PH. Information storage and retrieval through quantum phase. Science, 2000,287(5452):463~465.

[33] Knight P. Hanced: quantum information processing without entanglement. Science, 2000,287(5452):441~442.

[34] Peng XH, Zhu XW, Fang XM, Feng M, Liu ML, Gao KL. Experimental implementation of Hogg's algorithm on a three-quantum-bit NMR quantum computer. Technical Report, quant-ph/0108068, 2001.

附中文参考文献:

[22] 张镇九,张昭理.量子计算中的因子分解.物理,2000,29(9):560~564.