一种 Grover 量子搜索算法的改进策略

李盼池[1,2],李士勇[1]
(1. 哈尔滨工业大学 航天学院,黑龙江 哈尔滨 150001;2. 大庆石油学院 计算机系,黑龙江 大庆 163318)

摘 要:在使用 Grover 量子搜索算法对给定规模的数据库搜索时,随着搜索目标数的增加,获得正确结果的概率大幅度下降. 分析了出现这种现象的原因,提出了一种基于新的相位匹配条件的改进策略. 在新的相位匹配条件中,使 2 次相位旋转的大小相等方向相反. 当要搜索的目标数目多于记录总数的 1/3 时,应用改进后的算法只需一步搜索,能以至少 25/27 的概率得到全部搜索目标. 实验证明这种策略是有效的.

关键词: Grover 算法;相位匹配;量子搜索;量子计算
中图分类号: TP18 **文献标识码**: A **文章编号**: 1673-4785(2007)01-0035-05

An improved measure in Grover quantum searching algorithm

LI Pan-chi[1,2], LI Shi-yong[1]
(1. School of Astronautics, Harbin Institute of Technology, Harbin 150001, China; 2. Department of Computer Science, Daqing Petroleum Institute, Daqing 163318, China)

Abstract: When the current Grover algorithm is applied to search some objects in an unsorted quantum database, the probability of correct objects usually falls with the increase of the searched objects. The reason for this problem is analyzed in this paper, and an improved measure based on the new phase matching condition is proposed. In the new phase matching condition, the amplitudes of two phase rotations are the same and the directions of two phase rotations are contrary. When the objects are more than one third of the total items, with the new phase matching condition, all objects can be found by at least 25/27 of the probability and by the only one Grover iteration. The validity of the improved measure is proved by experiment.

Keywords: Grover algorithm; phase matching; quantum searching; quantum computing

Grover 量子搜索算法[1]和 Shor 大数质因子分解算法[2]是 2 个最著名的量子算法. 对于在无序数据库中搜索若干特定目标时, Grover 算法可以对许多(虽不是全部)启发式搜索的经典算法起到实质性的二次加速作用; Grover 算法在搜索时忽略搜索元素的性质,而把注意力放在那些元素的指标(对应 0 ～N - 1 的数字)上,因此具有很强的通用性[3]. 由于这 2 个特点, Grover 算法引起了人们广泛关注. 自 1996 年 Grover 算法首次提出以来,人们对于该算法的研究主要集中在改进、推广和应用 3 个方面. 在算法的改进方面, Grover 在文献[4]中指出,算法中的 Walsh-Hadamard 变换可由任意酉算子代替;龙桂鲁等人提出了新的 Grover 量子搜索算法中的相位匹配条件[5],认为搜索算法中的 2 次相位取反可以改为任意的相位旋转,但需满足 2 次相位旋转的大小和方向均相同. 在算法的推广方面,文献[6]考察了系统基态概率幅取任意初始分布时的 Grover 算法;文献[7]考察了系统取任意初始混合态时的 Grover 算法;文献[8]将 Grover 算法看作一个动态系统,详细分析了系统取任意纯态时,算法的各项性能. 在算法的应用方面,文献[9]将该算法和神经网络相融合提出一种量子联想记忆模型,与传统的 Hopfield 记忆模型相比,该模型的存储容量具有指数级的扩充;文献[10]对上述模型作了推广,提出了一种基于分布式查询的量子联想记忆模型等.

此外, Grover 算法也存在自身的缺陷. 当搜索

收稿日期:2006-05-18.
基金项目:国家自然科学基金资助项目(50138010).

目标大于数据库记录数的1/4时,搜索成功的概率快速降低,当搜索的目标大于数据库记录数的一半时,搜索失效.已有改进措施均不能解决这一问题.针对这一问题,文中从分析算法中旋转相位的匹配条件入手,提出了改进措施.该措施使搜索过程中2次相位旋转的大小相等,方向相反.应用改进后的算法,当搜索目标数较多时,只需一步搜索,即可获得很高的成功概率,并且随搜索目标数的增加,这种高概率变化很小.

1 普通 Grover 算法及存在问题

1.1 Grover 算法简介

假设在 N 个元素的搜索空间中进行搜索,为方便起见,假定 $N=2^n$,于是元素指标可以存储在 n 个量子比特中.假设搜索问题恰有 M 个解 $\Omega=\{\tau_1,\tau_2,\cdots,\tau_M\}$,$1\leq M\leq N$.

Grover 算法的初始状态为 n 个量子比特的均匀迭加态

$$|\phi>=\frac{1}{\sqrt{N}}\sum_j|j>+\frac{1}{\sqrt{N}}\sum_k|k>. \quad (1)$$

其中记号"$|>$"称为 Dirac 记号,它在量子力学中表示状态,另外记号"$|\alpha><\beta|$"表示量子态$|\alpha>$和$|\beta>$和的外积,其实质是一个描述量子态演化的酉算子.搜索过程包括以下4个步骤.

1)目标态取反:$|\phi_1>=O|\phi>$.

$$O=I-2\sum_m^M|\tau_m><\tau_m|. \quad (2)$$

式中:I为单位矩阵.

2)应用 Hadamard 变换:$|\phi_2>=|H^{\otimes n}|\phi_1>$.

式中:$H^{\otimes n}=\frac{1}{\sqrt{2^n}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}^{\otimes n}$.

3)执行条件相移:

$$|\phi_3>=(2|0><0|-I)|\phi_2>.$$

4)应用 Hadamard 变换:$|\phi_4>=H^{\otimes n}|\phi_3>$

由 Hadamard 门性质,将2)、3)、4)3步结合的效果为

$$U_s=2|\phi><\phi|-I. \quad (3)$$

记 $\lambda=\frac{M}{N}$,对于上述4步,调用次数 R 为

$$R=CI\left(\frac{\arccos\sqrt{\lambda}}{2\arcsin\sqrt{\lambda}}\right). \quad (4)$$

式中:CI(x)表示取最接近实数 x 的整数,按习惯将一半向下取整.因此,至多经过 R 次 Grover 调用,即能以至少1/2的概率搜索到问题的 M 个解.

1.2 Grover 算法成功搜索的概率

令$|\alpha>$为 $N-M$ 个非解均匀迭加态的归一化状态;$|\beta>$为 M 个解均匀迭加态的归一化状态.则初态$|\phi>$可在$|\alpha>$和$|\beta>$张成的空间中表示为

$$|\phi>=\cos(t)|\alpha>+\sin(t)|\beta>. \quad (5)$$

式中:$t=\arcsin\sqrt{\lambda}$ 经过 R 次 Grover 调用后,初态变为

$$G^R|\phi>=\cos(2R+1)\arcsin\sqrt{\lambda}|\alpha>+\sin((2R+1)\arcsin\sqrt{\lambda})|\beta>.$$

因此,Grover 算法成功搜索的概率为

$$P=\sin^2((2R+1)\arcsin\sqrt{\lambda}). \quad (6)$$

概率曲线如图1所示.

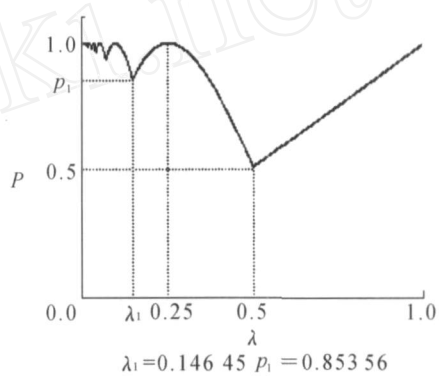


图1 普通 Grover 算法成功搜索概率曲线

Fig. 1 The successful research probability curve of general Grover algorithm

1.3 Grover 算法存在问题及分析

由式(4)、(6)可知,当 $\lambda\in(0.146\,45, 0.50)$ 时,$R=1$;$P_{\lambda=0.146\,45}=0.853\,56$;$P_{\lambda=0.25}=1.00$;$P_{\lambda=0.50}=0.50$.因此,普通 Grover 算法搜索成功概率在 $\lambda=0.25$ 时达到最大,之后迅速下降,在 $\lambda=0.5$ 时降到最低点.之后 $R=0$,算法失效,成功搜索的概率变为 λ.所以,普通 Grover 搜索算法在 $\lambda>0.25$ 之后,不再适用.

出现这种现象的原因在于:算法1)、3)中2次相移的大小相等(均为π);方向相同(均正向).根据文献[3],这样的相位旋转结果是:调用一次 Grover 搜索,使$|\phi>$正向旋转 $\theta=2\arcsin\sqrt{\lambda}$.当 $0\leq\lambda\leq0.25$ 时,将使$|\phi>$逐渐逼近$|\beta>$;当 $\lambda>0.25$ 时,将使$|\phi>$迅速偏离$|\beta>$.

2 Grover 算法的改进策略

根据前节对普通 Grover 量子搜索算法存在问题的分析,可首先将其搜索过程中的2次相位旋转由固定值π推广为任意值,然后通过探索2次相位

旋转的大小与获得正确结果的概率之间的关系,来确定新的相位匹配条件. 沿着这种思路,提出的新的相位匹配条件是:2 次相位旋转的大小相等(均等于 π/2),而方向相反.

2.1　改进算法的相位匹配条件

考察 Grover 算法的 2 个相移算子,写成一般形式为

$$O = I - (1 - e^{i\alpha}) \sum_{m=1}^{M} |\tau_m\rangle\langle\tau_m| . \quad (7)$$

$$U_s = (1 - e^{i\beta}) |\phi\rangle\langle\phi| + e^{i\beta} I. \quad (8)$$

在普通 Grover 算法中,$\alpha = \beta = \pi$. 根据量子力学基本假设[3]:一个封闭量子系统的演化由一个酉变换来刻画. 关于算子(7)、(8)的酉性,提出如下定理.

定理 1　由式(7)、(8)定义的算子都是酉算子.

证明　令 $U = I - (1 - e^{i\alpha}) \sum_{m=1}^{M} |\tau_m\rangle\langle\tau_m|$.

则 $U^+ = I - (1 - e^{-i\alpha}) \sum_{m=1}^{M} |\tau_m\rangle\langle\tau_m|$.

$$U^+ U = I - (2 - e^{i\alpha} - e^{-i\alpha}) \sum_{m=1}^{M} |\tau_m\rangle\langle\tau_m| +$$

$$(1 - e^{i\alpha})(1 - e^{-i\alpha}) \Big(\sum_{m=1}^{M} |\tau_m\rangle\langle\tau_m|\Big)^2 = I.$$

因此,由式(7)描述的算子是酉算子.

令 $V = (1 - e^{i\beta}) |\phi\rangle\langle\phi| + e^{i\beta} I$.

则 $V = (1 - e^{i\beta}) |\phi\rangle\langle\phi| + e^{-i\beta} I$.

$$V^+ V = (1 - e^{-i\beta})(1 - e^{i\beta}) |\phi\rangle\langle\phi| +$$

$$(1 - e^{-i\beta}) e^{i\beta} |\phi\rangle\langle\phi| +$$

$$e^{-i\beta}(1 - e^{i\beta}) |\phi\rangle\langle\phi| + e^{-i\beta} e^{i\beta} I = I.$$

因此,由式(8)描述的算子是酉算子. (证毕)

关于 α、β 的匹配,文献[5]指出,只有在满足 $\alpha = \beta$ 时量子搜索才能成功. 经过研究认为这个结论在 λ 较大时是不必要的. 在 λ 较大时,给出的相位匹配条件可表述为如下定理.

定理 2　当 $\lambda > 1/3$ 时,取 $\alpha = -\beta = \pi/2$,只需一次搜索,获得正确结果的概率 $P \geq 25/27$.

证明　设 $|\tau_1\rangle, |\tau_2\rangle, \cdots, |\tau_m\rangle$ 为 M 个要搜索的目标量子态,$\Omega = \{\tau_1, \tau_2, \cdots, \tau_M\}$. 则系统初始状态可表示为

$$|\phi\rangle = \frac{1}{\sqrt{N}} \Big(\sum_{j=\Omega} |j\rangle + \sum_{k=\bar{\Omega}} |k\rangle \Big) .$$

对于 $|\phi\rangle$,应用式(7)得

$$|\phi'\rangle = \sum_{j=\Omega} \frac{1}{\sqrt{N}} |j\rangle + \sum_{k=\bar{\Omega}} \frac{e^{i\alpha}}{\sqrt{N}} |k\rangle .$$

对于 $|\phi'\rangle$,应用式(8),整理后得

$$|\tilde{\phi}\rangle = ((1 - e^{i\beta}) |\phi\rangle\langle\phi| + e^{i\beta} I) |\phi'\rangle =$$

$$\frac{1}{N\sqrt{N}} \Big(\sum_{j=\Omega} (M(e^{i\alpha} + e^{i\beta} - e^{i(\alpha+\beta)}) + N - M) |j\rangle + \sum_{k=\bar{\Omega}} ((N - M)(e^{i(\alpha+\beta)} - e^{i\beta} + 1) + Me^{i\alpha}) |k\rangle \Big) .$$

令 $p = (N - M)(e^{i(\alpha+\beta)} - e^{i\beta} + 1) + Me^{i\alpha}$,则成功搜索的概率 P 为 $M|p|^2$. 整理后得

$$P = (-4\lambda^3 + 6\lambda^2 - 2\lambda)(\cos\alpha + \cos\beta) +$$
$$(2\lambda^3 - 2\lambda^2)\cos(\alpha - \beta) +$$
$$2\lambda(1 - \lambda)^2 \cos(\alpha + \beta) +$$
$$3\lambda(1 - \lambda)^2 + \lambda^3 .$$

当 $\alpha = -\beta = \pi/2$ 时,上式取得极大值:

$$\tilde{P} = P_{\max} = 4\lambda^3 - 8\lambda^2 + 5\lambda \quad (9)$$

比较式(6)和式(9)有以下结论:

1) 当 $0 < \lambda < 1/3$ 时,$\tilde{P} < P$;

2) 当 $\lambda = 1/3$ 时,$\tilde{P} = P$;

3) 当 $1/3 < \lambda < 1$ 时,$\tilde{P} > P$.

$$\tilde{P}_{1/3<\lambda<1} \geq \tilde{P}_{\lambda=5/6} = 25/27.$$ (证毕)

由定理 2,改进后算法的 2 个相移算子式(7)、(8)具体化为

$$O = I - (1 - i) \sum_{m=1}^{M} |\tau_m\rangle\langle\tau_m| . \quad (10)$$

$$U_s = (1 + i) |\phi\rangle\langle\phi| - iI. \quad (11)$$

改进前后成功搜索的概率曲线如图 2 所示.

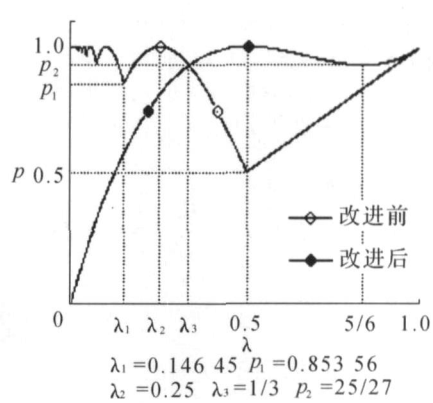


图 2　Grover 算法改进前后成功搜索概率对比

Fig. 2　Comparison of Successful research probability curve between general Grover algorithm and improved ones

从图 2 可以看出,当 $1/3 < \lambda < 1$ 时,改进后的算法明显优于普通 Grover 算法.

2.2　改进后的算法相位旋转的直观图示

关于改进后 Grover 搜索算法的相位旋转,给出了一种直观的几何表示,见图 3.

图中 $|\phi\rangle$、$|\alpha\rangle$、$|\beta\rangle$ 含义见式(5);O 为式(10)描述的相移算子;G 为式(11)描述的相移算子;$\tilde{G}$ 为 $|\alpha\rangle$、$|\beta\rangle$ 面上的投影算子;$\theta = \arcsin\sqrt{\lambda}$;$\theta = \arcsin$

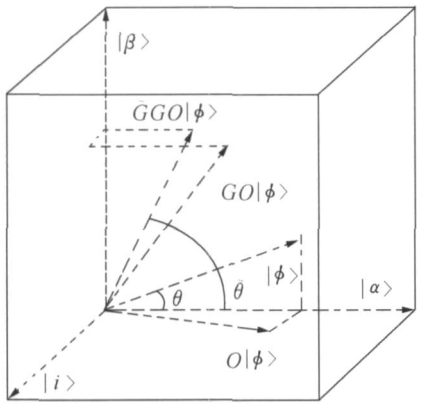


图3 改进后的算法相位旋转的直观图示

Fig. 3 The sketch map of phase rotation for the improved Grover algorithm

$\sqrt{4\lambda^3 - 8\lambda^2 + 5\lambda}$; $i = \sqrt{-1}$. 调用一次算法,相位旋转 $\theta - \theta$. 图3直观示出了搜索过程中相位的变化情况.

2.3 改进后的算法描述

以 $\lambda = 1/3$ 为分界点,分如下2种情况:

1) 若 $1/3 < \lambda \leq 1/3$,使用普通 Grover 搜索.

2) 若 $1/3 < \lambda < 1$,使用改进 Grover 搜索:

Step1 用式(10),使 $|\phi\rangle$ 中目标态的相位正向移动 $\pi/2$;

$$|\theta\rangle = (I - (1 - i)\sum_{m=1}^{M}|\tau_m\rangle\langle\tau_m|)|\phi\rangle$$

Step2 用式(11),使 $|\phi\rangle$ 正向旋转到 $|\tilde{\phi}\rangle$;

$$|\theta\rangle = ((1 + i)|\phi\rangle\langle\phi| - iI)|\theta\rangle.$$

Step3 对 $|\phi\rangle$ 实施测量.

3 算 例

某班有32名同学,学号 $n = 0, 1, \cdots, 31$. 搜索学号满足 $n = \left[\frac{5k+3}{3}\right]$ 的同学. $k = 0, 1 \cdots, 18$; $[\cdot]$ 为按四舍五入取整算符. 目标学号及对应量子比特状态见表1.

此算例中, $N = 32$; $M = 19$; $\lambda = 0.5938$. 取5位量子比特即可满足搜索要求. 5量子比特均匀迭加的初始状态 $|\phi\rangle$ 为

$$|\phi\rangle = \frac{1}{4\sqrt{2}}(|0\rangle + |1\rangle + \cdots + |31\rangle).$$

搜索过程如下:

1) $|\phi\rangle = (I - (1 - i)\sum_{m=1}^{M}|\tau_m\rangle\langle\tau_m|)|\phi\rangle$

$$\frac{1}{4\sqrt{2}}(1i1i\ i1i1\ ii1i\ 1ii1\ i1ii\ 1i1i\ i1i1\ ii1i).$$

2) $|\tilde{\phi}\rangle = ((1 + i)|\phi\rangle\langle\phi| - iI)|\phi\rangle$.

$$\frac{1}{128\sqrt{2}}(abab\ baba\ bbab\ abba\ babb\ abab\ baba\ bbab).$$

式中: $a = -6$; $b = 26 + 32i$.

表1 目标学号及量子比特目标状态

Table 1 The target serial number and its quantum state

k	目标学号	目标状态
0	1	|00001>
1	3	|00011>
2	4	|00100>
3	6	|00110>
4	8	|01000>
5	9	|01001>
6	11	|01011>
7	13	|01101>
8	14	|01110>
9	16	|10000>
10	18	|10010>
11	19	|10011>
12	21	|10101>
13	23	|10111>
14	24	|11000>
15	26	|11010>
16	28	|11100>
17	29	|11101>
18	31	|11111>

3) 正确结果的概率

$$\tilde{P} = 19\left(\left(\frac{26}{128\sqrt{2}}\right)^2 + \left(\frac{32}{128\sqrt{2}}\right)^2\right) = 0.9875.$$

作为对比,用普通 Grover 算法的搜索结果如下:

①$|\phi\rangle = (I - 2\sum_{m=1}^{M}|\tau_m\rangle\langle\tau_m|)|\phi\rangle$

$$\frac{1}{4\sqrt{2}}(1 - 11 - 1 - 11 - 11 - 1 - 11 - 11 - 1 - 11 - 11 - 1 - 11 - 11 - 1 - 11 - 11 - 1 - 11 - 1).$$

②$|\tilde{\phi}\rangle = (2|\phi\rangle\langle\phi| - I)|\phi\rangle$.

$$\frac{1}{32\sqrt{2}}(abab\ baba\ bbab\ abba\ babb\ abab\ baba\ bbab).$$

式中: $a = -11$; $b = 5$.

③正确结果的概率

$$P = 19\left(\frac{5}{32\sqrt{2}}\right)^2 = 0.2319.$$

4 结束语

针对目前 Grover 算法随着目标数增多,搜索概率迅速下降直至算法失效的问题,文中提出了一种新的相位匹配策略,不同于文献[5]的结论,该策略使算法中 2 次相移大小相等方向相反. 该策略较好地解决了目前 Grover 算法中存在的上述问题. 算例证明,该策略是有效的. 在搜索目标较多时如何进一步提高成功搜索的概率,以及如何将 Grover 量子搜索算法与梯度量子遗传算法[11]融合是下一步要解决的问题.

参考文献:

[1]GROVER L K. A fast quantum mechanical algorithm for database search [A]. Proceedings of the 28th Annual ACM Symposium on the Theory of Computing [C]. Pennsylvania, 1996.

[2]SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring[A]. Proceedings of the 35th Annual Symposium on the Foundation of Computer Science [C]. Los Alamitos, 1994.

[3]NIELSEN M A, CHUANG I L. Quantum computation and quantum information [M]. London: Cambridge University Press, 2000.

[4]GROVER L K. Quantum computers can search rapidly by using almost any transformation [J]. Physical Review Letters,1998, 80(29): 4329 - 4332.

[5]LONG G L, LI Y S, ZHANG W L, et al. Phase matching in quantum searching[J]. Physics Letters A,1999, 26(10):27 - 34.

[6]BIHAM E, BIHAM O, BIRON D, et al. Grover's quantum search algorithm for an arbitrary initial amplitude distribution [J]. Physical Review A,1999, 60(4): 2742 - 2745.

[7]BIHAM E, KENIGSBERG D. Grover's quantum search algorithm for an arbitrary initial mixed state [J]. Physical Review A,2002,66(6): 2301 - 2304.

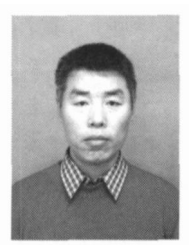
[8]BIHAM O, SHAPIRA D, SHIMONI Y. Analysis of Grover's quantum search algorithm as a dynamical system [J]. Physical Review A,2003, 68(2): 2326 - 2333.

[9]VENTURA D, MARTINEZ T. Quantum associative memory [J]. Information Sciences,2000(124): 273 - 296.

[10]EZHOV A, NIFANOVA A, VENTURA D. Quantum associative memory with distributed queries [J]. Information Sciences,2000(128): 271 - 293.

[11]李士勇, 李盼池. 基于实数编码和目标函数梯度的量子遗传算法[J]. 哈尔滨工业大学学报,2006, 38(8): 1216 - 1218.
LI Shiyong, LI Panchi. A quantum genetic algorithm based on real encoding and gradient information of object function [J]. Journal of Harbin Institute of Technology,2006, 38(8): 1216 - 1218.

作者简介:



李盼池,男,1969 年生,副教授,博士研究生,主要研究方向为量子计算、智能优化算法及其在智能控制、智能信息处理、模式识别等方面的应用. 发表学术论文多篇.

E-mail: lipanchi@vip.sina.com.

李士勇,男,1943 年生,教授,博士生导师,主要研究方向为模糊控制、神经控制、智能控制、智能优化算法、非线性科学与复杂性科学等. 中国自动化学会智能自动化专业委员会委员,《计算机测量与控制》编委. 编著教材与专著共 5 部,在国内外发表学术论文 120 余篇.

E-mail: lsy@hit.edu.cn