迭代次数自适应的 Grover 算法

朱皖宁[1,2],陈汉武[2,3]
(1. 金陵科技学院软件工程学院,江苏南京 211199;2. 东南大学计算机科学与工程学院,江苏南京 210096;
3. 东南大学计算机网络和信息集成教育部重点实验室,江苏南京 210096)

摘 要: 本文提出了利用相位门自动控制 Grover 搜索算法迭代次数的算法. Grover 搜索算法最终得到目标分量的概率非常依赖于酉算子迭代的次数. 迭代次数的计算依赖于目标分量的数量. 因此当目标分量数未知时,该方法无法以高概率测量到目标分量. 在以往的解决方案中需要较高的 Oracle 查询复杂度才能以一定概率得到目标分量的数量. 本文提出了一种通过判断叠加态相位正负性,可自动控制 Grover 搜索算法迭代次数的方法. 只需要添加一个判断相位的门电路,仅增加一次 Oracle 查询次数就可以精确的在最优迭代次数时停止 Grover 搜索算法,在搜索空间较小时可比原算法有更大的概率得到目标分量.

关键词: Grover 搜索算法; 相位正负性; 自动控制
中图分类号: TP387; TN911. 73 **文献标识码:** A **文章编号:** 0372-2112 (2016)12-2975-06
电子学报 URL: http://www. ejournal. org. cn **DOI:** 10. 3969/j. issn. 0372-2112. 2016. 12. 023

Grover Auto-Control Searching Algorithm

ZHU Wan-ning[1,2], CHEN Han-wu[2,3]
(1. *Department of Software Engineering, Jinling Institute of Technology, Nanjing, Jiangsu* 211199, *China*;
2. *Department of Computer Science and Engineering, Southeast University, Nanjing, Jiangsu* 210096, *China*;
3. *Key Laboratory of Computer Network and Information Integration of Ministry of Education, Southeast University, Nanjing, Jiangsu* 210096, *China*)

Abstract: This paper presents an improved Grover searching algorithm which can automatically control the iterative processing when the number of target states is unknown. The probability of success of Grover searching algorithm depends on the number of iteration times and the number of the time of iterations relies on the number of target states. Therefore, it is hard to get the target state with high probability when the number of target states is unknown. To this question, the time complexity of conventional solution is high and the answer is non-deterministic. This paper shows an improved Grover searching algorithm, which is based on the sign for the phases of superposition state. Compared to existing research results, this algorithm can always stop the Grover iterations when the number of iteration times is optimal by the cost where just one more gate, and one more time Oracle call are needed to judge the sign of phase.

Key words: Grover searching algorithm; sign of phase; auto-control

1 引言

量子计算以量子物理学为基本原理,通过对多个量子比特的叠加态进行并行处理,对经典算法的计算速度进行二次加速甚至指数级加速. 对量子计算进行的研究可以追溯到几十年前,但是直到 1994 年,Shor 利用量子傅里叶变换在多项式时间内解决了大数质因子分解算法以后[1],量子计算才开始被关注. 1996 年,Grover 提出了在无结构数据库中进行搜索的算法,在经典的算法复杂度基础上进行了二次加速[2]. NP 问题可以转换为一个多项式时间复杂度的判定问题和一个无结构数据库中的搜索问题. 在经典算法中,求解无结构数据库中的搜索问题需要指数级的时间复杂度. 因此寻求高效无结构数据库搜索算法是加速 NP 问题的关键. 在 Grover 搜索算法被提出后,对 Grover 搜索算法的研究已经有了一定成果[3~11]. 在 Grover 搜索算法在实际问题的应用方面,学者们已经做出了大量有关的研

收稿日期:2015-03-10;修回日期:2016-05-10;责任编辑:梅志强
基金项目:国家自然科学基金(No. 61170321, No. 61502101);高等学校博士学科点专项科研基金(No. 20110092110024);江苏省自然科学基金(No. BK20140651);金陵科技学院高层次人才科研启动基金(No. jit-b-201624)

究.早在2000年时,Zalka等人就已经提出使用Grover搜索算法进行数据库搜索[12];2006年,Yamashita提出了如何在通用编程中使用Grover搜索算法加速程序[13].在最近几年中,国内学者也开始重视Grover搜索算法的应用,例如在2014年,阮越等人提出了基于Grover搜索算法的人脸识别算法,将人脸识别的效率在经典基础上进行了二次加速[14];同年,彭宏等人提出了基于Grover搜索算法的无线量子网络路由算法,可以在限定跳数内搜索出目标路径[15];2015年,孙国栋等人提出了基于Grover搜索算法的量子求根算法,将算法复杂度降低到了$O(\sqrt{M/k})$[16].从大量的文献中可以看出Grover搜索算法的应用面广泛,具有很高的研究价值.

Grover搜索算法构造了一个由Oracle算子和均值反演算子复合而成的Grover算子.将Grover算子进行若干次迭代后进行测量,会以较高的概率输出目标分量.迭代的次数需要选取一个合适的值.无论高于或者低于最优值,测量到目标分量的概率都会下降.根据Grover搜索算法分析,得到目标分量概率最大的迭代次数和目标分量的数量有关.因此必须预先知道目标分量的数量才能有效的使用Grover搜索算法[8].当前对于量子算法的许多研究都是在经典量子算法基础上的应用算法.Grover搜索算法就是一个经典量子算法,因此从Grover搜索算法被提出后,许多著名的量子算法在其之上被陆续提出,例如2003年Shenvi等人提出的基于超立方体上量子行走的一种无结构数据库搜索算法[17],可以看成是在方向空间使用了Grover搜索算法;Aaronson等人将Grover搜索算法嵌入到量子行走中[18],将二维格上的搜索效率提高到了$O(\sqrt{N}\log^2 N)$,三维格上的搜索效率提高到$O(\sqrt{N})$.Ambainis等人又更进一步的发现硬币态在行走时是否变化影响了搜索效率[19],将二维格搜索效率提高到$O(\sqrt{N}\log N)$.Ambainis将这种类型的搜索算法称为Grover-Like搜索算法.2004年,基于这种Grover-Like搜索算法,Ambainis又提出了元素独立性判定算法[20].2005年,在元素独立性算法的基础上,Childs又提出了子集判定算法[21].至今大量的量子算法都是在以上量子算法的基础上研究而成,因此对Grover搜索算法本身的研究可以优化改良很多已有的量子算法.本文重点讨论的是Grover搜索算法的一个很自然的问题:当目标分量数未知时如何使用Grover搜索算法?

当N元问题的目标分量数未知时,需要先确定问题的目标分量数.用经典的方法需要$O(N)$的时间复杂度.至今为止,使用量子计算解决这一问题的方法有两个:(1)使用量子计数,需要$O(\sqrt{N})$的Oracle查询复杂度[9];(2)在文献[8,10]中提出一种逐步测试的方法,但Oracle查询复杂度依然在$O(\sqrt{N/M})$数量级上(这里M为目标分量的数量).即使获得了目标分量的数量,也无法精确的获得最优的迭代次数.可以看到这两种方法都造成了非常大的开销.到目前为止对Grover搜索算法的研究只给出了搜索空间趋向于无穷大时所需迭代次数的精确上界.但是这并不等于给出了最佳的迭代次数,而这又对是否能够以较大概率测量到目标分量产生了至关重要的影响.因此我们需要一种可以在Grover搜索算法迭代到最佳次数时停止的高效的方法.

本文提出了一种基于判定X基下($|\pm\rangle=\{|0\rangle\pm|1\rangle\}$)特定分量相位的正负性的新Grover算法.新算法只需要多一个可逆门和一次Oracle调用,就可以在目标分量未知时仍然可以以最高的概率测量出目标分量.

2 准备知识

Grover搜索算法是由一组酉算子的迭代运算组成.可以简单的由下图表示[9]:

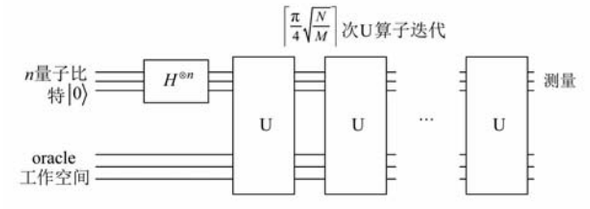

图1 Grover搜索算法线路框架

当n个量子比特初态$|0\rangle^{\otimes n}$经过门$H^{\otimes n}$后变成n量子均匀叠加态,具体变换过程由如下公式表示:

$$|0\rangle^{\otimes n}\xrightarrow{H^{\otimes n}}\frac{1}{(\sqrt{2})^n}(|0\rangle+|1\rangle)^{\otimes n}=\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle \quad (1)$$

其中$N=2^n$.令$|s\rangle$表示初态的均匀叠加态.U算子由一个Oracle决定解(即用一个函数可以表达出解)和一个Grover均值反演算子来增加解的概率.

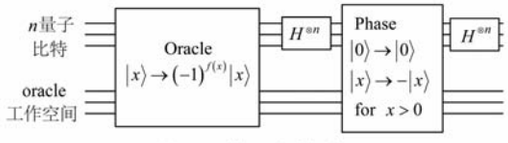

图2 U算子线路框架

如图2所示的Oracle算子令所求目标分量相位翻转:Oracle$=I-2|\varphi\rangle\langle\varphi|$;Grover均值反演算子通过简单计算可以得到如下表示:

$$\begin{aligned}\text{Grover}&=H^{\otimes n}(2|0\rangle\langle 0|-I)^{\otimes n}H^{\otimes n}\\&=2H^{\otimes n}(|0\rangle\langle 0|)^{\otimes n}H^{\otimes n}-H^{\otimes n}I^{\otimes n}H^{\otimes n}\\&=2|s\rangle\langle s|-I\end{aligned} \quad (2)$$

设一共有 M 个目标分量,将均匀叠加态作为初值,经过 $T=\left\lceil\frac{\pi}{4}\sqrt{\frac{N}{M}}\right\rceil$ 次 U 算子的迭代后,对叠加态进行 Z 基投影测量就有至少$\frac{1}{2}$的概率得到目标分量. 这里要注意到的事实是,当迭代次数高于 T 或者低于 T 时,都可能会降低最终得到目标分量的概率,而 T 又依赖于目标分量的个数 M. 那么当不知道目标分量的个数 M 时,就无法获得合适的迭代次数,可能导致得到目标分量的概率明显降低.

在文献[9]中给出了一个 M 未知时的解决方案. 使用 Grover 迭代和基于量子 Fourier 变换的相位估计计数相结合的方法来对 M 进行量子计数,可以在 $\Theta(\sqrt{N})$次 Oracle 查询复杂度下,以 $O(\sqrt{M})$的精度得到 M 的值. 在文献[8,10]中提出了另外一种方法:先给出一个足够大的 k 作为目标分量数量,然后使用 Grover 搜索算法,如果算法失败则降低 k 的值. 毫无疑问这个方法需要调用多次 Grover 搜索算法,因此 Oracle 查询复杂度依然是 $O(\sqrt{N})$.

3　迭代次数自适应的 Grover 搜索算法

每次进行 Grover 算子迭代后,目标分量的幅度都会发生变化. 且可以证明运行最佳迭代次数,目标分量的幅度都会增加,而目标分量的幅度直接影响最终测量出结果的概率. 因此可以通过判断目标分量幅度是否已经最大化,控制 Grover 搜索算法的迭代次数.

定理 1(搜索次数定理)　$T=\left\lceil\frac{\pi}{4}\sqrt{\frac{N}{M}}\right\rceil$ 是 Grover 搜索算法的运算次数上界,当满足 $M\ll N$ 时正好让目标分量的幅度首次达到最大值.

证明:假设一共有 N 个分量,其中 M 个为目标分量. 那么可以将目标分量定义为$|\beta\rangle\equiv\frac{1}{\sqrt{M}}\sum_{x}|x\rangle$. 一般分量定义为$|\alpha\rangle\equiv\frac{1}{\sqrt{N-M}}\sum_{x'}|x'\rangle$. 因此初态可以重新定义为$|\psi\rangle=\sqrt{\frac{N-M}{N}}|\alpha\rangle+\sqrt{\frac{M}{N}}|\beta\rangle$. 将每次 U 算子的迭代看成在以$|\alpha\rangle$相位为横坐标和以$|\beta\rangle$相位为纵坐标的直角坐标系上的一次旋转. 根据 Grover 搜索算法,设初始角度为$\frac{\theta}{2}$,即 $\sin\frac{\theta}{2}=\sqrt{\frac{M}{N}}$,那么每次旋转 θ 角. 因此可以将初态表示为$|\psi\rangle=\cos\frac{\theta}{2}|\alpha\rangle+\sin\frac{\theta}{2}|\beta\rangle$(这里需要注意到一个事实是:Oracle 算子作用在初态上的作用是将平面坐标系上的向量以横坐标做了一次反射,而 Grover 均值反演算子的作用是将这个反射过的向量再以$|\psi\rangle$做反射,因此每次增加的角度都是初始角度的 2 倍[7]). 从而,迭代 k 次 U 算子以后 $U^k|\psi\rangle=\cos\left(k\theta+\frac{\theta}{2}\right)|\alpha\rangle+\sin\left(k\theta+\frac{\theta}{2}\right)|\beta\rangle$. 注意到目标分量的幅度为 $\left|\sin\left(k\theta+\frac{\theta}{2}\right)\right|$. 那么显然目标分量相位首次达到最大值的时候是当 $k\theta+\frac{\theta}{2}\approx\frac{\pi}{2}$. 当 $M\ll N$,可以认为$\frac{\theta}{2}$足够小,即当运行次数 $k\approx\left|\frac{\pi}{2\theta}\right|$时目标分量相位首次达到最大值. 且当 $M\ll N$ 时,有$\frac{\theta}{2}\approx\sin\frac{\theta}{2}=\sqrt{\frac{M}{N}}$,因此$\left\lceil\frac{\pi}{4}\sqrt{\frac{N}{M}}\right\rceil\approx\left\lceil\frac{\pi}{2\theta}\right\rceil$. 因此 Grover 算法执行的次数正好使得目标分量相位首次达到最大值.

定理 2(均值反演定理)　经过均值反演算子作用,叠加态所有分量的相位之和首次变为负值时目标分量的概率幅首次达到最大值.

证明:定义一个一般的量子叠加态为$|\varphi\rangle\equiv\sum_i\alpha_i|i\rangle$,其中假设 α_i 满足归一化. 当 Oracle 算子作用后即可获得新状态$|\varphi'\rangle=\sum_i(-1)^{f(i)}\alpha_i|i\rangle$. 为了研究目标分量相位的变化,可以将目标分量(即令 $f(i)=1$)表示为 $\sum_{i'}-\alpha_{i'}|i'\rangle$,一般分量表示为 $\sum_{i''}\alpha_{i''}|i''\rangle$. 现在将 Grover 均值反演算子作用在新状态$|\varphi'\rangle$上:

$$\begin{aligned}&(2|s\rangle\langle s|-I)\sum_i(-1)^{f(i)}\alpha_i|i\rangle\\&=\frac{2\sum_i(-1)^{f(i)}\alpha_i\langle i|i\rangle]}{N}\sum_i|i\rangle\\&\quad-\left(\sum_{i'}-\alpha_{i'}|i'\rangle+\sum_{i''}\alpha_{i''}|i''\rangle\right)\end{aligned}\tag{3}$$

注意到 $\frac{\sum_i(-1)^{f(i)}\alpha_i\langle i|i\rangle}{N}$ 其实就是所有分量相位的均值,因此可以表示为$\langle\alpha\rangle$. 继续演算:

$$\begin{aligned}&=\sum_{i'}2\langle\alpha\rangle|i'\rangle+\sum_{i''}2\langle\alpha\rangle|i''\rangle\\&\quad-\left(\sum_{i'}-\alpha_{i'}|i'\rangle+\sum_{i''}\alpha_{i''}|i''\rangle\right)\\&=\sum_{i'}(2\langle\alpha\rangle+\alpha_{i'})|i'\rangle+\sum_{i''}(2\langle\alpha\rangle-\alpha_{i''})|i''\rangle\end{aligned}\tag{4}$$

现在我们考察目标分量的相位变化[7,8]:$\alpha'_{i'}=2\langle\alpha\rangle+\alpha_{i'}$

当初始状态为均匀叠加态时,且目标分量的数目 $M\leqslant\frac{N}{2}$,可以很容易发现第一次运算的均值一定非负(若

不满足 $M \leqslant \frac{N}{2}$,则可以直接猜一个解也有大于$\frac{1}{2}$的概率),而且目标分量前的相位也为正.

每次 U 算子运算后,当均值$\langle\alpha\rangle$为正时目标分量相位 $\alpha_{i'}$的相位值都必然会增加. 显然当$\langle\alpha\rangle$首次变化为负值时停止算法可以令 $|\alpha_{i'}|$达到最大值. 而 $\langle\alpha\rangle = \frac{\sum_i (-1)^{f(i)}\alpha_i\langle i \mid i\rangle}{N}$,因此$\langle\alpha\rangle$的负号就由 $\sum_i (-1)^{f(i)}\alpha_i$ 所决定. 所以可以得到经过 Oracle 算子后叠加态所有分量相位之和首次变为负值时目标分量幅度首次达到最大值.

定理 3(相位和定理) 叠加态分量 Z 基下相位和正负性由 X 基下的$|++\cdots+\rangle$分量相位正负性所决定.

证明:这个结果可以很容易的通过变换基底获得. 假设初始基底为 Z 基,即$\{|0\rangle,|1\rangle\}$基. 那么一个 n 量子比特的叠加态总是可以表示为:

$$(\alpha_{00}|0\rangle+\alpha_{01}|1\rangle)(\alpha_{10}|0\rangle+\alpha_{11}|1\rangle)\cdots (\alpha_{(n-1)0}|0\rangle+\alpha_{(n-1)1}|1\rangle) \tag{5}$$

计算这个叠加态的相位和为: $\prod_{i=0}^{n-1}\sum_{j=0}^{1}\alpha_{ij}$.

现在将 Z 基转化为 X 基,即$\{|+\rangle,|-\rangle\}$基,某一量子比特的转换公式可如下表示:

$$(\alpha_{i0}|0\rangle+\alpha_{i1}|1\rangle)\rightarrow \frac{1}{\sqrt{2}}((\alpha_{i0}+\alpha_{i1})|+\rangle+(\alpha_{i0}-\alpha_{i1})|-\rangle) \tag{6}$$

注意到第 i 个$|+\rangle$的相位为$\frac{1}{\sqrt{2}}\sum_{j=0}^{1}\alpha_{ij}$,则$|1++\cdots+\rangle$的分量相位为$\left(\frac{1}{\sqrt{2}}\right)^n\prod_{i=0}^{n-1}\sum_{j=0}^{1}\alpha_{ij}$. 显然$\left(\frac{1}{\sqrt{2}}\right)^n$不影响正负性,因此将 Z 基转化为 X 基后$|++\cdots+\rangle$的分量相位正负性就是 Z 基下的所有分量相位和的正负性.

由于相位正负性可以估测[22,23],所以使用相位检测门 Phase 门,输入为需要进行相位判断的叠加态和一个辅助比特$|\psi\rangle\otimes|\beta\rangle$. 经过 Phase 门后,叠加态$|\psi\rangle$不产生变化. 辅助位根据叠加态在 X 基下$|++\cdots+\rangle$分量前相位 $\phi_{|++\cdots+\rangle}$正负性进行运算:当 $\phi_{|++\cdots+\rangle}$为正时不做任何操作,否则翻转控制端. 显然此电路为可逆电路. Phase 门可以由图 3 所示的线路所表示:

将这个电路加入到 Grover 算法电路的 U 算子中,

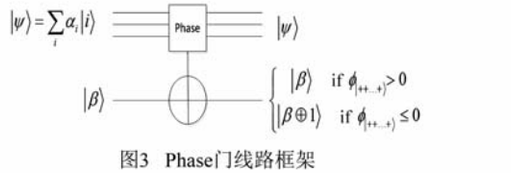

图3 Phase门线路框架

令$|\psi\rangle$为经过 Oracle 算子的叠加态,令$|\beta\rangle = |0\rangle$.

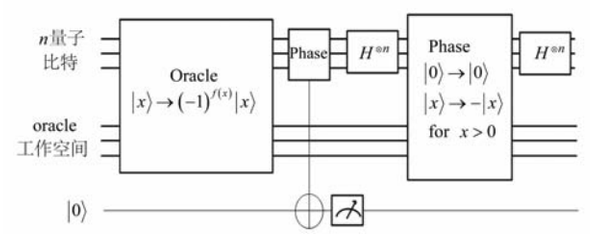

图4 迭代次数自适应的Grover算法电路U算子线路框架

如图 4 所示,每迭代一次 U 算子时,都在运行 Oracle 算子后对辅助位进行一次测量再决定是否进行 Grover 均值反演算子的计算. 当测量结果为$|0\rangle$时继续进行算法迭代,当测量结果为$|1\rangle$时结束算法. 由此嵌入 Phase 门后的 Grover 搜索算法可以自适应的控制 U 算子迭代次数.

当测量结果为$|1\rangle$时,$\phi_{|++\cdots+\rangle}\leqslant0$. 根据定理三可知当 $\phi_{|++\cdots+\rangle}\leqslant0$ 时,叠加态 $\sum_i\alpha_i|i\rangle$的相位和 $\sum_i\alpha_i\leqslant0$,又根据定理二可知相位和首次发生正负性变化时,目标分量的幅度达到最大值. 虽然多调用了一次 Oracle,但是 Oracle 的作用仅仅在于将目标分量相位取反,幅度并没有变化. 因此当测量结果为$|1\rangle$时,目标分量的幅度达到最大值. 相对于原 Grover 算法,本文所展示的算法只增加了一个门电路,且只增加一次 Oracle 查询次数,查询渐进复杂度没有增加.

在定理1 中使用了条件 $M \ll N$,当这个条件不满足的时候,由于$\frac{\theta}{2}<\frac{\pi}{2}$,所以$\frac{\theta}{2}>\sin\frac{\theta}{2}$,因此$\left\lceil\frac{\pi}{4}\sqrt{\frac{N}{M}}\right\rceil>\left\lceil\frac{\pi}{2\theta}\right\rceil$,即$\left\lceil\frac{\pi}{4}\sqrt{\frac{N}{M}}\right\rceil$并不是最佳迭代次数,而是大于最佳迭代次数. 实际上,这个条件在多目标的情况下不满足的可能性很大. 即使是在单目标的情况下,当 N 不足够大时,也不能以最佳迭代次数停止算法. 实际上由于 Grover 迭代计算的是均值,因此当 M 为 N 的一个因子时,其最佳迭代次数和搜索空间为$\frac{N}{M}$的单目标搜索最佳次数是相同的. 但是迭代次数自适应的算法不需要满足 $M \ll N$ 条件,总是可以在目标分量幅度值最大时停止迭代. 下面对原始的 Grover 搜索算法(即迭代次数固定为$\left\lceil\frac{\pi}{4}\sqrt{\frac{N}{M}}\right\rceil$)和迭代次数自适应的 Grover 搜索算法在搜索空间较小的情况下进行了仿真实验:

如图 5 所示,在不满足 $M \ll N$ 的条件下使用迭代次数$\left\lceil\frac{\pi}{4}\sqrt{\frac{N}{M}}\right\rceil$总是比自适应算法迭代次数要多,因

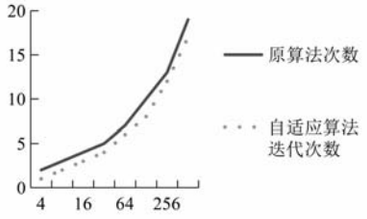

图5　搜索空间从4-512的迭代次数对比

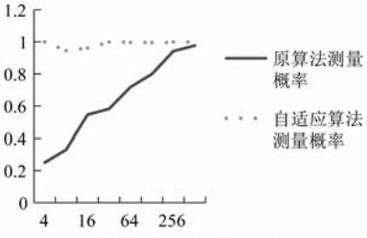

图6　搜索空间从4-512的测量概率对比

此原算法测量到目标分量的概率也就会相应的降低. 如图 6 所示,在 N 较小时,测量到目标分量的概率远低于自适应算法,但是随着 N 逐渐变大,两种算法得到的概率渐渐相等,即在 $M \ll N$ 的情况下,两种算法测量到目标分量的概率会相等.

4　小结

Grover 搜索算法是一种效率极高的无结构数据库量子搜索算法,在经典最好的算法基础上进行了二次加速. Grover 搜索算法是一组酉算子的迭代,其迭代的次数直接影响了最终测量出目标分量的概率,无论是大于或者小于最优次数都有可能导致概率降低. 而最优次数的计算依赖于目标分量的数量 M,当 M 未知时将很难以很高概率测得目标分量. 在以往的解决方案中,有利用量子计数和逐步探测等方法在 M 未知的情况下进行 Grover 计算. 但是这些方法至少需要 $O(\sqrt{N})$ 的 Oracle 查询次数,并且只能以一定概率逼近 M 的值.

本文提出了一种在 M 未知时运行 Grover 算法的解决方案. 利用判断经过 Oracle 后叠加态相位和的正负性,自动控制 Grover 算法酉算子的迭代次数,可以精确在目标分量概率达到最大值时停止算法,并且只加入了一个进行相位判断的门电路,只增加一次 Oracle 查询次数. 不仅如此迭代次数自适应的 Grover 算法在搜索空间较小时会获得更高的概率测量到目标分量. 在近几年来有许多学者对 Grover 算法进行了改进,增加测量出目标分量的概率并减少 Oracle 调用的次数. 这些改进算法并没有改动均值反演算子这个核心,因此本文所述的方法均可以用于这些改进算法.

参考文献

[1] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring[A]. Proceedings of the 35th Annual Symposium on foundations of Computer Science[C]. Santa Fe, NM: IEEE, 1994. 124 – 134.

[2] GroverL K. A fast quantum mechanical algorithm for database search[A]. Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing[C]. Philadelphia, USA: ACM, 1996. 212 – 219.

[3] Grover L K. Quantum mechanics helps in searching for a needle in a haystack[J]. Physical Review Letters, 1997, 79(2): 325 – 328.

[4] Grover L K. Quantum computers can search rapidly by using almost any transformation[J]. Physical Review Letters, 1998, 80(19): 4329 – 4332.

[5] Long G L, Li Y S, Zhang W L, et al. Dominant gate imperfection in Grover's quantum search algorithm[J]. Physical Review A, 2000, 61(4): 042305.

[6] Biron D, Biham O, Biham E, et al. Generalized Grover search algorithm for arbitrary initial amplitude distribution [A]. Quantum Computing and Quantum Communications [C]. Palm Springs, CA: Springer Berlin Heidelberg, 1999. 140 – 147.

[7] Chuang I L, Gershenfeld N, Kubinec M. Experimental implementation of fast quantum searching[J]. Physical Review Letters, 1998, 80(15): 3408 – 3411.

[8] Boyer M, Brassard G, Høyer P, et al. Tight bounds on quantum searching [OL]. arXiv Preprint Quant-ph/9605034, 1996.

[9] Michael A Nielsen, Isaac L Chuang. Quantum Computation and Quantum Information[M]. British: Cambridge University Press, 2000. 240 – 243.

[10] Daniel Reitzner, Daniel Nagaj, Vladimir Buzek. Quantum walks[J]. Acta Physica Slovaca, 2011, 61(6): 603 – 725.

[11] 金文梁,陈向东. 相位不匹配的量子搜索算法[J]. 电子学报,2012,40(1):189 – 192.
Jin Wenliang, Chen Xiangdong. Phase-unmatched quantum search algorithm[J]. Acta Electronica Sinica, 2012, 40(1): 189 – 192. (in Chinese)

[12] Zalka Christof. Using Grover's quantum algorithm for searching actual databases[J]. Physical Review A, 2000, 62(5): 052305 – 052301.

[13] Yamashita S. How to utilize a Grover search in general paogramming[J]. Laser Physics, 2006, 16(4): 730 – 734.

[14] 阮越,陈汉武,刘志昊,等. 量子主成分分析算法[J]. 计算机学报,2014,37(3):666 – 676.
Ruan Yue, Chen Hanwu, Liu Zhihao. Quantum principal

component analysis algorithm [J]. Chinese Journal of Computers,2014,37(3):666 – 676. (in Chinese)
[15] 彭宏,荆晶. 无线自组织量子通信网络的 Grover 路由算法研究[J]. 浙江工业大学学报,2014,42(6):612 – 615.
Peng Hong, Jing Jing. Research on routing algorithm of Grover for wireless ad hoc quantum communication network[J]. Journal of Zhejiang University of Technology, 2014,42(6):612 – 615. (in Chinese)
[16] 孙国栋,苏盛辉,徐茂智. 求根问题的量子计算算法[J]. 北京工业大学学报,2015,41(3):366 – 371.
Sun Guodong, Su Shenghui, Xu Maozhi. Quantum mechanical algorithms for solving root finding problem[J]. Journal of Beijing University of Technology, 2015, 41(3):366 – 371. (in Chinese)
[17] Shenvi N, Kempe J, Whaley R B. A quantum random walk search algorithm [J]. Physical Review A, 2003, 67(5):052307.
[18] Aaronson S, Ambainis A. Quantum search of spatial regions[A]. Proceedings of 44th Annual IEEE Symposium on Foundations of Computer Science [C]. MA, USA: IEEE,2003. 200 – 209.
[19] Ambainis A, Kempe J, Rivosh A. Coins make quantum walks faster[A]. Proceedings of 16th ACM-SIAM SODA [C]. British Columbia, Canada: ACM, 2005. 1099 – 1108.
[20] Ambainis A. Quantum walk algorithm for element distinctness[A]. Proceedings of 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS'04)[C]. Rome, Italy: IEEE,2004. 22 – 31.
[21] Childs A M, Eisenberg J M. Quantum algorithms for subset finding[J]. Quantum Information and Computation, 2005,5(7):593 – 604.
[22] Dorner U, Demkowicz-Dobrzanski R, Smith B J, et al. Optimal quantum phase estimation[J]. Physical Review Letters,2009,102(4):040403.
[23] Hradil Z. Phase measurement in quantum optics [J]. Quantum Optics: Journal of the European Optical Society Part B,1992,4(2):93 – 110.

作者简介

朱皖宁 男,1983 年生,安徽淮南人,博士,主要研究领域为量子计算与量子可逆逻辑综合.
E-mail: granny025@163.com

陈汉武 男,1955 年生,江苏南京人,博士,教授,主要研究领域为量子信息与量子计算技术.
E-mail: hanwu_chen@163.com