

# 相位不匹配的量子搜索算法

金文梁, 陈向东

(西南交通大学信息科学与技术学院, 四川成都 610031)

**摘要:** 当搜索空间局限在二维复子空间中时, 如果无序数据库中的总个数足够大, 那么倘若任意的两个完全独立的相位旋转角集合(但其中一个集合中元素的个数相对于无序数据库中的总个数相对较小)满足多相位匹配方程, 则仍然能以较高的成功概率找到唯一的目标态. 本文针对一种带有特定前提条件的量子搜索问题, 说明了可通过结合多相位匹配方程和经典的穷举算法以使得该目标态能以几乎接近 100% 的成功概率找到. 最后给出了一个实例.

**关键词:** Grover 量子搜索算法; 二维复子空间; 多相位匹配方程; 穷举算法

**中图分类号:** TP301.6      **文献标识码:** A      **文章编号:** 0372-2112 (2012) 01-0189-04

**电子学报 URL:** <http://www.ejournal.org.cn>

**DOI:** 10.3969/j.issn.0372-2112.2012.01.031

## Phase-Unmatched Quantum Search Algorithm

JIN Wen-liang, CHEN Xiang-dong

(School of Information Science and Technology, Southwest Jiaotong University, Chengdu, Sichuan 610031, China)

**Abstract:** For the case when the search space is confined to a two-dimensional complex subspace, if the total number of an unsorted database is sufficiently large, then a unique desired state can still be found with high success probability provided any two sets of phase rotation angles, which are completely independent (unrelated to each other) but the number of elements in one of the sets is relatively small compared to the total number of an unsorted database, satisfy the multiphase matching equation. In this paper we showed that for a quantum search problem with some specific requirements, one may combine the multiphase matching equation and the classical exhaustive algorithm such that a unique desired state can be found with success probability almost close to unity. Finally, we gave a numerical example.

**Key words:** Grover quantum search algorithm; two-dimensional complex subspace; multiphase matching equation; exhaustive algorithm

## 1 引言

在一个大型无序数据库中, Grover 量子搜索算法<sup>[1]</sup>能以数量级为  $O(\sqrt{N})$  的查找次数找到唯一的目标态. 该算法已被证明为最优<sup>[2,3]</sup>且有多方面的应用<sup>[4,5]</sup>. 迄今为止主要是从以下的方面对该量子搜索算法进行了扩展: (1) 假设有多个目标态<sup>[6,7]</sup>; (2) 以任意的酉变换来代替 Walsh-Hadamard 变换<sup>[7,8]</sup>; (3) 引入了概率幅扩大的思想<sup>[7,9]</sup>; (4) 通过并行的量子计算方式来进一步降低搜索次数<sup>[10,11]</sup>; (5) 以任意的相位旋转代替反方向的相位旋转<sup>[12]</sup>; (6) 初始态是任意的复概率幅分布, 而不再是等概率幅分布<sup>[13,14]</sup>; (7) 讨论了任意的纠缠初始态<sup>[15]</sup>; (8) 将量子搜索空间由二维复子空间扩展至三维复子空间<sup>[16]</sup>.

原先的 Grover 量子搜索算法<sup>[1]</sup>是不能以 100% 的概率找到唯一的目标态的. 为确保以 100% 的概率找到该目标态, 在二维复子空间条件下国内外的研究工作者给

出了不同形式的相位旋转角公式<sup>[12,17,18]</sup>. 我们证明了在三维复子空间情形下(指偏角  $0 < \psi < \pi/2$ ), 初始量子纯态无论以何种形式出现目标态都不能以 100% 的概率找到, 但只要无序数据库中总个数  $N$  足够大, 那么对应于两个相位旋转角相等的情形( $\phi = \theta \in (0, \pi)$ ), 找到目标态的最大成功概率近似等于  $\cos^2 \psi$ <sup>[16]</sup>. 本文中, 我们进一步指出当搜索空间局限在二维复子空间中时(对应于偏角  $\psi = 0$ ), 即便每次叠代的两个相位旋转角都不相等( $\phi_j \neq \theta_j, 1 \leq j \leq k, k \geq 2$ )且每个相位对  $\{\phi_j, \theta_j\}$  彼此独立, 如果整数  $k$  的值相对于总个数  $N$  较小且满足多相位匹配方程( $\sum_{j=1}^k \theta_j = \sum_{j=1}^k \phi_j = \Delta, \Delta$  为任意实数), 则仍然能以较高的成功概率找到唯一的目标态(文献[19]只讨论了  $k=2$  的情况). 相位匹配公式  $\phi = \theta$ <sup>[12]</sup>是多相位匹配方程的一个特例. 文献[20]指出如果设定  $\theta = \pi$ , 那么对任意固定的针对目标态的相位旋转角  $\phi \in (0, \pi)$  这种情形, 量子搜索算法是失效的. 但是如果相位旋转角

$\phi$  不固定,即对于任意给定的定义在实数域  $\mathbf{R}$  上的相位旋转角集合  $\{\phi_k, \phi_{k-1}, \dots, \phi_1\}$ , 如果其满足  $\sum_{j=1}^k \phi_j = k\pi$ , 则可通过穷举算法对该集合  $\{\phi_k, \phi_{k-1}, \dots, \phi_1\}$  作出进一步修正后, 最终却是能够以几乎接近 100% 的成功概率找到目标态的. 最后通过一个具体的实例阐明了这点.

## 2 二维酉矩阵表象

假设量子系统的初始叠加态(纯态)为

$$|\gamma_0\rangle = \sum_{x=0}^{N-1} c_x |x\rangle = \cos\beta_0 |\alpha\rangle + \sin\beta_0 e^{i\zeta} |\beta\rangle \quad (1)$$

其中  $\zeta$  是任意实数,  $\{c_0, c_1, \dots, c_{N-1}\}$  是一组不全为 0 的任意复数集合且满足归一化条件

$$\sum_{x=0}^{N-1} |c_x|^2 = 1$$

$$|\alpha\rangle = \frac{1}{\sqrt{\sum_{x \in \bar{Y}} |c_x|^2}} \sum_{x \in \bar{Y}} c_x |x\rangle \quad (2)$$

$$|\beta\rangle = \frac{e^{-i\zeta}}{\sqrt{\sum_{x \in Y} |c_x|^2}} \sum_{x \in Y} c_x |x\rangle$$

$$\beta_0 = \arcsin\left(\sqrt{\sum_{x \in Y} |c_x|^2}\right) > 0$$

符号  $\bar{Y}$  和  $Y$  分别表示非目标态和目标态的集合(在本文中我们假设目标态的个数为  $M$ , 并且  $\beta_0$  的值较小).

对任意给定的两个不为  $2k'\pi$  ( $k'$  为任意整数)的实数  $\phi$  和  $\theta$  (两个相位旋转角), 定义以下两个酉算子

$$U_\phi = I + (e^{i\phi} - 1) \sum_{x \in \bar{Y}} |x\rangle\langle x| \quad (3)$$

$$U_\theta = I + (e^{i\theta} - 1) |\eta\rangle\langle \eta| \quad (4)$$

其中  $i = \sqrt{-1}$ ,  $|\eta\rangle$  是由所有的目标态和非目标态所张成的  $N$  维复 Hilbert 空间中的一个单位向量且满足下面的关系式(6). 则 Grover 算子  $G = -AU_\theta A^{-1}U_\phi$  ( $A$  是任意的酉算子,  $A^{-1}$  是  $A$  的逆算子)可以表示为

$$G = -(I + (e^{i\theta} - 1) |\mu\rangle\langle \mu|) (I + (e^{i\phi} - 1) \sum_{x \in \bar{Y}} |x\rangle\langle x|) \quad (5)$$

$I$  表示单位算子,

$$|\mu\rangle = A|\eta\rangle \quad (6)$$

如果  $|\mu\rangle \in L$ , 那么  $|\mu\rangle$  可以表示成下面最一般的情形

$$|\mu\rangle = e^{it_1} \cos t_2 |\alpha\rangle + \sin t_2 e^{it_2} |\beta\rangle \quad (7)$$

$L$  表示由正交基  $\{|\alpha\rangle, |\beta\rangle\}$  所张成的二维复平面,  $0 < t \leq \beta_0$ ,  $t_1, t_2 \in \mathbf{R}$ .

根据等式(5)和(7), 通过计算得到

$$G[|\alpha\rangle, |\beta\rangle] = [|\alpha\rangle, |\beta\rangle] Q \quad (8)$$

上式中

$$Q = - \begin{pmatrix} Q_{11} & Q_{12} \\ Q_{21} & Q_{22} \end{pmatrix} \quad (9)$$

$$Q_{11} = e^{i\theta} \cos^2 t + \sin^2 t$$

$$Q_{12} = e^{i\phi} e^{-i\Lambda} (e^{i\theta} - 1) \frac{\sin(2t)}{2}$$

$$Q_{21} = (e^{i\theta} - 1) e^{i\Lambda} \frac{\sin(2t)}{2}$$

$$Q_{22} = e^{i\phi} (e^{i\theta} \sin^2 t + \cos^2 t)$$

参数  $\Lambda = t_2 - t_1$ .

## 3 穷举法在量子搜索中的应用

对任意的整数  $k \geq 2$ , 首先定义算子

$$\tilde{G}_k = G(\phi_k, \theta_k) G(\phi_{k-1}, \theta_{k-1}) \cdots G(\phi_1, \theta_1) \quad (10)$$

那么有下面的结论.

**定理 1** 假设  $N$  较大. 对定义在实数域  $\mathbf{R}$  上的两个任意集合  $\{\theta_k, \theta_{k-1}, \dots, \theta_1\}$  和  $\{\phi_k, \phi_{k-1}, \dots, \phi_1\}$ , 如果满足多相位匹配方程

$$\sum_{j=1}^k \theta_j = \sum_{j=1}^k \phi_j = \Delta \quad (11)$$

那么总能够通过选择合适的  $k \geq 2$  ( $k$  相对于  $N$  较小) 和  $n \geq 1$  以使得初始态  $|\gamma_0\rangle$  在算子  $(\tilde{G}_k)^n$  作用下以较高的成功概率找到一个目标态.

这个定理可以首先通过忽略式(9)中  $t$  的高阶项, 然后对式(10)中的  $k$  施以数学归纳法的方式来证明, 即  $k$  的值从 2 开始直至任意一个相对于  $N$  较小的正整数, 上述结论都成立. 由于其证明过程需要占用较大的篇幅, 我们在这里不打算给出其详细的证明过程. 我们的重点在于阐明由下面所给出的具体实例(见表 1 和图 1)是如何得到的, 从而表明当  $\theta_k = \theta_{k-1} = \dots = \theta_1 = \pi$ , 通过利用多相位匹配方程并结合穷举算法能够得到一组满足条件  $\{\phi_j \neq \pi, 1 \leq j \leq k\}$  且  $\phi_k \neq \phi_{k-1} \neq \dots \neq \phi_1$  的数值以使得接近于 100% 的成功概率找到目标态. 这同时也表明了要从理论上以接近 100% 的成功概率找到一个目标态并不一定需要遵从相位匹配条件  $\phi = \theta$ <sup>[12]</sup>. 如果令  $\phi_j = \theta_j = \sigma \in (0, \pi]$ ,  $1 \leq j \leq k$ , 那么显然该相位匹配条件  $\phi = \theta$  实际上就是式(11)的一个特例.

为简单起见, 假设  $n = 1, M = 1, \beta_0 = \arcsin(\sqrt{1/N})$ . 经过对初始态  $|\gamma_0\rangle$  的  $j$  ( $1 \leq j \leq k$ ) 次叠代作用, 从等式(1), (8)和(9)得到

$$\begin{pmatrix} u_j \\ d_j \end{pmatrix} = Q(\phi_j, \theta_j) Q(\phi_{j-1}, \theta_{j-1}) \cdots Q(\phi_1, \theta_1) \times \begin{pmatrix} \cos(\beta_0) \\ \sin(\beta_0) e^{i\zeta} \end{pmatrix} \quad (12)$$

则找到目标态的成功概率  $P_j = |d_j|^2$ . 现在具体结合表 1 中所设定的参数来说明如何运用多相位匹配方程并结合经典的穷举算法以获得几乎接近 100% 的成功概率

找到目标态. 为保证足够高的精度, 我们在 MATLAB 环境下保留了小数点后 14 位有效数字.

**第一步** 设定各项必要的参数并初始化  $\theta_{24} = \theta_{23} = \dots = \theta_1 = \pi$ .  $\phi_{23}, \phi_{22}, \dots, \phi_1$  的数值由计算机系统随机产生并使  $\phi_{24} = 24\pi - \sum_{j=1}^{23} \phi_j$ , 接着检验条件  $P_{j=24} = |d_{j=24}|^2 > 0.9$  是否满足. 如满足则转入下一步, 否则重新按上述方式确定  $\phi_{24}, \phi_{23}, \dots, \phi_1$  的数值.

**第二步** 首先赋值  $\phi'_{24} \leftarrow \phi_{24} \leftarrow \phi_{24} - \pi/50$ , 然后使  $\phi_{24}$  的值每次以增量 0.0001 的方式递增至  $\phi'_{24} + \pi/25$ , 同时每次都计算出新的  $P_{j=24}$  值并与上次记录的  $P_{j=24}$  值进行比较, 如果目前的  $P_{j=24}$  值比上次记录的  $P_{j=24}$  值大则同时更新上次记录的  $\phi_{24}$  和  $P_{j=24}$  值.

**第三步** 对  $\{\phi_j, j = 23 \rightarrow 1\}$  的情形重复第二步.

**第四步** 如果现在的  $P_{j=24}$  值已经几乎接近于 1 那么就终止程序的运行, 否则转至第二步.

按照上述算法, 最后我们列出了表 1 中的其中一组数据.

表 1 相位不匹配时仍以几乎接近 100% 的成功概率找到目标态的一个实例

$n = 1, N = 100, M = 1, k = 24,$			
$t = \beta_0 = \arcsin(0.1), \Delta = 2\pi/3, \zeta = \pi/4$			
$j$	$\phi_j$	$\theta_j = \pi$	$P_j$
1	2.74693546171360	3.14159265358979	0.04366720905957
2	0.39828214016856	3.14159265358979	0.00054554900806
3	2.48833695270913	3.14159265358979	0.04236514463243
4	1.73964289056824	3.14159265358979	0.10042469718810
5	0.58043353704706	3.14159265358979	0.01566909697381
6	4.45838129862463	3.14159265358979	0.02889814813813
7	3.94062881006929	3.14159265358979	0.13113440664562
8	2.26321781589114	3.14159265358979	0.24991790499712
9	2.24415685987322	3.14159265358979	0.28072174486909
10	1.00275699685193	3.14159265358979	0.13012427131784
11	2.75632915768029	3.14159265358979	0.06581602684862
12	6.05617274918125	3.14159265358979	0.10865748067297
13	4.36972813166616	3.14159265358979	0.25520219912522
14	4.05749371815842	3.14159265358979	0.34617385077964
15	3.89135508767492	3.14159265358979	0.32873877913832
16	3.64438547831505	3.14159265358979	0.25064081311826
17	0.05998018813862	3.14159265358979	0.33814365765471
18	3.86135920128299	3.14159265358979	0.52848663455115
19	3.18486364339076	3.14159265358979	0.71631782902581
20	3.29347389448605	3.14159265358979	0.87429387628613
21	3.49908183896486	3.14159265358979	0.97040478005902
22	1.43286253370092	3.14159265358979	0.95485558950199
23	0.15138778378410	3.14159265358979	0.96039946932160
24	13.71855915018830	3.14159265358979	0.99999999999600
$\Sigma$	75.83980532012950	75.39822368615504	

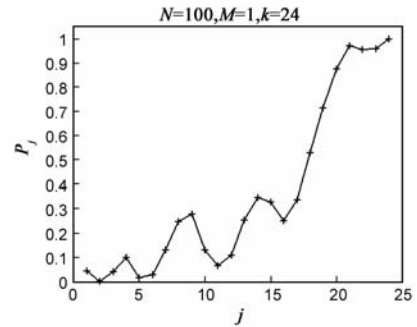


图 1 表 1 中成功概率和叠代次数的关系曲线图

## 4 结束语

本文将经典穷举算法引入到了 Grover 量子搜索算法中. 通过一个具体的实例表明, 将多相位匹配方程  $\sum_{j=1}^k \theta_j = \sum_{j=1}^k \phi_j = \Delta$  和穷举算法两者相结合可以有效地解决某些带有特定前提条件的量子搜索问题. 这样就进一步扩大了 Grover 量子搜索算法的适用性范围. 在实际工作中, 无论是理论研究还是工程计算都经常会遇到这样的问题: 人们能够证明某类问题的精确解的存在, 但却很难用具体的公式将这些精确解完整地表示出来. 对待这类问题可视不同的具体情况, 采用穷举算法或许能给我们带来一定的启迪 (最终目的是为了进一步提高精度). 实际上这种思想对于解决量子遗传算法中有关量子旋转门调整策略操作<sup>[21,22]</sup>也是有所裨益的.

**致谢** 作者感谢审稿专家提出的宝贵意见和编辑老师所给予的帮助!

## 参考文献

- [1] L K Grover. Quantum mechanics helps in searching for a needle in a haystack[J]. Physical Review Letters, 1997, 79(2): 325 - 328.
- [2] C H Bennett, E Bernstein, et al. Strengths and weaknesses of quantum computing[J]. SIAM Journal on Computing, 1997, 26(5): 1510 - 1523.
- [3] C Zalka. Grover's quantum searching algorithm is optimal[J]. Physical Review A, 1997, 60(4): 2746 - 2751.
- [4] 徐文旭, 廖明宏. 最长公共子序列的量子算法[J]. 电子学报, 2007, 35(12A): 99 - 103.  
Xu Wen-xu, Liao Ming-hong. Quantum algorithm for longest common subsequence [J]. Acta Electronica Sinica, 2007, 35(12A): 99 - 103. (in Chinese)
- [5] 鲍皖苏, 宋晨, 钟普查, 付向群. 子集和问题的量子中间相遇搜索算法[J]. 电子学报, 2011, 39(1): 128 - 132.  
Bao Wan-su, Song Chen, Zhong Pu-cha, Fu Xiang-qun. Quantum mechanical meet-in-the-middle algorithm for subset sum problem[J]. Acta Electronica Sinica, 2011, 39(1): 128 - 132.

(in Chinese)

- [6] M Boyer, G Brassard, et al. Tight bounds on quantum searching [J]. *Fortschritte Der Physik-progress of Physics*, 1996, 46(4-5): 493-506.
- [7] L K Grover. Quantum computers can search rapidly by using almost any transformation [J]. *Physical Review Letters*, 1998, 80(19): 4329-4332.
- [8] G Brassard, P Hoyer, et al. Quantum counting [J]. *Lecture Notes in Computer Science*, 1998, 1443: 820-831.
- [9] G Brassard, P Hoyer, et al. Quantum amplitude amplification and estimation [DB/OL]. <http://arxiv.org/abs/Quant-ph/0005055v1>, 2000.
- [10] Y Ozhigov. Speedup of iterated quantum search by parallel performance [DB/OL]. <http://arxiv.org/abs/Quant-ph/9904039v4>, 1999.
- [11] R Gingrich, C P Williams, et al. Generalized quantum search with parallelism [J]. *Physical Review A*, 2000, 61(5): 1-8.
- [12] G L Long, Y S Li, et al. Phase matching in quantum searching [J]. *Physics Letters A*, 1999, 262(1): 27-34.
- [13] E Biham, O Biham, et al. Grover's quantum search algorithm for an arbitrary initial amplitude distribution [J]. *Physical Review A*, 1999, 60(4): 2742-2745.
- [14] E Biham, O Biham, et al. Analysis of generalized Grover quantum search algorithms using recursion equations [J]. *Physical Review A*, 2000, 63(1): 2742-2749.
- [15] A Carlini, A Hosoya. Quantum computers and unstructured search: Finding and counting items with an arbitrarily entangled initial state [J]. *Physics Letters A*, 2001, 280(3): 114-120.
- [16] W L Jin, X D Chen. A desired state can not be found with certainty for Grover's algorithm in a possible three-dimensional complex subspace [J]. *Quantum Information Processing*, 2011, 10(3): 419-429.
- [17] G L Long, L Xiao, et al. General phase matching condition for quantum searching [DB/OL]. <http://arxiv.org/abs/quant-ph/0107013>, 2001.
- [18] P Hoyer. Arbitrary phases in quantum amplitude amplification [J]. *Physical Review A*, 2000, 62(5): 1-5.
- [19] A Tulsı. Quantum computers can search rapidly by using almost any selective transformation [J]. *Physical Review A*, 2008, 78(2): 4329-4332.
- [20] G L Long, W L Zhang, et al. Arbitrary phase rotation of the marked state can not be used for Grover's quantum search algorithm [J]. *Communications in Theoretical Physics*, 1999, 32(3): 335-338.
- [21] 杨俊安, 庄镇泉, 史亮. 多宇宙并行量子遗传算法 [J]. *电子学报*, 2004, 32(6): 923-928.  
Yang Jun-an, Zhuang Zhen-quan, Shi Liang. Multi-universe parallel quantum genetic algorithm [J]. *Acta Electronica Sinica*, 2004, 32(6): 923-928. (in Chinese)
- [22] 熊焰, 陈欢欢, 苗付友, 王行甫. 一种解决组合优化问题的量子遗传算法 QGA [J]. *电子学报*, 2004, 32(11): 1855-1858.  
Xiong Yan, Chen Huan-huan, Miao Fu-you, Wang Xing-fu. A quantum genetic to solve combinatorial optimization problem [J]. *Acta Electronica Sinica*, 2004, 32(11): 1855-1858. (in Chinese)

#### 作者简介



金文梁 男, 1968 年 12 月出生于浙江绍兴, 博士, 从事量子信息论和量子算法方面的研究.

E-mail: wenliang20021@yahoo.cn

陈向东 男, 1967 年 5 月出生于江西宜春, 教授、博士生导师, 从事传感器应用方面的研究.