

量子搜索算法的多相位关系研究

金文梁

(扬州大学信息工程学院 江苏 扬州 225127)

摘 要 假设给定一个总数为 N 的无序数据库, 极其复杂的计算使得几乎不可能建立一个精确的数学公式来描述这个结论: 在二维复子空间中, 对于一个等幅分布的初始态, 存在两个定义在实数域上的相位旋转角集合以使得唯一的目标态能以 100% 的成功概率找到; 文中采取了一种近似的计算方法, 通过归纳法推导出了多相位匹配方程. 倘若其中一个相位旋转角集合中的元素个数 j 相对于 N (N 足够大) 较小, 则该方程就能保证唯一的目标态以较高的成功概率找到. 接着, 通过文中推导出的一个递推关系式, 对任意给定的 $j > 2$, 分析了 Long 算法的计算复杂性. 最后, 通过一些数值模拟的实例进一步验证了多相位匹配方程的有效性.

关键词 Grover 量子搜索算法; Long 算法; Long 算子; 二维复子空间; 多相位匹配方程

中图法分类号 TP301 **DOI 号:** 10.3724/SP.J.1016.2012.01440

Investigation of Multiphase Relationship for Quantum Search Algorithm

JIN Wen-Liang

(College of Information Engineering, Yangzhou University, Yangzhou, Jiangsu 225127)

Abstract Suppose we are given an unsorted database of size N . Whereas the extremely complicated calculations make it almost impossible to establish a precise mathematical formulation to describe the conclusion that for a uniform initial amplitude distribution, there exist two sets of the phase rotation angles defined in the real domain such that a unique desired state can be found with certainty in a two-dimensional complex subspace, we resorted to an approximate computational method for simplifying the calculations and thus derived the multiphase matching equation by induction. This equation guarantees that a unique desired state can be found with high success probability provided the number j of elements in one of the sets of the phase rotation angles is relatively small compared to N (N is sufficiently large). In this case, for any given $j > 2$, we analyze the computational complexity of Long algorithm by exploiting a recurrence relation derived in this paper. Finally, we further verify the validity of the multiphase matching equation by some examples of numerical simulation.

Keywords Grover quantum search algorithm; Long algorithm; Long operator; two-dimensional complex subspace; multiphase matching equation

1 引 言

在一个大型无序数据库中, 原先的 Grover 量子搜索算法^[1]能以数量级为 $O(\sqrt{N})$ 的叠代次数找到

唯一的目标态. 并且该算法已经被证明是最优的^[2-3]. 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^[4-5]; (2) 以任意的酉变换来代替 Walsh-Hadamard 变换^[5-6]; (3) 引入了概率幅扩大的思想^[5,7]; (4) 通过并行的

量子计算方式来进一步降低搜索次数^[8]; (5) 以任意的相位旋转代替反方向的相位旋转^[9] (这种推广的量子搜索算法称之为 Long 算法并给出了相位匹配条件 $\theta=\phi$); (6) 初始态是任意的复概率幅分布, 而不再是等概率幅分布^[10-11]; (7) 讨论了任意的纠缠初始态^[12]; (8) 将量子搜索空间由二维复子空间扩展至三维复子空间^[13].

原先的 Grover 量子搜索算法^[1] 不能以 100% 的概率找到唯一的目标态. Long 等人^[14] 首先指出相位不匹配不能构造量子搜索算法. 为确保以 100% 的概率找到所指定的目标态, 在二维复子空间条件下国内外的工作者给出了不同形式的相位旋转角公式^[9,15-17]. 相位匹配在三维空间中有一个直观的几何解释, 这在文献^[18]中已给出. 相位匹配已经被 3 个实验所证实^[19-21]. 在文献^[22]中, Long 等人对有关量子搜索算法作了全面详尽的论述. 此外, Li 等人^[23] 指出 Long 算法中的算子 $Q = -I_\tau U^{-1} I_\tau U$ 中的 U^{-1} (U^{-1} 是 U 的逆算子) 可被任意的酉算子 V 所代替, 即 $Q = -I_\tau U^{-1} I_\tau U$ 可写成 $Q = -I_\tau V I_\tau U$ 的形式. 我们证明了在三维复子空间情形下 (指偏角 $0 < \psi < \pi/2$), 初始态 (纯态) 不管以何种形式出现, 目标态都不能以 100% 的概率找到^[13]; 但是只要无序数据库中总个数 N 足够大, 那么在满足相位匹配条件 $\theta=\phi \in (0, \pi]$ 的条件下找到目标态的最大成功概率近似等于 $\cos^2 \psi$ ^[13,24]. 本文提出了这样一个推测, 即在二维复子空间中, 如果无序数据库中总的个数 N 足够大 (这里假设只有一个目标态, 初始态为平均叠加态) 且正整数 j ($j \geq 2$) 的值相对于 N 而言较小, 那么对定义在实数域 $\mathbb{R}$ 上的两个任意相位角集合 $\{\theta_j, \theta_{j-1}, \dots, \theta_1\}$ 和 $\{\phi_j, \phi_{j-1}, \dots, \phi_1\}$, 如果满足

多相位匹配方程 $\sum_{m=1}^j \theta_m = \sum_{m=1}^j \phi_m$, 则能以较高的成功概率找到目标态 (在文献^[25]中只讨论了 $j=2$ 的情形). 这个结论的有效性由下面的一个工作提供了支持: Long 等^[26] 发现在量子搜索算法中, 相位系统误差是主要误差, 这样的结果导致两个相位转角的累积和不同, 而随机误差不重要, 这样导致两个相角的累计和基本相等.

2 二维酉矩阵表象

假设量子系统中目标态和非目标态的总个数 N 足够大, 要找的唯一目标态是 $|\tau\rangle$. 单位矢量 $|\alpha\rangle$ 定义为

$$|\alpha\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq \tau} |x\rangle \quad (1)$$

任意给定两个不为 $2k'\pi$ (k' 为任意整数) 的实数 ϕ 和 θ (两个相位旋转角), 定义以下两个酉算子

$$U_\phi = I + (e^{i\phi} - 1) |\tau\rangle\langle\tau| \quad (2)$$

$$U_\theta = I + (e^{i\theta} - 1) |\eta\rangle\langle\eta| \quad (3)$$

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 (5), 那么 Long 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) 可表示为

$$G = -(I + (e^{i\theta} - 1) |\mu\rangle\langle\mu|) (I + (e^{i\phi} - 1) |\tau\rangle\langle\tau|) \quad (4)$$

I 表示单位算子,

$$|\mu\rangle = A |\eta\rangle \quad (5)$$

如果 $|\mu\rangle \in L$ (L 表示由正交基 $\{|\alpha\rangle, |\tau\rangle\}$ 所张成的二维复平面), 那么 $|\mu\rangle$ 可以表示成下面最一般的情形

$$|\mu\rangle = e^{i\gamma_1} \cos t |\alpha\rangle + \sin t e^{i\gamma_2} |\tau\rangle \quad (6)$$

$t_1, t_2 \in \mathbb{R}$, $0 < t \leq \beta_0$, 其中

$$\beta_0 = \arcsin(\sqrt{1/N}) \quad (7)$$

根据式 (4) 和 (6), 通过计算可得到

$$G\{|\alpha\rangle, |\tau\rangle\} = \{|\alpha\rangle, |\tau\rangle\} Q \quad (8)$$

上式中

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

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

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

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

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

参数 $\Delta = t_2 - t_1$.

3 Long 算法的多相位匹配问题

对任意给定的两个集合 $\{\theta_j, \theta_{j-1}, \dots, \theta_1\}$ 和 $\{\phi_j, \phi_{j-1}, \dots, \phi_1\}$ ($j \geq 2$), 定义算子

$$\tilde{G}_j = G(\phi_j, \theta_j) G(\phi_{j-1}, \theta_{j-1}) \cdots G(\phi_1, \theta_1) \quad (10)$$

此算子 $\tilde{G}_j$ 在基 $\{|\alpha\rangle, |\tau\rangle\}$ 下所对应的矩阵形式是

$$\tilde{Q}_j = Q(\phi_j, \theta_j) Q(\phi_{j-1}, \theta_{j-1}) \cdots Q(\phi_1, \theta_1) \quad (11)$$

该酉矩阵 $\tilde{Q}_j$ 最终可表示成下面包含 4 个实参数的最一般的矩阵形式

$$\tilde{Q}_j = \begin{bmatrix} \cos(\Phi_j) e^{i\alpha_j} & \sin(\Phi_j) e^{i\gamma_j} \\ -\sin(\Phi_j) e^{i(\beta_j - \gamma_j)} & \cos(\Phi_j) e^{i(\beta_j - \alpha_j)} \end{bmatrix} \quad (12)$$

$\Phi_j, \alpha_j, \beta_j, \gamma_j$ 为 4 个实参数 (任意的一个二阶酉矩阵都可以表示成式 (12) 的形式, 参见文献^[27]中等

式(5.50)). 当 $\alpha_j = \beta_j - \alpha_j$ 时, 式(12)可简化为

$$\tilde{Q}_j = e^{i\alpha_j} \begin{pmatrix} \cos(\Phi_j) & \sin(\Phi_j) e^{i\lambda_j} \\ -\sin(\Phi_j) e^{-i\lambda_j} & \cos(\Phi_j) \end{pmatrix},$$

其中 $\lambda_j = \gamma_j - \alpha_j$. 当满足条件

$$\lambda_{j_n} = \lambda_{j_{n-1}} \cdots = \lambda_{j_1} = \lambda \quad (13)$$

时(λ 是一个实数), 可得

$$\begin{aligned} \mathbf{X}_{k=\sum_{s=1}^n j_s} &= \tilde{Q}_{j_n} \tilde{Q}_{j_{n-1}} \cdots \tilde{Q}_{j_1} \\ &= e^{i(\sum_{s=1}^n \alpha_{j_s})} \times \begin{pmatrix} \cos(\sum_{s=1}^n \Phi_{j_s}) & \sin(\sum_{s=1}^n \Phi_{j_s}) e^{i\lambda} \\ -\sin(\sum_{s=1}^n \Phi_{j_s}) e^{-i\lambda} & \cos(\sum_{s=1}^n \Phi_{j_s}) \end{pmatrix} \end{aligned} \quad (14)$$

其中正整数 $n \geq 1$, $k = \sum_{s=1}^n j_s$ 是总的叠代次数, 整数 $j_s \geq 2$.

现作一个基变换:

$$\{|\beta\rangle, |\tau\rangle\} = \{|\alpha\rangle, |\tau\rangle\} \mathbf{V} \quad (15)$$

其中过渡矩阵

$$\mathbf{V} = \begin{pmatrix} e^{i\lambda} & 0 \\ 0 & 1 \end{pmatrix} \quad (16)$$

则在基 $\{|\beta\rangle, |\tau\rangle\}$ 下, 式(14)可改写为

$$\begin{aligned} \mathbf{X}'_{k=\sum_{s=1}^n j_s} &= \mathbf{V}^{-1} \mathbf{X}_{k=\sum_{s=1}^n j_s} \mathbf{V} \\ &= e^{i(\sum_{s=1}^n \alpha_{j_s})} \begin{pmatrix} \cos(\sum_{s=1}^n \Phi_{j_s}) & \sin(\sum_{s=1}^n \Phi_{j_s}) \\ -\sin(\sum_{s=1}^n \Phi_{j_s}) & \cos(\sum_{s=1}^n \Phi_{j_s}) \end{pmatrix} \end{aligned} \quad (17)$$

现假设初始态 $|\gamma_0\rangle = \cos\beta_0 |\beta\rangle + \sin\beta_0 |\tau\rangle$. 经过 Long 算子对初始态 $|\gamma_0\rangle$ 总数为 k 的叠代作用, 此时目标态 $|\tau\rangle$ 前的概率幅变成

$$d_{k=\sum_{s=1}^n j_s} = e^{i(\sum_{s=1}^n \alpha_{j_s})} \sin(\Theta + \beta_0) \quad (18)$$

其中 $\Theta = -\sum_{s=1}^n \Phi_{j_s} > 0$. 为避免确定关系式(13), 令

$\tilde{Q}_{j_n} = \tilde{Q}_{j_{n-1}} \cdots = \tilde{Q}_{j_1} = \tilde{Q}_j$, 则式(17)和(18)分别变成

$$\tilde{Q}_2 \doteq \begin{pmatrix} e^{i(\theta_1 + \theta_2)} \\ t e^{i\Lambda} [e^{i\theta_1} (e^{i\theta_2} - 1) + e^{i\phi_2} (e^{i\theta_1} - 1)] \end{pmatrix}$$

如果 $\theta_1 + \theta_2 = \phi_1 + \phi_2 = \Delta$, 上式变为

$$\begin{aligned} \mathbf{X}'_{k=nj} &= \mathbf{V}^{-1} (\tilde{Q}_j)^n \mathbf{V} \\ &= e^{i(n\alpha_j)} \begin{pmatrix} \cos(-n\Phi_j) & -\sin(-n\Phi_j) \\ \sin(-n\Phi_j) & \cos(-n\Phi_j) \end{pmatrix} \end{aligned} \quad (19)$$

和

$$d_{k=nj} = e^{i(nj)} \sin(\Theta' + \beta_0) \quad (20)$$

其中 $\Theta' = -n\Phi_j > 0$. 当 $\sin(\Theta' + \beta_0) = 1$, 就能以 100% 的最大成功概率找到目标态 $|\tau\rangle$.

4 多相位匹配方程

上节讨论了在理论上存在着两个集合 $\{\theta_j, \theta_{j-1}, \dots, \theta_1\}$ 和 $\{\phi_j, \phi_{j-1}, \dots, \phi_1\}$ ($j \geq 2$), 在基 $\{|\beta\rangle, |\tau\rangle\}$ 下, 经过式(10)中所定义的酉算子 $\tilde{G}_j$ 对初始态 $|\gamma_0\rangle = \sqrt{N-1/N} |\beta\rangle + \sqrt{1/N} |\tau\rangle$ 的 n 次叠代作用, 目标态 $|\tau\rangle$ 能以 100% 的最大成功概率找到. 但要建立这两个集合之间精确的数学关系式却是件非常困难的事情. 现在自然就有这样一个问题产生: 如果把条件 $\sin(\Theta' + \beta_0) = 1$ 放宽为 $\sin(\Theta' + \beta_0) \approx 1$, 那么集合 $\{\theta_j, \theta_{j-1}, \dots, \theta_1\}$ 和 $\{\phi_j, \phi_{j-1}, \dots, \phi_1\}$ 应大致满足什么样的条件才可使得 $\sin(\Theta' + \beta_0) \approx 1$ 成立? 对于这个问题, 我们下面的一个推测 (conjecture).

推测: 假设 N 较大. $\{\theta_j, \theta_{j-1}, \dots, \theta_1\}$ 和 $\{\phi_j, \phi_{j-1}, \dots, \phi_1\}$ ($\theta_m, \phi_m \neq 2k'\pi, 1 \leq m \leq j, k'$ 是任意的整数) 是定义在实数域 $\mathbb{R}$ 上的两个任意的相位旋转角集合. 如果整数 $j \geq 2$ 的值相对于 N 较小且这两个相位旋转角集合满足下面的多相位匹配方程

$$\sum_{m=1}^j \theta_m = \sum_{m=1}^j \phi_m = \Delta \quad (21)$$

则总能够通过选择某个合适的整数 $n \geq 1$ 以使得初始态 $|\gamma_0\rangle = \cos\beta_0 |\beta\rangle + \sin\beta_0 |\tau\rangle$ 在经过定义的式(10)中的算子 $\tilde{G}_j$ 的 n 次叠代作用后, 目标态 $|\tau\rangle$ 以较高的成功概率找到.

证明. 忽略 t 的高阶项, 式(9)可近似表示为

$$\mathbf{Q} \doteq - \begin{pmatrix} e^{i\theta} & e^{i\phi} e^{-i\Lambda} (e^{i\theta} - 1)t \\ (e^{i\theta} - 1)e^{i\Lambda} t & e^{i\phi} \end{pmatrix} \quad (22)$$

(1) $j=2$ 的情形

当 $j=2$ 时, 忽略 t 的高阶项, 式(11)近似成为

$$t e^{-i\Lambda} [e^{i\theta_2} e^{i\phi_1} (e^{i\theta_1} - 1) + e^{i\phi_1} e^{i\phi_2} (e^{i\theta_2} - 1)] \quad (23)$$

$$\tilde{Q}_2 \doteq e^{i\delta} \begin{bmatrix} 1 & t[e^{-i(\Lambda-\phi_1)} - e^{-i(\Lambda+\phi_2-\theta_2)} + e^{-i(\Lambda-\theta_2)} - e^{-i\Lambda}] \\ t[-e^{i(\Lambda-\phi_1)} + e^{i(\Lambda+\phi_2-\theta_2)} - e^{i(\Lambda-\theta_2)} + e^{i\Lambda}] & 1 \end{bmatrix} \quad (24)$$

忽略对最后结果没有影响的总的相位因子 $e^{i\delta}$ 并且观察到上面矩阵副对角线上的两个元素满足关系式

$\tilde{Q}_{2(21)} = -\overline{(\tilde{Q}_{2(12)})}$ ($\overline{(\tilde{Q}_{2(12)})}$ 是 $\tilde{Q}_{2(12)}$ 的共轭复数), 式(24)可简化为

$$\tilde{Q}_2 \doteq \begin{bmatrix} 1 & tr e^{i\delta} \\ -tr e^{-i\delta} & 1 \end{bmatrix} = \mathbf{I} + tr \mathbf{T} \approx e^{t' \mathbf{T}} \quad (25)$$

$\mathbf{I}$ 表示单位矩阵, 实数 $r > 0$ 和实数 δ 通过关系式 $r e^{i\delta} = e^{-i(\Lambda-\phi_1)} - e^{-i(\Lambda+\phi_2-\theta_2)} + e^{-i(\Lambda-\theta_2)} - e^{-i\Lambda}$ 来定义, 即 $r = |e^{i\phi_1} - e^{i(\theta_2-\phi_2)} + e^{i\theta_2} - 1|$ (符号 $|\cdot|$ 表示一个复数的模), $t' = tr$, $\mathbf{T} = \begin{bmatrix} 0 & e^{i\delta} \\ -e^{-i\delta} & 0 \end{bmatrix}$. 利用性质 $\mathbf{T}^2 =$

$-\mathbf{I}$, $\mathbf{T}^3 = -\mathbf{T}$, $\mathbf{T}^4 = \mathbf{I}$, $\mathbf{T}^5 = \mathbf{T}$, $\dots$, 可得

$$(\tilde{Q}_2)^n \doteq e^{nt' \mathbf{T}} = \cos(nt') \mathbf{I} + \sin(nt') \mathbf{T} \\ = \begin{bmatrix} \cos(nt') & e^{i\delta} \sin(nt') \\ -e^{-i\delta} \sin(nt') & \cos(nt') \end{bmatrix} \quad (26)$$

根据式(15)给出的基变换 $\{|\beta\rangle, |\tau\rangle\} = \{|\alpha\rangle, |\tau\rangle\} \mathbf{V}$, 在基 $\{|\beta\rangle, |\tau\rangle\}$ 下, 式(26)可重新表示为

$$(\tilde{Q}_2)^n = \begin{bmatrix} \cos(nt') & -\sin(nt') \\ \sin(nt') & \cos(nt') \end{bmatrix},$$

注意此时式(16)中的过渡矩阵取为

$$\mathbf{V} = \begin{bmatrix} -e^{-i\delta} & 0 \\ 0 & 1 \end{bmatrix}.$$

因此初始态 $|\gamma_0\rangle = \cos\beta_0 |\beta\rangle + \sin\beta_0 |\tau\rangle$ 经过算子 $\tilde{G}_2 = G(\phi_2, \theta_2)G(\phi_1, \theta_1)$ 的 n 次叠代作用(此时实际总的叠代次数为 $k = 2n$), $|\beta\rangle$ 前的概率幅变成 $d_{k=2n} = \sin(nt' + \beta_0)$. 当 $\sin(nt' + \beta_0) \approx 1$, 即 $n \approx \lceil (\pi/2 - \beta_0)/t' \rceil$ 时, 就能以较高的成功概率找到目标态, 符号 $\lceil \cdot \rceil$ 表示按四舍五入的方式取符号内实数的整数.

(2) $j \geq 3$ 的情形

令 $j = j' - 1$, $j' \geq 4$ 是一个相对于 N 较小的正整数. 假设在忽略 t 的高阶项的情况下矩阵 $\tilde{Q}_{j'-1}$ 可表示成下列形式

$$\tilde{Q}_{j'-1} \doteq (-1)^{j'-1} \begin{bmatrix} e^{i(\theta_1+\theta_2+\dots+\theta_{j'-1})} & t e^{-i\Lambda} z_1 \\ t e^{i\Lambda} z_2 & e^{i(\phi_1+\phi_2+\dots+\phi_{j'-1})} \end{bmatrix} \quad (27)$$

且其与式(23)中的矩阵 $\tilde{Q}_2$ 有着完全相同的性质(即对所有的 $2 \leq j \leq j' - 1$, 矩阵 $\tilde{Q}_j = \mathbf{Q}(\phi_j, \theta_j) \mathbf{Q}(\phi_{j-1}, \theta_{j-1}) \dots \mathbf{Q}(\phi_1, \theta_1)$ 的两个列矢量互相正交且该两个列

矢量所对应的范数相等), 这里的 z_1 和 z_2 是两个复数. 那么当 $j = j'$ 时有

$$\tilde{Q}_{j'} \doteq \begin{bmatrix} e^{i\theta_{j'}} & e^{i\phi_{j'}} e^{-i\Lambda} (e^{i\theta_{j'}} - 1)t \\ (e^{i\theta_{j'}} - 1)e^{i\Lambda} t & e^{i\phi_{j'}} \end{bmatrix} \times \\ \begin{bmatrix} e^{i(\theta_1+\theta_2+\dots+\theta_{j'-1})} & t e^{-i\Lambda} z_1 \\ t e^{i\Lambda} z_2 & e^{i(\phi_1+\phi_2+\dots+\phi_{j'-1})} \end{bmatrix} \\ \doteq (-1)^{j'} \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix} \quad (28)$$

其中

$$p_{11} = e^{i(\theta_1+\theta_2+\dots+\theta_{j'})}, \\ p_{12} = t e^{-i\Lambda} [e^{i\theta_{j'}} z_1 + e^{i(\phi_1+\phi_2+\dots+\phi_{j'-1})} e^{i\phi_{j'}} (e^{i\theta_{j'}} - 1)], \\ p_{21} = t e^{i\Lambda} [e^{i\phi_{j'}} z_2 + e^{i(\theta_1+\theta_2+\dots+\theta_{j'-1})} (e^{i\theta_{j'}} - 1)], \\ p_{22} = e^{i(\phi_1+\phi_2+\dots+\phi_{j'})}.$$

根据归纳假设很容易证明上述矩阵 $\tilde{Q}_{j'}$ 中的两个列矢量也互相正交且它们各自所对应的范数也相等. 从而可以得到以下结论: 对任意给定的一个相对于 N 较小的正整数 j' , 在忽略 t 的高阶项的情况下, 所有矩阵 $\tilde{Q}_j$ ($2 \leq j \leq j'$) 中的两个列向量互相正交且它们所对应的范数相等.

现令 $\sum_{m=1}^{j'} \theta_m = \sum_{m=1}^{j'} \phi_m = \Delta$ 且忽略对最后结果没有影响的总的复数因子 $e^{i\delta}$, 则可将式(28)化简为下列形式

$$\tilde{Q}_{j'} \doteq (-1)^{j'} \begin{bmatrix} p'_{11} & p'_{12} \\ p'_{21} & p'_{22} \end{bmatrix} \quad (29)$$

其中

$$p'_{11} = 1, \quad p'_{12} = t e^{-i\Lambda} [e^{i(\theta_{j'}-\Delta)} z_1 + e^{i\theta_{j'}} - 1], \\ p'_{21} = t e^{i\Lambda} [e^{i(\phi_{j'}-\Delta)} z_2 - e^{-i\theta_{j'}} + 1], \quad p'_{22} = 1.$$

利用式(27)中矩阵 $\tilde{Q}_{j'-1}$ 两个列向量的正交性条件可得到关系式

$$p'_{12} = -\overline{(p'_{21})} \quad (30)$$

利用式(30)可将式(29)化简为

$$\tilde{Q}_{j'} \doteq (-1)^{j'} \begin{bmatrix} 1 & t\tau' e^{i\sigma} \\ -t\tau' e^{-i\sigma} & 1 \end{bmatrix} \quad (31)$$

这里的正实数 τ' 和实数 σ 通过 $\tau' e^{i\sigma} = e^{-i\Lambda} [e^{i(\theta_{j'}-\Delta)} z_1 + e^{i\theta_{j'}} - 1]$ 来定义, 即

$$\tau' = |e^{i(\theta_{j'}-\Delta)} z_1 + e^{i\theta_{j'}} - 1| \quad (32)$$

如果 N 足够大, 那么对所有相对于 N 较小的正整数 j' ($j' \geq 4$), 式(31)可以近似表示为

$$\begin{pmatrix} 1 & t\tau'e^{i\sigma} \\ -t\tau'e^{-i\sigma} & 1 \end{pmatrix} = (-1)^{j'}(\mathbf{I} + t\tau'\mathbf{T}') \\ \approx (-1)^{j'}\left[\mathbf{I} + \sum_{N'=1}^{\infty} \frac{1}{N'!}(\xi\mathbf{T}')^{N'}\right] = (-1)^{j'}e^{\xi\mathbf{T}'} \quad (33)$$

其中

$$\xi = t\tau', \quad \mathbf{T}' = \begin{pmatrix} 0 & e^{i\sigma} \\ -e^{-i\sigma} & 0 \end{pmatrix}.$$

矩阵 $\mathbf{T}'$ 同样具有性质: $(\mathbf{T}')^2 = -\mathbf{I}$, $(\mathbf{T}')^3 = -\mathbf{T}'$, $(\mathbf{T}')^4 = \mathbf{I}$, $(\mathbf{T}')^5 = \mathbf{T}'$, ... 下面的证明步骤和 $j = 2$ 时的情形类似. 重新取过渡矩阵

$$\mathbf{V} = \begin{pmatrix} -e^{-i\sigma} & 0 \\ 0 & 1 \end{pmatrix},$$

经过算子 $\tilde{G}_{j'} = G(\phi_{j'}, \theta_{j'}) \cdots G(\phi_2, \theta_2)G(\phi_1, \theta_1)$ 对初始态 $|\gamma_0\rangle = \cos\beta_0|\beta\rangle + \sin\beta_0|\tau\rangle$ 的

$$n \approx \lceil (\pi/2 - \beta_0)/\xi \rceil \quad (34)$$

次叠代作用, 就能以较高的成功概率找到目标态. 最后把符号 j' 换成 j 即得推测中的结论.

从上面的证明过程可以看出, 式(21)是个近似公式, 在量子搜索算法中它不是最佳的关系式, 只是说明二维复子空间中, 在满足该式且整数 $j \geq 2$ 相对于 N 较小的情况下, 目标态(初始态是平均叠加态)仍然能以较高的成功概率找到. 现在分析对任意给定的两个相位角集合 $\{\theta_j, \theta_{j-1}, \dots, \theta_1\}$ 和 $\{\phi_j, \phi_{j-1}, \dots,$

$\phi_1\}$ ($j \geq 3$), 当满足多相位匹配方程 $\sum_{m=1}^j \theta_m = \sum_{m=1}^j \phi_m = \Delta$ 时, 如何来确定式(34). 当出现在式(6)中的参数 t 确定时, $\xi = t\tau'$ 可由式(32)中定义的 τ' 来予以确定. 比较矩阵(27)和(28)中的第 1 行第 2 列中的两个矩阵元素, 可得以下递推关系式

$$z_{1(j-1)} = e^{i\theta_{j-1}} z_{1(j-2)} + e^{i(\phi_1 + \phi_2 + \dots + \phi_{j-2})} e^{i\phi_{j-1}} (e^{i\theta_{j-1}} - 1) \quad (35)$$

同样通过比较矩阵(23)和(27)中第 1 行第 2 列中的两个矩阵元素, 可得

$$z_{1(j=2)} = e^{i\theta_2} e^{i\phi_1} (e^{i\theta_1} - 1) + e^{i\phi_1} e^{i\phi_2} (e^{i\theta_2} - 1) \quad (36)$$

对任意的 $\{\theta_{j-1}, \theta_{j-2}, \dots, \theta_1\}$ 和 $\{\phi_{j-1}, \phi_{j-2}, \dots, \phi_1\}$, 从式(36)出发, 利用递推关系式(35), 可最终求得 $z_{1(j-1)}$, 最后利用矩阵(31)中第 1 行第 2 列元素的因子定义式 $\tau' e^{i\sigma} = e^{-i\Delta} [e^{i(\theta_{j'} - \Delta)} z_1 + e^{i\theta_{j'}} - 1]$, 通过式(32)来求得 τ' . 从而利用 $\xi = t\tau'$ 和式(34)可近似得到叠代次数 n , 注意总的叠代次数是 $k = jn$.

显然在基 $\{|\beta\rangle, |\tau\rangle\}$ 下, 可将矢量关系式 $|\gamma'_n\rangle = (\tilde{G}_j)^n |\gamma_0\rangle$ 写成下面的矩阵形式

$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = (\tilde{\mathbf{Q}}_j)^n \begin{pmatrix} \cos\beta_0 \\ \sin\beta_0 \end{pmatrix} \quad (37)$$

对于所有的整数 $n \geq 1$, 成功概率由

$$P_n = |v_n|^2 \quad (38)$$

来确定.

注释: 最后, 我们需要指出以下两点:

(1) 从矩阵(22)中第 1 行第 2 列中的元素可得

$$z_{1(j=1)} = e^{i\phi_1} (e^{i\theta_1} - 1) \quad (39)$$

这实际上就是文献[9]中所对应的 $\theta_1 = \phi_1$ 情形. 根据递归关系式(35)容易得到式(36). 因此, 一方面式(21)可视为对相位匹配条件 $\theta_1 = \phi_1$ [9] 的进一步推广; 另一方面, 却有可能出现下面的情况: 当 N 不是太大且满足式(21)时, 在式(37)中的 $n = 1$ 情形下, 此时的成功概率 $P_1 = |v_1|^2$ 也有可能较大. 这意味着当总的叠代次数 $k = j$ 时, 即便任意的两个相位旋转角 θ_m 和 ϕ_m 完全独立且所有的相位对 (θ_m, ϕ_m) 都不相同 ($1 \leq m \leq j = k$), 在满足多相位匹配方程(21)条件下, Long 算法也依然有效. 对这种情况, 实际上可通过结合多相位匹配方程(21)和经典穷举算法, 在对两个相位角集合 $\{\theta_j, \theta_{j-1}, \dots, \theta_1\}$ 和 $\{\phi_j, \phi_{j-1}, \dots, \phi_1\}$ 作出适当调整后, 最后是仍然能够以几乎接近 100% 的成功概率找到目标态的. 由于篇幅关系, 这个问题在这里就不作详述了.

(2) 当 j 的值较小时, 比如: $j = 1, 2$ 情形下, Long 算法的复杂性较容易确定. 但随着 j 值的逐步增大, 针对不同的 j 值, 该算法的复杂性以统一的公式给出却是非常困难的. 这是因为对于不同的 j 值, 算法的复杂性公式完全不同. 但对于某个给定的 j 值而言, 却总能够从初始关系式(39)出发, 按照递推关系式(35)来确定与该 j 值所对应的 z_1 值, 从而最终确定其复杂性.

5 多相位匹配方程有效性的仿真验证

本节将通过给出下面的具体算例来进一步验证多相位匹配方程(21)的有效性. 图 1~图 5 是按下列方式得出的成功概率仿真曲线图. 首先设定必要的参数: $N = 10000$, $t = \beta_0 = \arcsin(1/100)$, $\Delta = 2\pi/3$. 然后针对每个确定的参数 $j = 2, 3, 10, 20, 50$, 由计算机系统随机任意产生 $0 < \phi_m, \theta_m < 50$ ($m = 1, 2, \dots, j$)

(调整前). 接着将 (ϕ_j, θ_j) 改变为 $\phi_j = \Delta - \sum_{m=1}^{j-1} \phi_m, \theta_j = \Delta - \sum_{m=1}^{j-1} \theta_m, \Delta = \{-4\pi/5, 0, 2\pi/3\}$ (调整后 3 种情形). 成功概率 P_n 由式(38)确定.

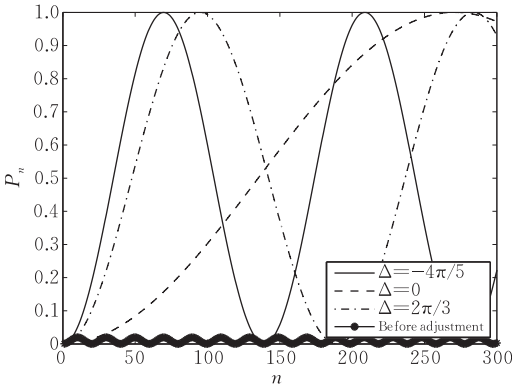


图 1 $j=2$ 时调整前和调整成功概率 P_n 和叠代次数 n 关系曲线图($N=10^4, j=2$)

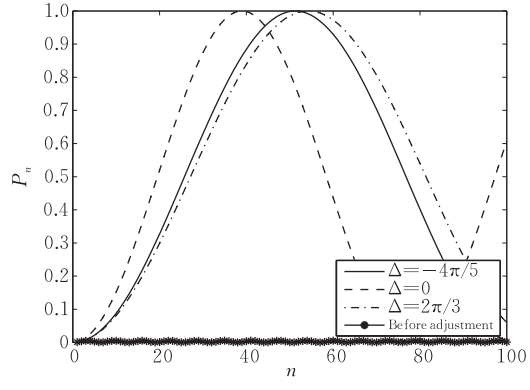


图 2 $j=3$ 时调整前和调整成功概率 P_n 和叠代次数 n 关系曲线图($N=10^4, j=3$)

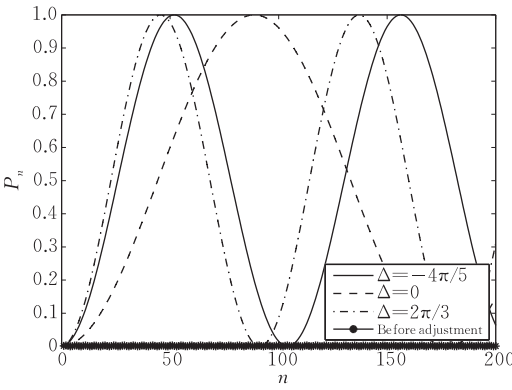


图 3 $j=10$ 时调整前和调整成功概率 P_n 和叠代次数 n 关系曲线图($N=10^4, j=10$)

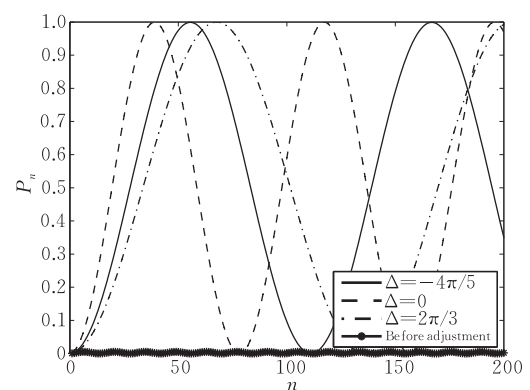


图 4 $j=20$ 时调整前和调整成功概率 P_n 和叠代次数 n 关系曲线图($N=10^4, j=20$)

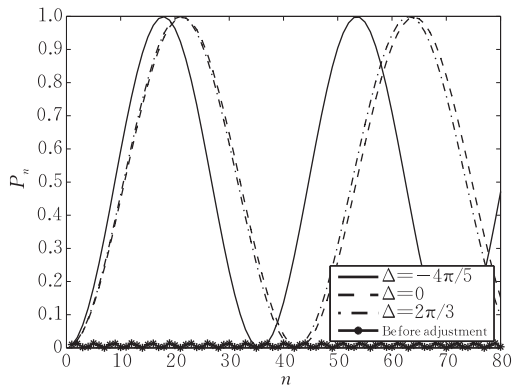


图 5 $j=50$ 时调整前和调整成功概率 P_n 和叠代次数 n 关系曲线图($N=10^4, j=50$)

6 结 论

提出了二维复子空间中 Long 算法的多相位匹配问题,即假设初始态为

$|\gamma_0\rangle = \sqrt{N-1/N}|\beta\rangle + \sqrt{1/N}|\tau\rangle$ (N 足够大), 在酉算子 $\tilde{G}_j = G(\phi_j, \theta_j)G(\phi_{j-1}, \theta_{j-1}) \cdots G(\phi_1, \theta_1)$ 作用下,在理论上存在着两个集合 $\{\theta_j, \theta_{j-1}, \dots, \theta_1\}$ 和 $\{\phi_j, \phi_{j-1}, \dots, \phi_1\}$, 目标态 $|\tau\rangle$ 能以 100% 的最大成功

概率找到. 同时给出了一个推测:如果这两个相位角集合满足多相位匹配方程 $\sum_{m=1}^j \theta_m = \sum_{m=1}^j \phi_m = \Delta$ 且整数 $j \geq 2$ 相对于 N 较小,则目标态 $|\tau\rangle$ 能以较高的成功概率找到. 尽管该多相位匹配方程的推导过程和文献[9]中推导单相位匹配条件 $\theta = \phi$ 的过程有些类似,但他们的基本思想出发点是不一致的. 一方面,多相位匹配方程是针对多相位匹配问题而给出的一个近似公式(对应于 $j \geq 2$ 的情形). 在文献[15]中证明了单相位匹配条件 $\theta = \phi$ 也是一个精确的相位公式;然而,随着 j 值的增大以及对于不同的 j 值($j \geq 2$),要进一步证明多相位匹配方程是否也是个精确公式却是异常困难的. 另一方面,却给予了我们以下启示:当 N 不是太大且满足多相位匹配方程时,有可能出现每次叠代的相位旋转角 θ_m 和 ϕ_m 完全独立且所有的相位对 (θ_m, ϕ_m) 都不相同($1 \leq m \leq j = k, k$ 表示总的叠代次数)的情况下,Long 算法也依然有效.

致 谢 作者感谢审稿专家所提供的帮助和提出的宝贵意见及为此文付出劳动的编辑老师!

参 考 文 献

- [1] Grover L K. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 1997, 79(2): 325-328
- [2] Bennett C H, Bernstein E, Brassard G et al. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 1997, 26(5): 1510-1523
- [3] Zalka C. Grover's quantum searching algorithm is optimal. *Physical Review A*, 1997, 60(4): 2746-2751
- [4] Boyer M, Brassard G, Hoyer P et al. Tight bounds on quantum searching. *Fortschritte Der Physik-Progress of Physics*, 1996, 46(4-5): 493-506
- [5] Grover L K. Quantum computers can search rapidly by using almost any transformation. *Physical Review Letters*, 1998, 80(19): 4329-4332
- [6] Brassard G, Hoyer P, Tapp A. Quantum counting//*Proceedings of the 25th ICALP, Aalborg, Denmark. Lecture Notes in Computer Science* 1443. Springer, 1998: 820-831
- [7] Brassard G, Hoyer P, Mosca M et al. Quantum amplitude amplification and estimation. *Quantum Computation and Quantum Information: AMS Contemporary Mathematics Series Millennium Volume*, 2002, 305: 53-74
- [8] Gingrich R, Williams C P, Cerf N. Generalized quantum search with parallelism. *Physical Review A*, 2000, 61(5): 1-8
- [9] Long G L, Li Y S, Zhang W L et al. Phase matching in quantum searching. *Physics Letters A*, 1999, 262(1): 27-34
- [10] Biham E, Biham O, Biron D et al. Grover's quantum search algorithm for an arbitrary initial amplitude distribution. *Physical Review A*, 1999, 60(4): 2742-2745
- [11] Biham E, Biham O, Biron D et al. Analysis of generalized Grover quantum search algorithms using recursion equations. *Physical Review A*, 2000, 63(1): 2742-2749
- [12] Carlini A, Hosoya A. Quantum computers and unstructured search: Finding and counting items with an arbitrarily entangled initial state. *Physics Letters A*, 2001, 280(3): 114-120
- [13] Jin W L, Chen X D. A desired state can not be found with certainty for Grover's algorithm in a possible three-dimensional complex subspace. *Quantum Information Processing*, 2011, 10(3): 419-429
- [14] Long G L, Zhang W L, Li Y S et al. Arbitrary phase rotation of the marked state can not be used for Grover's quantum search algorithm. *Communications in Theoretical Physics*, 1999, 32(3): 335-338
- [15] Long G L, Xiao L, Sun Y. Phase matching condition for quantum search with a generalized quantum database. *Physics Letters A*, 2002, 294(3-4): 143-152
- [16] Long G L. Grover algorithm with zero theoretical failure rate. *Physical Review A*, 2001, 64(2): 022307
- [17] Hoyer P. Arbitrary phases in quantum amplitude amplification. *Physical Review A*, 2000, 62(5): 052304
- [18] Long G L, Tu C C, Li Y S et al. An SO(3) picture for quantum searching. *Journal of Physics A: Mathematical and General*, 2001, 34(4): 861-866
- [19] Long G L, Yan H Y, Li Y S et al. Experimental NMR realization of a generalized quantum search algorithm. *Physics Letters A*, 2001, 286(2): 121-126
- [20] Bhattacharya N, van den Heuvell H B V, Spreeuw R J C. Implementation of quantum search algorithm using classical fourier optics. *Physical Review Letters*, 2002, 88(13): 137901
- [21] Puentes G, Mela C L, Ledesma S et al. Optical simulation of quantum algorithms using programmable liquid-crystal displays. *Physical Review A*, 2004, 69(4): 042319
- [22] Long G L, Liu Y. Search an unsorted database with quantum mechanics. *Frontiers of Computer Science in China*, 2007, 1(3): 247-271
- [23] Li D F, Li X X. More general quantum search algorithm $Q = -I_V VI_U$ and the precise formula for the amplitude and the non-symmetric effects of different rotating angles. *Physics Letters A*, 2001, 287(5-6): 304-316
- [24] Jin W L. Quantum search in a possible three-dimensional complex subspace. *Quantum Information Processing*, 2012, 11(1): 41-54
- [25] Tulsi A. Quantum computers can search rapidly by using almost any selective transformation. *Physical Review A*, 2008, 78(2): 022332
- [26] Long G L, Li Y S, Zhang W L et al. Dominant gate imperfection in Grover's quantum search algorithm. *Physical Review A*, 2000, 61(4): 042305
- [27] Joshi A W. *Matrices and Tensors in Physics*. New Delhi: New Age International (P) Ltd., Reprint, 2005, 69

JIN Wen-Liang, born in 1968, Ph.D.. His research interests include quantum algorithm, quantum information theory.



Background

Grover's search algorithm is one of the key algorithms in the field of quantum computing. It allows one to find a single desired state in a large unsorted database of size N using merely a number of queries in $O(N^{1/2})$, compared to the classical $O(N)$, and thus provides a quadratic speedup. There have been various improvements made to the original Grover's search algorithm over the past decade. To guarantee the effectiveness of the Long algorithm, which is one of the generalized Grover's algorithms, the phase matching condition (i. e. identical rotation angles) shall be observed by using an approximate method. Biham et al. also thought that in order for the Long algorithm to apply, the two rotation angles must be equal. Subsequently, Long et al. further showed that this phase condition is actually an exact relation. By now the Grover's search algorithm has been verified experimentally in NMR (nuclear magnetic resonance) system with a few qubits, and the experimental implementation of the Long algorithm has been successfully completed in optical device and in NMR system.

When the search space is extended to a possible three-dimensional complex subspace, we proved that no matter what the initial superposition may be, a desired state cannot be found with certainty, and demonstrated that if N is sufficiently large then corresponding to the case of identical rota-

tion angles, the maximum success probability of finding a unique desired state is approximately equal to the square of the cosine function of a deflection angle. Furthermore, we also showed that in this case, as the difference between the two rotation angles increases, the Long algorithm fails to enhance the probability of measuring a unique desired state irrespective of whether or not a deflection angle is small.

Most of the previous work on quantum search focused primarily on the study of the single-phase matching. In the present paper we made a remarkable advance beyond this limit by introducing the notion of the multiphase matching, so as to make the Long algorithm more generally applicable. Our analysis showed that a unique desired state can be found with high probability of success provided the multiphase matching equation is satisfied for an equally-weighted initial superposition of all basis states in a two-dimensional complex subspace.

We have another purpose in this paper to reveal that when N is not too large, maybe the multiphase matching equation is able to provide the following particular situation; in the case that any two phase rotation angles corresponding to each iteration of Long operator are completely independent and all of the pairs of phases are different from one another, the Long algorithm can still be effective.