

一种改进的 Grover 量子搜索算法

夏克文^{1,2}, 苏昶², 沈钧毅¹, 李昌彪¹

(1. 西安交通大学电子与信息工程学院, 710049, 西安; 2. 河北工业大学信息工程学院, 300401, 天津)

摘要: 经分析发现, Grover 量子搜索算法及 Long 的改进算法均无法达到 100% 成功概率的搜索结果, 为此在 Long 的改进算法基础上提出了一种新的搜索算法. 它主要将相位取反替换成具有自适应调整特点的、与目标数据量和数据总量有关的相位旋转, 当目标数据量为数据总量的 1/2 时, 将数据总量扩展 2 倍, 这样算法的搜索可以做到 100% 的成功概率. 通过对背包问题的仿真研究表明, 所提算法优于 Grover 算法和 Long 的改进算法, 其求解速度快、准确率高, 在带有数据误差的实际问题求解中进行相位匹配能够得到满意的效果.

关键词: 量子搜索算法; 成功概率; 相位旋转; 相位匹配; 背包问题

中图分类号: TP309 **文献标识码:** A **文章编号:** 0253-987X(2007)10-1127-05

Improved Grover's Quantum Searching Algorithm

Xia Kewen^{1,2}, Su Chang², Shen Junyi¹, Li Changbiao¹

(1. School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China;

2. School of Information Engineering, Hebei University of Technology, Tianjin 300401, China)

Abstract: The analysis shows that the Grover's algorithm and the improved algorithm of Long are hard to attain 100% success probability. So a new searching algorithm is presented based on the improved algorithm of Long. The main contributions are to replace the inverting phase with a rotation phase which has the characteristic of self-adaption related with the data total amount and the target data quantity, and expand twice as big as the total amount when the target data quantity is half of the total amount. The new algorithm can attain 100% searching success rate in any case. The simulation result of knapsack problem indicates that the new algorithm is superior to Grover's algorithm and the improved algorithm of Long, it possesses of quick speed and high accuracy in searching, and gets good effect to solve actual problems with data error for phase matching.

Keywords: quantum searching algorithm; success probability; phase rotation; phase matching; knapsack problem

量子算法融入了量子力学的许多基本特性, 如相干叠加性、纠缠性、并行性、测量坍缩等, 极大地提高了计算效率, 已逐步成为一种崭新的计算模式. 1996 年 Grover 提出的未加整理的数据库搜索量子算法^[1-3]是量子计算机有效执行计算任务的一个实例, 在该算法中, 数据总量为 N 的经典信息串可以以 $1/N^{1/2}$ 幅度概率的叠加形式存放在量子寄存器

中, 再经 $N^{1/2}$ 量级步数的变换, 便可以寻找到目标态, 并以幅度概率 $A=1$ 的形式表示出来, 而经典计算机则需要 N 量级的运行时间. 1998 年 IBM 公司及斯坦福大学的 Chuang 等人第一次用核磁共振 (NMR) 方法在 2 个异核的分子特性上演示了 Grover 算法, 这是目前量子计算理论和实验中研究最广泛的、已被核磁共振实验验证的一种量子算法,

这一算法虽未改变问题的复杂性,但量子加速甚至比 Shor 分解因子算法还要快得多.由于验证一个问题的解比寻找这个问题的解要容易得多,因此量子搜索算法可以作为求解 NP 类问题的方法.

然而, Grover 算法仍无法做到搜索的成功概率 $P=100\%$, 且在实际应用中出现的相位误差会导致 P 下降等问题. 在分析 Grover 算法的基础上, 本文提出了一种改进的算法, 并针对一类可用于公钥密码体制设计的 NP 完全问题, 即 0/1 背包问题进行仿真研究, 分析并指出了相位匹配是求解带有数据误差问题的一个重要环节.

1 Grover 算法的量子改进算法

1.1 Grover 算法

Grover 算法就是通过寻找一个么正变换^[4]来反复迭代、放大要寻找的态 $|\Phi\rangle$ 的概率, 同时减小态 $|x \neq \Phi\rangle$ 的概率^[5]. 令初始态为 $|\Psi\rangle$, 则初始态通过 m 次迭代后得

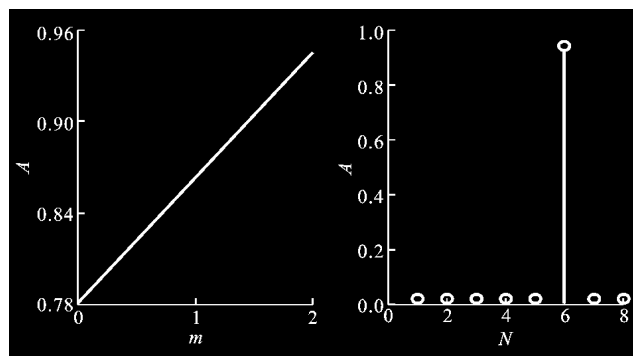
$$|\Psi_m\rangle = |\Psi(k_x^m, l_x^m)\rangle \quad (1)$$

式中: k_x^m, l_x^m 分别表示所找的目标态 $|\Phi\rangle$ 和其他非目标态经过 m 次搜索后的幅度概率, 即

$$A = \begin{cases} l_x^m = \frac{1}{(N-1)^{1/2}} \cos(2m+1)\theta \\ k_x^m = \sin(2m+1)\theta \end{cases} \quad (2)$$

当满足 $\sin(2m+1)\theta = 1 (N \gg 1)$ 时, $\sin\theta = 1/N^{1/2} \approx \theta$, 则可获得最少的搜索次数 $m = \lceil \pi N^{1/2}/4 \rceil$. 因此, Grover 算法只需要进行 $O(N^{1/2})$ 次操作就可从海量数据(库)中找到惟一的目标态数据. 若有 M 个数据满足查找条件, 则只需进行 $m = \lceil \frac{\pi}{4} \left(\frac{N}{M}\right)^{1/2} \rceil$ 次查询.

采用随机查找, 若目标态数 $j=6$, 数据总量 $N=8$, 则幅度概率 A 的仿真结果如图 1 所示.



(a) 搜索次数与幅度概率的关系

(b) 数据总量与幅度概率的关系

图 1 幅度概率的变化情况

由图 1a 可知, 若目标态数 $j=6$ 经过了 2 次查找, 第 1 次查找获得目标态的概率 $A=0.7812$, 第 2 次查找获得目标态的概率 $A=0.9453$. 由图 1b 可知, 经过 2 次搜索之后, 找到目标态的概率均在 90% 以上, 而非目标态的获取概率很小, 趋于 0, 可以忽略不计.

然而, Grover 算法还存在如下不足.

(1) 当 $M=N/2, \theta=\pi/4$ 时, 有

$$P = (k_x^m)^2 = (\sin(2m+1)\theta)^2 = 1/2 \quad (3)$$

其中, m 取正整数 $1, 2, \dots$. 从式(3)看出, 无论迭代多少次, P 仅为 50%, 这样的搜索结果肯定是失败的.

(2) 当搜索总量是无穷大时, P 接近于 1, 若数据库规模不够大, 则一定存在搜索失败的概率.

式(3)所示的 $P = (k_x^m)^2 = (\sin(2m+1)\theta)^2$, 将随着 N 的增加而不断增大, 而 P 振荡幅度随之减小, 且最终趋于稳定 (P 趋于 100%), P 与 N 的关系如图 2 所示. 但是, 当 N 比较小时, P 的变化幅度就比较大且不稳定.

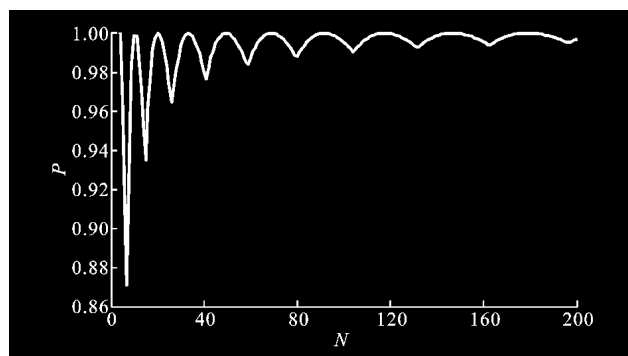


图 2 P 与 N 的关系

1.2 Grover 算法的量子改进算法

由于 Grover 算法存在 P 难以达到 100% 的缺点, 为此 Long 等人^[6-8]对 Grover 算法进行了改进, 即先将相位取反, 使其成为一个与数据库大小有关的旋转相位, 相位旋转角不再是固定不变的 π , 而是随搜索数据量变化的量, 然后将相位旋转角代入迭代算子进行迭代. 该相位旋转角

$$\phi = \theta = 2\arcsin\left[\sin\left[\frac{\pi}{4J+6}\right]/\sin\beta\right] = 2\arcsin\left[\sin\left[\frac{\pi}{4J+6}\right]N^{1/2}\right] \quad (4)$$

式中: $J \geq J_{\infty}$, J_{∞} 为迭代次数, 即

$$J_{\infty} = \left\lceil \frac{\pi/2 - \beta}{2\beta} \right\rceil = \left\lceil \frac{\pi}{4\beta} - \frac{1}{2} \right\rceil \quad (5)$$

$$\beta = \arcsin[(1/N)^{1/2}] \quad (6)$$

然而,该算法是有缺陷的,一是其仅适用于一个搜索目标态,二是无法解决目标态数是 $1/2$ 搜索总量时的情况.因此,本文在 Long 算法的基础上进行了改进,即将相位旋转角改为

$$\phi = \theta = 2\arcsin\left[\sin\left[\frac{\pi}{4J+2}\right]/\sin\beta\right] = 2\arcsin\left[\sin\left[\frac{\pi}{4J+2}\right]\left(\frac{N}{j}\right)^{1/2}\right] \quad (7)$$

式中

$$\beta = \arcsin[(j/N)^{1/2}] \quad j = 1, 2, \dots, N \quad (8)$$

其中 j 表示目标态数.

式(7)、式(8)是在 Long 算法中增加了一个搜索目标态数 j ,这样便提高了算法的实时性提高了搜索多目标态的效率.要使旋转角 $\phi = \theta$,可以根据 j 进行自适应调整.

当 $N=16$ 时,本文算法经过多次计算,可得到 $\theta = \phi = 2.1269 \text{ rad}$ 时的 $P=100\%$,采用 Grover 算法的 $P=94.53\%$,采用 Long 算法的 $P=99.91\%$,显然本文算法效果最优.

对于 $j=N/2$ 的情况,可以牺牲计算机资源为代价,将数据存储量扩大为 $2N$,再将扩展的 N 个数据赋 0.这样,要寻找的目标态所占的比例变为 $1/4$,因此本文算法仍然适用.

本文算法的具体步骤描述如下.

步骤 1: 若目标态数为搜索总量的 $1/2$,则将搜索总量扩大为 $2N$,然后转步骤 2,否则直接执行步骤 2.

步骤 2: 初始化量子态,并将所有量子态放入寄存器之中,得到 N (或 $2N$)个等幅量子叠加态.

步骤 3: 构造迭代算子

$$Q \equiv -I_r U^{-1} I_\tau U \quad (9)$$

式中

$$\begin{aligned} I_r &= I - (1 - e^{i\phi}) |r\rangle\langle r| \\ I_\tau &= I - (1 - e^{i\theta}) |\tau\rangle\langle \tau| \end{aligned} \quad (10)$$

则有

$$Q = \begin{bmatrix} |r\rangle \\ U^{-1} |\tau\rangle \end{bmatrix} = \begin{bmatrix} -e^{i\theta} - (1 - e^{i\theta})(1 - e^{i\phi}) |U_\tau|^2 & (1 - e^{i\phi}) U_\tau \\ (1 - e^{i\theta}) e^{i\phi} U_\tau^* & -e^{i\phi} \end{bmatrix} \cdot \begin{bmatrix} |r\rangle \\ U^{-1} |\tau\rangle \end{bmatrix} \quad (11)$$

式中: $\theta = \phi$.

步骤 4: 将目标态数 j 代入式(5)、式(7)、式(8),得到 θ (或 ϕ).

步骤 5: 将迭代算子 Q 作用于初始态,经过多次迭代得到目标态.

步骤 6: 检测目标态,若检测结果正确则停止算法,否则继续上述步骤.

取 $N=64$,量子位 $n=6$,本文算法与 Long 算法的 P 随搜索目标态数 j 的变化如图 3 所示.

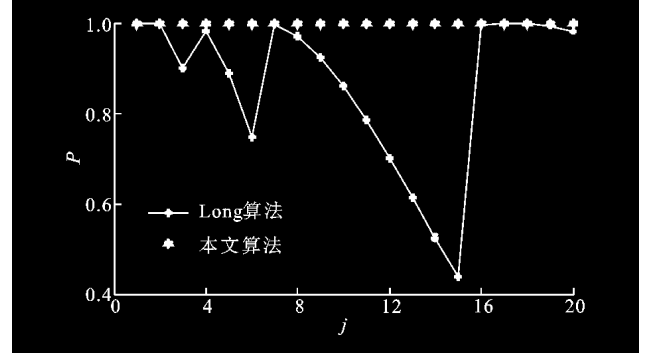


图3 2种算法的搜索成功概率随搜索目标态数 j 的变化

由于 Long 算法^[7-8]的相位旋转角不具实时性,所以它只有在目标态数为 1 时才有效,而当 j 取多个数据时, P 就无法达到 100% ,例如 $j=10$ 时, P 仅为 85% (见图 3).本文算法的相位旋转角随 N 、 j 而变,所以该算法具有实时性,且成功概率一直为 100% (见图 3).

2 求解背包问题的仿真分析

用 W 表示背包的质量容限,现有 n 种物品准备放入背包内,代号分别为 $x_1, x_2, \dots, x_n$,且 x_i 取值为 0 或 1,0 表示不选取,1 表示选取^[9].每种物品的价值分别为 $y_1, y_2, \dots, y_n$,质量分别为 $g_1, g_2, \dots, g_n$.那么,背包问题就是如何选取 n ,使得一些物品的若干件放入一个背包中,而其质量等于或小于一个给定值 W ,且背包内物品的价值最大,即满足

$$\left. \begin{aligned} \sum_{i=1}^n x_i g_i &\leq W \\ \max(\sum_{i=1}^n x_i y_i) \end{aligned} \right\} \quad (12)$$

若取 $n=4$, $W=10$,价值 $y=[10, 40, 30, 50]$,质量 $g=[5, 4, 6, 3]$,经过计算得出:当选取第 2 种和第 4 种物品时满足条件 $x=[0, 1, 0, 1]$,则有

$$\sum_{i=1}^4 x_i g_i = 7 < 10; \quad \max(\sum_{i=1}^n x_i y_i) = 90$$

0/1 背包问题是一个典型的 NP 完全问题,下面用本文算法来求解,并与 Grover 算法和 Long 算

法进行比较.

例如,一个背包的质量容限为 6 kg,现有 16 种物品选择性地放入背包之中,每种产品的质量 $g=[5,2,16,4,12,1,7,9,8,10,3,14,15,11,13,6]$,每种产品的价值 $y=[10,80,30,85,20,15,70,60,45,35,25,55,75,65,40,50]$,要求背包内放入的物品质量不得超过背包的容限,且放入背包内物品的价值最大.

采用本文算法,将迭代算子作用于初始态,经 2 次迭代后得到的目标态为 $[0,1,0,1,0,0,0,0,0,0,0,0,0,0,0,0]$. 采用 Grover 算法,其 A 、 m 、 N 的关系如图 4 所示.

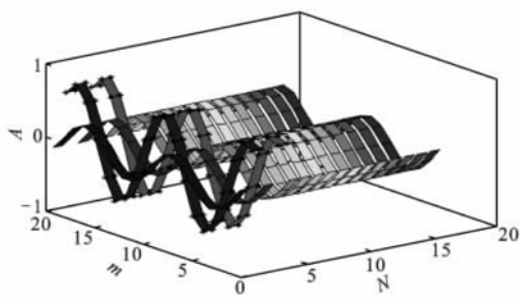


图4 Grover 算法中 A 、 m 、 N 的关系

从图 4 可以看出,要求的期望输出应是 $[0,1,0,1,0,0,0,0,0,0,0,0,0,0,0,0]$,而用 Grover 算法通过 2 次迭代的实际输出是 $[-0.088\ 4, 0.972\ 3, -0.088\ 4, 0.972\ 3, -0.088\ 4, -0.088\ 4, -0.088\ 4, -0.088\ 4, -0.088\ 4, -0.088\ 4, -0.088\ 4, -0.088\ 4, -0.088\ 4, -0.088\ 4, -0.088\ 4, -0.088\ 4]$,若将 $A \geq 0.972\ 3$ 记为 1,其他情况记为 0,即可求得问题的解.若继续进行多次迭代, A 的峰值会出现周期性变化,其最大值仍然是 0.972 3.显然,采用 Grover 算法效果不如本文算法.若 N 随机变化,Grover 算法与本文算法的成功概率如图 5 所示.

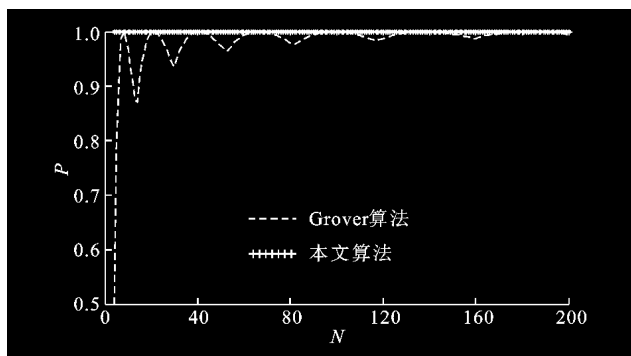


图5 2种算法搜索的成功概率比较

由图 5 可见,无论 N 为多少,本文算法的 P 始终为 100%,而 Grover 算法的 P 随 N 的变化呈准周期振荡.由此可见,本文算法的目标态的 P 不再随 N 变化,所以搜索精度得以提高.

当 $j=1$ 、 $j=2$ 时,3 种算法目标态的 P 比较如表 1、表 2 所示.

表1 3种算法目标态搜索的成功概率比较($j=1$)

N	m	$P/\%$		
		本文算法	Long 算法	Grover 算法
4	1	100.00	100.00	100.00
8	2	100.00	100.00	94.53
16	3	100.00	100.00	96.13
50	5	100.00	100.00	99.99
100	7	100.00	100.00	99.53
1 000	24	100.00	100.00	99.96
1×10^4	78	100.00	100.00	100.00
1×10^6	785	100.00	100.00	100.00
1×10^7	2 483	100.00	100.00	100.00
1×10^8	7 853	100.00	100.00	100.00

表2 3种算法目标态搜索的成功概率比较($j=2$)

N	m	$P/\%$		
		本文算法	Long 算法	Grover 算法
4	1	100.00	50.00	50.00
8	1	100.00	95.82	1.00
16	2	100.00	99.91	94.53
50	3	100.00	99.92	97.42
100	5	100.00	98.31	99.99
1 000	17	100.00	99.83	100.00
1×10^4	55	100.00	99.99	100.00
1×10^6	555	100.00	100.00	100.00
1×10^7	1 756	100.00	100.00	100.00
1×10^8	5 553	100.00	100.00	100.00

由表 1 可知,当 $j=1$ 时,本文算法和 Long 算法的目标态的 P 优于 Grover 算法.由表 2 可知,当 $j=2$ 时,本文算法的目标态的 P 均优于 Long 和 Grover 算法.

3 相位匹配问题分析

在严格相位匹配的情况下($\theta=\phi$),本文算法的 P 始终为 100%,若存在相位误差 σ , P 将随之变化,因此量子搜索算法的相位匹配非常重要^[10].在实际应用中,必须考虑相位匹配问题,否则将会带来很大的误差.若初始态与目标态的相位无法匹配,那么随着量子位数 n 的增加, P 将会随之下降. $\sigma=|\theta-\phi|=0.1, 0.01, 0.001, 0.0001$, σ 与 P 、 n 的关系如图 6 所示.

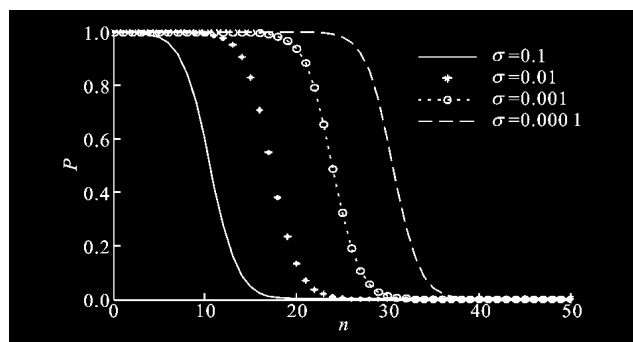


图 6 σ 与 P 、 n 的关系

由图 6 可见,随着 σ 减小、 n 增加($N=2^n$),达到 $P=100\%$ 的搜索时间将会延长,因为在 n 的取值范围内, P 具有普适性.带有相位误差的 P 随 n 的变化如表 3 表示.

表 3 带有相位误差的 P 与 n 的关系

n	$P_{\sigma=0.1}/\%$	$P_{\sigma=0.01}/\%$	$P_{\sigma=0.001}/\%$	$P_{\sigma=0.0001}/\%$
5	97.99	99.98	100.00	100.00
10	60.28	99.35	99.99	100.00
15	4.64	82.94	99.79	100.00
20	0.15	13.23	93.85	99.93
25	0.00	0.47	32.28	97.95
30	0.00	0.01	1.47	59.84
35	0.00	0.00	0.05	4.45
40	0.00	0.00	0.00	0.01

从表 3 看出,由于存在各种误差,在进行背包问题求解时,可以根据数据量的大致范围,在误差容许范围内进行测量.例如,当 $n=15$ 、 $N=32\ 768$ 时,可在 $\sigma=|\theta-\phi|<0.001$ 下进行测量,其搜索准确率也比较高.当搜索准确率放宽到 80% 时, $\sigma=|\theta-\phi|<0.01$ 即可.在实际应用中可以灵活掌握.

4 结 论

本文算法与 Grover 算法一样都是谋求加速求解过程.理论分析表明,本文算法比 Grover、Long 算法更为优越.通过求解背包问题的仿真分析表明,本文算法不但提高了搜索速度,而且对于大数据量同样可以达到 100% 的搜索成功概率.对于应用中出现的相位误差问题,可以根据实际需要选取合适的量子位数 n 进行相位匹配,同样可以获得理想的搜索结果.

参考文献:

- [1] Grover L K. A Fast quantum mechanical algorithm for database search [C]//Proceedings of the 28th Annual ACM Symposium on the Theory of Computing. New York: ACM,1996:212-219.
- [2] Grover L K. Quantum mechanics helps in searching for a needle in a haystack [J]. Phys Rev Lett, 1997, 79(2):326-328.
- [3] Grover L K. Quantum computers can search rapidly by using almost any transformation [J]. Phys Rev Lett, 1998, 80(19):4329-4332.
- [4] 夏培肃. 量子计算[J]. 计算机研究与发展, 2001, 38(10):1154-1155.
Xia Peisu. Quantum computation [J]. Journal of Computer Research and Development, 2001, 38(10):1154-1155.
- [5] 孙力, 须文波. 量子搜索算法体系及其应用 [J]. 计算机工程与应用, 2006, 42(14):55-57.
Sun Li, Xu Wenbo. Quantum search algorithm system and its applications [J]. Computer Engineering and Applications, 2006, 42(14):55-57.
- [6] Long Guilu. Grover algorithm with zero theoretical failure rate [J]. Phys Rev, 2001, A64(2):022307.
- [7] Long Guilu. Phase matching in quantum searching and the improved grover algorithm [J]. Nuclear Phys Rev, 2004, 21(2):114-116.
- [8] Long Guilu, Xiao Li. General phase matching condition for quantum searching [J]. Phys Lett, 2002, A294(4/3):143-152.
- [9] 钟诚, 赵跃华. 信息安全概论 [M]. 武汉: 武汉理工大学出版社, 2003.
- [10] Hsieh J Y, Li Cheming. General SU(2) formulation for quantum searching with certainty [J]. Phys Rev: A, 2002, 65(5):052322.

(编辑 苗凌)