背包问题的量子计算算法

钟普查[1]，鲍皖苏[1]，范得军[2]，徐 浩[3]
ZHONG Pu-cha[1]，BAO Wan-su[1]，FAN De-jun[2]，XU Hao[3]

1.解放军信息工程大学 电子技术学院，郑州 450004
2.解放军 75130 部队，广西 贵港 537100
3.解放军信息工程大学 电子技术学院 广州训练大队，广州 510510
1.Institute of Electronic Technology，the PLA Information Engineering University，Zhengzhou 450004，China
2.PLA 75130 Unit，Guigang，Guangxi 537100，China
3.Training Military Unit，Institute of Electronic Technology，the PLA Information Engineering University，Guangzhou 510510，China

ZHONG Pu-cha，BAO Wan-su，FAN De-jun，et al.Quantum mechanical algorithm to solve knapsack problem.Computer Engineering and Applications，2009，45（20）：63-64.

Abstract：Knapsack problem is one of the NP complete problems.Its computational complexity is $O(2^n)$.This paper presents the quantum mechanical algorithm based on the fixed phase quantum search to solve the knapsack problem，and the algorithm also gets probability of success at least 98% in $O(\sqrt{N/M})$ quantum mechanical steps（Where M is the number of matches）.This quantum algorithm has higher probability of success than the algorithm based on Grover algorithm with multiple matches in the search space.
Key words：quantum algorithm；Grover algorithm；fixed phase；knapsack problem

摘 要：背包问题属于 NP 完全问题，经典算法对规模为 n 的背包问题求解的时间复杂度为 $O(2^n)$。给出了基于固定相位的背包问题量子计算算法，证明了该算法在多解的情况下，能够以不低于 98%的成功率在 $O(\sqrt{N/M})$ 步完成对规模为 n 的背包问题求解（M 是解的数目），而基于原始 Grover 算法的背包问题量子计算算法计算复杂度为 $O(\sqrt{N/M})$，成功率是 50%~100%。
关键词：量子算法；Grover 算法；固定相位；背包问题
DOI：10.3778/j.issn.1002-8331.2009.20.019 **文章编号**：1002-8331（2009）20-0063-02 **文献标识码**：A **中图分类号**：TN301.6

1 引言

随着物理学的原理和计算机科学的交融和相互促进，量子信息与量子计算理论科学逐步发展起来。1982 年 Feyman[1]制造了一个抽象的模型，该模型示范了如何利用量子系统做运算，一般认为量子计算机的概念由此产生。1985 年 David Deutsch[2]深入地研究并证明了量子计算机比经典计算机有更强大的计算能力。1994 年 Peter Shor[3]在 Simon[4]研究的基础上提出了量子计算机上的大数质因子分解算法，其算法能够在多项式时间内完成，这对基于大数质因子分解和离散对数问题的公钥密码如 RSA 等提出了巨大的挑战。1996 年 Grover[5]提出了量子计算机上未加整理数据库的搜索算法，相对于经典的算法，提供了二次加速（quadratic speed-up）。很多学者[6-10]对 Grover 算法进行了研究，分别从计算复杂度、算法成功率和硬件实现等方面进行了改进。文献[11]证明 Grover 算法有唯一解的情况下为最优的算法，即以最少的计算次数和最大的成功率求解。针对 Grover 算法在多解时随着解个数接近 $N/2$ 成功率降低的情况（在解个数 $N/2$ 时成功率为 50%），文献[7]提出使用固定相位为 $\psi=\varphi=1.825\pi$ 的量子搜索算法，确保成功率不小于 98%，使得量子搜索算法的应用范围越来越广泛。对于 NP 问题的求解，常用量子计算方法是将其归结于隐含子群问题[12]，有效地利用量子 Fourier 变换和量子黑盒变换在指数时间内求解。背包问题是典型的 NP 完全问题，在经典算法中的计算复杂度为 $O(2^n)$，利用隐含子群的思想来分析背包问题得到其解 K 为平凡子群，因而不能实现指数级加速。文献[13]提出解向量唯一时的问题量子算法，但在解向量不唯一时，该算法不能有效地解决问题，本文提出多个解向量时的量子算法，并以 98%以上的成功率求解背包问题。

2 背包问题

背包问题是背包公钥密码的基础，其数学描述如下：

定义[14] 已知向量 $\boldsymbol{B}=(b_1,b_2,\cdots,b_n)$ 和常量 S，其中 $n\geqslant 3$，

基金项目：国家自然科学基金（the National Natural Science Foundation of China under Grant No.10501053）。
作者简介：钟普查（1982-），男，硕士，主要研究方向：量子计算；鲍皖苏（1966-），男，教授，博士生导师，主要研究方向：量子密码，公钥密码等；范得军（1983-），男，主要研究方向：信息安全；徐浩（1982-），男，主要研究方向：计算机应用。

收稿日期：2008-04-23 修回日期：2008-07-21

求解向量 $X_j=(x_1,x_2,\cdots,x_n)$ 满足 $\sum_{i=1}^{n} b_i x_i=S$ 的问题称为背包问题，其中 $1\leqslant j\leqslant 2^n$，$x_i\in\{0,1\}$，$N=2^n$。

背包公钥加密基于子集和问题。基本思想是选择一个特殊的子集和问题实例，然后将它伪装成一个很难求解的一般子集和问题实例。大多数背包公钥密码仅仅利用了背包问题中的一些特例作为私钥加密，如超递增背包，因此存在很多安全隐患。但背包问题本身确实是一个 NP 完全问题，对背包问题进行穷举攻击的计算复杂度为 $O(2^n)$。

3 固定相位量子搜索算法

算法使用一个 n 量子比特寄存器和一个 1 量子比特寄存器。

首先，对 n 量子比特寄存器初态置全零，$|s\rangle^{\otimes n}=|0\rangle^{\otimes n}$，将变换 U 作用在初态上，$U=H^{\otimes n}$，H 为 Hadamard 变换，得到均衡叠加态

$$|\phi\rangle=U|s\rangle^{\otimes n}=\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle=\sqrt{M/N}\,|\alpha\rangle+\sqrt{(N-M)/N}\,|\beta\rangle$$

$$|\alpha\rangle=\frac{1}{\sqrt{M}}\sum_x{}'|x\rangle,\ |\beta\rangle=\frac{1}{\sqrt{N-M}}\sum_x{}''|x\rangle$$

其中 $\sum_x{}'|x\rangle$ 表示解向量之和，$\sum_x{}''|x\rangle$ 为非解向量之和，M 为解向量的个数。令 $\sin\theta=\sqrt{M/N}$，$0<\theta<\pi/2$，则有 $|\phi\rangle=\sin\theta|\alpha\rangle+\cos\theta|\beta\rangle$。

其次，设变换

$$D=UR_s(\psi)U^{\dagger}R_t(\varphi)$$

$$R_s(\psi)=I-(1-e^{i\psi})|s\rangle\langle s|$$

$$R_t(\varphi)=I-(1-e^{i\varphi})|t\rangle\langle t|$$

$|t\rangle$ 为解向量，取 $\psi=\varphi=1.825\pi$。将变换 D 作用在 $|\phi\rangle$ 上，得到

$$|\phi^{(1)}\rangle=D|\phi\rangle=a_1|\alpha\rangle+b_1|\beta\rangle$$

$$a_1=\sin(\theta)(2\cos(\delta)e^{\psi i}+1),\ b_1=e^{i\psi}\cos(\theta)(2\cos(\delta)+1)$$

$$\cos(\delta)=2\sin^2(\theta)\sin^2(\psi/2)-1$$

假设经过 q 次 D 变换作用后以最高的概率得到目标向量。则有

$$|\phi^{(q)}\rangle=D^q|\phi^{(0)}\rangle=a_q|\alpha\rangle+b_q|\beta\rangle$$

$$a_q=\sin(\theta)(e^{\psi qi}U_q(y)+e^{\psi(q-1)i}U_{q-1}(y))$$

$$b_q=\cos(\theta)e^{\psi(q-1)i}(U_q(y)+U_{q-1}(y)),\ y=\cos(\delta)$$

$$U_q(y)=\sin((q+1)\delta)/\sin(\delta)$$

P^g 为此时测得解向量的概率

$$P^g=|a_q|^2\geqslant 98\%,\ q=\left\lfloor\frac{\psi}{2\sin\theta}\right\rfloor=O\left(\sqrt{\frac{N}{M}}\right)$$

通过检验算法的最终状态，无论解向量的数目如何，在 $O(\sqrt{N/M})$ 迭代后得到 $|\alpha\rangle$ 最小的几率幅 a_q。

引理 1[7] 固定相位 $\psi=\varphi=1.825\pi$ 的搜索算法使得迭代过程中，初始向量与目标向量之间的角度总能达到最小，且以最大概率测量得到目标向量。

引理 2[12] 当解的数目为 $N/2$ 时，无论迭代次数如果变化，Grover 算法测量得到目标向量的概率都为 50%。

由引理 1 与引理 2 的对比，显然可以发现固定相位 $\psi=\varphi=1.825\pi$ 搜索算法在多目标向量时算法的优势所在。

4 背包问题的量子算法

对背包问题分两种情况进行求解，即已知解向量个数和未知解向量个数。当解的个数唯一时，文献[13]中算法与以下算法的效率相当，但随着解向量个数接近 $N/2$ 时，以下算法的优势将明显表现出来。

4.1 已知解向量个数的背包问题量子计算算法

步骤 1 对第一寄存器的 n 量子比特初态置全 0，将变换 $U=H^{\otimes n}$ 作用在初态上得到均衡叠加态 $|\phi\rangle=\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle$，$x$ 的全部状态穷尽可能的解空间。

步骤 2 黑盒设置，当 $\sum_{i=1}^{n} b_i x_i=S$ 时 $f(X_i,B,S)=1$，标识 X_i 为正确解向量 $|s\rangle$，否则 $f(X_i,B,S)=0$。应用黑盒，对 $|\phi\rangle$ 执行 $R_s(\psi)$ 变换，$R_s(\psi)=I-(1-e^{i\psi})|s\rangle\langle s|$，然后执行 $UR_s(\psi)U^{\dagger}$ 变换 $UR_s(\psi)U^{\dagger}=I-(1-e^{i\varphi})|\phi\rangle\langle\phi|$，其中 $\psi=\varphi=1.825\pi$。

步骤 3 重复执行步骤 $2\sqrt{N/M}$ 次（M 为解的个数），对第一寄存器进行测量得到解向量。

4.2 解向量个数未知的背包问题量子计算算法

设 $1\leqslant M\leqslant N$（由于采用固定相位搜索算法所以不受文献[15]中 $1\leqslant M\leqslant 3N/4$ 的限制），算法如下：

步骤 1 初始化 $m=1$，设置 $\lambda=6/5$。

步骤 2 在小于 m 的非负整数中均匀地选择整数 k。

步骤 3 设置初态为 $\left(\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle,|0\rangle\right)$，调用 4.1 节中量子算法，将迭代次数由 $\sqrt{N/M}$ 次改为 k 次。

步骤 4 对第一寄存器的量子向量进行测量，如果测量的结果满足 $\sum_{i=1}^{n} b_i x_i=S$，则输出 $X_j=(x_1,x_2,\cdots,x_n)$；否则，继续。

步骤 5 重新设置 m，令 $m=\min(\lambda m,\sqrt{N})$，返回步骤 2。

4.3 算法分析

背包问题的量子算法主要使用 Hadamard 变换和相位旋转变换等基本量子门，这些硬件操作可以在多项式时间内完成，因此主要计算时间复杂度取决于量子黑盒的调用次数。在解向量个数已知的情况下黑盒调用次数为 $O(\sqrt{N/M})$，解向量个数未知的情况下黑盒调用次数为 $O(c\sqrt{N/M})$。

由固定态量子搜索算法的分析可知，当 $\psi=\varphi=\pi$ 时，该算法为初始的 Grover 算法，即 Grover 算法只是固定相位搜索算法的一个特例。但是，当解的个数 $M=N/2$ 时，Grover 算法只能以 50%的概率搜索到解向量。而固定相位 $\psi=\varphi=1.825\pi$ 量子搜索无论解的数目如何，都能保证 98%以上的成功率[7]。因此基于该算法之上的背包问题量子算法也同样保证成功率高于 98%。与文献[13]中的算法相比在多解时大大提高了算法的效率。

5 结束语

上述背包问题的量子算法主要应用固定相位 $\psi=\varphi=1.825\pi$ 的量子搜索算法，使得算法在多解的情况下成功率不小于

（下转 67 页）

由 R_t 的性质 $R_t(u,v)\geqslant v$ 知，式(6)显然成立。以下证明式(5)成立。设 $x\in E_y\cap K_y$，则

$$C(y)=\sup_{x\in E_y\cap K_y}\{A^*(x)\wedge(A(x)\to_t B(y))\}\geqslant$$

$$A^*(x)\wedge R_t(A(x),B(y))$$

这时，

$$M_{xy}\geqslant(A(x)\to_t B(y))\to_t(A^*(x)\to_t(A^*(x)\wedge(A(x)\to_t B(y))))=(A(x)\to_t B(y))\to_t((A^*(x)\to_t A^*(x))\wedge(A^*(x)\to_t(A(x)\to_t B(y))))=(A(x)\to_t B(y))\to_t(A^*(x)\to_t A(x)\to_t B(y)))\geqslant(A(x)\to_t B(y))\to_t(A(x)\to_t B(y))=1\geqslant\alpha$$

若 $x\notin E_y$，则 $t-A^*(x)>R_t(A(x),B(y))$，而 $A^*(x)\to_t C(y)\geqslant t-A^*(x)$，$M_{xy}=(A(x)\to_t B(y))\to_t(A^*(x)\to_t C(y))=1\geqslant\alpha$。

若 $x\notin K_y$，则 $t-\alpha\geqslant A^*(x)\wedge R_t(A(x),B(y))$，$\alpha\leqslant t-A^*(x)\wedge R_t(A(x),B(y))$，则 $\alpha\leqslant t-A^*(x)$ 且 $\alpha\leqslant t-R_t(A(x),B(y))$。

$$M_{xy}=(A(x)\to_t B(y))\to_t(A^*(x)\to_t C(y))\geqslant$$

$$(A(x)\to_t B(y))\to_t((t-A^*(x))\vee C(y))\geqslant$$

$$(A(x)\to_t B(y))\to_t\alpha\geqslant\alpha$$

其次证明 $B^*(y)$ 是满足式(2)的最小的 Fuzzy 集。

设对某个 $y\in Y$，$D(y)<B^*(y)$，则

$D(y)<\sup_{x\in E_y\cap K_y}\{A^*(x)\wedge(A(x)\to_t B(y))\}$ 且 $D(y)<\alpha$，这时有 $x_0\in E_y\cap K_y$，使得 $D(y)<A^*(x_0)\wedge R_t(A(x_0),B(y_0))$，则 $D(y)<A^*(x_0)$ 且 $D(y)<R_t(A(x_0),B(y_0))$。

由 $D(y)<A^*(x_0)$ 知，$A^*(x_0)\to_t D(y)=(t-A^*(x_0))\vee D(y)$，又 $x_0\in E_y$，则

$$t-A^*(x_0)\leqslant R_t(A(x),B(y))$$

$$(t-A^*(x_0))\vee D(y)\leqslant R_t(A(x_0),B(y))$$

则 $(A(x_0)\to_t B(y))\to_t(A^*(x_0)\to_t D(y))=$

$$(A(x_0)\to_t B(y))\to_t((t-A^*(x_0))\vee D(y))=$$

$$(t-(A(x_0)\to_t B(y)))\vee((t-A^*(x_0))\vee D(y))$$

又 $x_0\in K_y$，则 $t-A^*(x)\leqslant\alpha$，$t-(A(x_0)\to_t B(y))\leqslant\alpha$。$D(y)<\alpha$。所以 $(A(x_0)\to_t B(y))\to_t(A^*(x_0)\to_t D(y))<\alpha$，即用小于 B^* 的 D 替代 B^*，式(2)不成立。这就说明了 B^* 的最小性。

推论1 在定理3中，令 $t=1$，则得到逻辑系统 W 中的 α-三-I 算法。

参考文献：

[1] Zadeh L A.Outline of a new approach to the analysis of complex systems and decision processes[J].IEEE Trans，System，Man and Cybernetics，1973，1：28-44.
[2] 王国俊.模糊推理的全蕴涵三 I 算法[J].中国科学：E 辑，1999，29(1)：43-53.
[3] Wang Guo-jun.On the logic foundation of fuzzy reasoning[J].Information Science，1997，17(7)：47-88.
[4] 王国俊.模糊命题演算的一种形式演绎系统[J].科学通报，1997，42(10)：1041-1045.
[5] 马巧云，吴洪博.逻辑系统 H_t 中三-I 算法的另一种证明[J].计算机工程与应用，2008，44(7)：91-93.
[6] 吴洪博，马巧云.基于 L* 系统的一种非单调推理系统[J].陕西师范大学学报：自然科学版，2004，32(4)：4-8.
[7] 宋士吉，冯纯伯，吴从炘.关于模糊推理全蕴涵三 I 算法的约束理论[J].自然科学进展，2000，10(10)：884-889.
[8] 王国俊，兰蓉.系统 Ha 中的广义重言式理论[J].陕西师范大学学报：自然科学版，2003，31(2)：1-11.
[9] 王国俊.非经典数理逻辑与近似推理[M].北京：科学出版社，2000.

（上接64页）

98%，且迭代次数仍然为 $O(c\sqrt{N/M})$。同时由于使用固定相位搜索作为基本手段，使得量子计算中所用的硬件更少，减少硬件实现的难度。该算法没有使用任何经典的手段，因此可以推广到其他的 NP 完全问题的求解。

参考文献：

[1] Feynman R.Simulating physics with computers[J].Int Theor Phys，1982，21：467.
[2] Deutsch D.Quantum theory，the church-turing principle and universal quantum computer[C]//Proc R Soc，London，1985，400：97-117.
[3] Shor P W.Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J].SIAM Journal on Computing，1997，26(5)：1484-1509.
[4] Simon D R.On the power of quantum computation[C]//Proceeding of the 35th Annual IEEE Computer Society，Los Alamitos，1994：116-123.
[5] Grover L K.A fast quantum mechanics algorithm for database search[C]//Proceedings of the 28th ACM Symposium on Theory of Computation，New York，1996：212-219.
[6] Grover L K，Radhakrishnan J.Is partial quantum search of a database any easier?[C]//Proceedings of the 17th Annual ACM Symposium on Parallelixm in Algorithms and Architectures，2005：186-194.
[7] Younes A.Fixed phase quantum search algorithm.[2007].http://www.ArXiv/quant-ph 0704.1585v.
[8] Bonanome M，HIllery M，Bužek V.Application of quantum algorithms to the study of permutations and group automorphisms[J].Physical，Review A，2007，76：012324.
[9] Schutzhold R，Schaller G.Adiabatic quantum algorithms as quantum phase transition：First versus second order[J].Physical Review A，2006，74：060304.
[10] Kato G.Grover-algorithm-like operator using only single-qubit gates[J].Physical Review A，2005，72：032319.
[11] Zalka C.Grove's quantum searching algorithm is optimal[J].Physical Review A，1999，60(4)：2746-2751.
[12] Nielson M A，Chuang I L.Quantum computation and quantum information[M].Cambridge：Cambridge University Press，2000.
[13] 吕欣，冯登国.背包问题的量子算法分析[J].北京航空航天大学学报，2004，30(11).
[14] Menezes A J，van Oorschot P C，Vanstone S A.Handbook of applied cryptography[M].CRC Press LLC，1997：300-306.
[15] Boyer M，Brassard G，Hoyer P，et al.Tight bounds on quantum searching[J].Fortschritte der Physik，1998，46：493.