计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200800117

基于 Grover 搜索算法的整数分解

宋慧超　刘晓楠　王　洪　尹美娟　江　舵
数学工程与先进计算国家重点实验室(信息工程大学)　郑州 450000
(quantumsong@163.com)

摘　要　非结构化搜索是计算机科学中最基本的问题之一,而 Grover 量子搜索算法就是针对非结构化搜索问题设计的。Grover 量子搜索算法可用于解决图着色、最短路径排序等问题,也可以有效破译密码系统。文中提出基于 Grover 搜索算法并结合经典预处理实现整数分解。首先基于 IBMQ 云平台对不同量子比特的 Grover 算法量子电路进行了仿真,以及模拟使用 Grover 算法求解 N 的素因子 P 和 Q;然后将化简后的方程转化为布尔逻辑关系,以此来构建 Grover 算法中的 Oracle;最后通过改变迭代次数来改变搜索到解的概率。仿真结果验证了使用 Grover 算法求解素因子 P 和 Q 的可行性。文中实现了在搜索空间为 16 且一次 G 迭代条件下以近 78%的成功概率搜索到目标项。文中还比较了 Grover 算法与 Shor 算法在求解一些数字时所耗费的量子比特数和时间渐近复杂度的差异。通过 Grover 量子搜索算法分解整数的实验拓展了该算法的应用领域,Grover 算法的加速效果在大型搜索问题中尤为明显。

关键词:Grover 算法;VQF 算法;IBMQ;整数分解;Shor 算法
中图法分类号　TP385

Integer Decomposition Based on Grover Search Algorithm

SONG Hui-chao,LIU Xiao-nan,WANG Hong,YIN Mei-juan and JIANG Duo
State Key Laboratory of Mathematical Engineering and Advanced Computing,PLA Information Engineering University,Zhengzhou 450000,China

Abstract　One of the most fundamental problems in computer science is unstructured search,and Grover quantum search algorithm is designed for the unstructured search problem. Grover quantum search algorithm can be used to solve graph coloring, shortest path sorting and other problems,and it can also effectively decipher the cipher system. In this paper,Grover search algorithm combined with classical pretreatment is proposed to realize integer decomposition. Firstly,quantum circuits of Grover algorithm with different qubits are simulated based on IBMQ cloud platform,and the prime factors P and Q of N are simulated using Grover algorithm. Then,the simplified equation is transformed into Boolean logic relation to build Oracle in Grover algorithm. Finally,the probability of finding the solution is changed by changing the number of iterations. According to the experimental results of the simulation circuit,the feasibility of solving prime factors P and Q using Grover algorithm is verified,and the target item is searched with 78% probability of success under the condition of 16 search space and one G iteration. The differences of quantum bit number and time asymptotic complexity between Grover algorithm and Shor algorithm for solving some numbers are compared. The experiment of integer decomposition by Grover quantum search algorithm expands the application field of this algorithm,and the acceleration effect of Grover algorithm is especially obvious in large search problems.

Keywords　Grover algorithm,Variational quantum factoring algorithm,IBMQ,Integer factorization,Shor algorithm

1　引言

1996 年,Grover 开创性地提出了量子搜索算法。该方法通过放大目标解的出现概率,实现了对无序数据库的平方根加速[1],因其极大地推动了量子计算的发展而成为最经典的算法之一。

近年来,随着量子搜索算法的不断发展,已有许多学者在 Grover 算法的优化和应用方面取得了诸多研究成果。文献[2-3]提出部分扩散操作优化 Grover 算法,当搜索空间解的数目大于 $N/3$ 时,仅一次迭代就能以高于 90%的概率搜索到目标项。文献[4]针对目标项个数未知时 Grover 算法无法确定迭代次数的问题,提出新型量子计数改进方法。文献[5]提出的定点优化算法能够同时兼顾 Grover 搜索算法的概率和运行时间两个方面,即在目标项未知时能够避免因过度迭代

到稿日期:2020-08-19　返修日期:2020-11-19　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金项目(61972413,61701539);国家密码发展基金(mmjj20180212)
This work was supported by the National Natural Science Foundation of China(61972413,61701539) and National Cryptography Development Fund(mmjj20180212).
通信作者:刘晓楠(prof.liu.xn@foxmail.com)

而导致成功概率降低，并实现最佳时间缩放。文献[6]证明了相较于经典搜索算法而言 Grover 搜索算法是最优的。文献[7]将 Grover 迭代自适应算法应用于约束多项式二进制优化问题，相较于暴力破解而言提供了二次加速。Ruan 等[8]将 Grover 算法融入机器学习的主成分分析中，对原算法起到了平方根加速的效果。文献[9]实现了应用 Grover 搜索算法对高级加密标准（Advanced Encryption Standard，AES）进行密钥搜索，并优化了量子线路的深度。Wang 等[10]应用 Grover 算法进行哈希原象攻击，并将时间复杂度优化至 $O(2^{n/3})$。文献[11]提出将 Grover 搜索算法应用于字符串比较，通过设计一种特殊的 Oracle 结构，能够实现并行比较字符串的所有字母，从而提高整体的性能。

Grover 量子搜索算法可用于图着色[12]、最短路径排序等问题的求解，还可以有效破译 AES 密码体系。变分量子整数分解算法（Variational Quantum Factoring Algorithm，VQF）是一种混合经典量子算法[13]，其目的和 Shor 算法一样，都是对整数进行分解，差别在于 VQF 用二进制表示整数 N、因子 P 和 Q，通过因子 P 和 Q 的二进制乘法得到相关方程，最终转化为求 p_i 和 q_j 的问题（p_i，q_j 分别表示因子 P，Q 二进制的第 i 位和第 j 位）。本文通过 Grover 算法对 p_i 和 q_j 进行求解，达到分解整数 N 的目的。

IBMQ 是一个可以通过量子门电路和量子程序设计语言对相应的量子算法进行模拟仿真的云平台。它提供基本的量子门和量子比特，能实现量子比特的各种幺正变换和测量操作。本文将在 IBMQ 云平台上对不同比特的 Grover 算法进行模拟，以及实现 Grover 算法对因子 P，Q 问题的模拟验证，最后通过实验结果验证所提想法的可行性。

本文第 2 节介绍 Grover 算法的主要过程、VQF 的算法原理以及应用 Grover 算法求解 P，Q 的主要步骤；第 3 节通过 IBMQ 平台模拟不同比特 Grover 算法，并重点对文中提出的结合经典预处理的 Grover 算法求解 P，Q 进行实验模拟；第 4 节介绍不同比特 Grover 算法的实验结果，以及搜索概率、量子比特数、线路深度随迭代次数的变化情况，并对实验结果进行分析；最后对实验结果进行总结，重申该实验的可行性和重要意义，指出该实验的局限性并对未来工作进行展望。

2　Grover 算法和 VQF 算法

2.1　Grover 的主要步骤

Grover 量子搜索算法主要是通过变换量子基态的概率幅，从而令所查询目标项对应的量子基态的概率幅达到最大[14]。图 1 给出了一个完整的 Grover 算法量子线路框架，其中涵盖初始化至等权叠加态、中间的 Oracle（$\boldsymbol{U}_w$）、平均反演算子（$\boldsymbol{U}_s$）和最终的测量模块。Oracle 和平均反演算子组成一个完整的 G 迭代，可通过重复 G 迭代来改变所有量子态的概率。

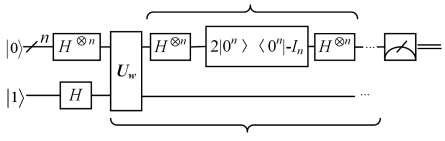

图 1　Grover 算法框架线路图

Fig. 1　Frame circuit diagram of Grover algorithm

（1）初始化制备等权叠加态。对输入基态进行 Hadamard 变换得到所有计算基态的等权叠加态，如式（1）所示。图 2 为初始化的原理图。

$$|\boldsymbol{s}\rangle = H^{\otimes n}|00\cdots0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n+1}|x\rangle \tag{1}$$

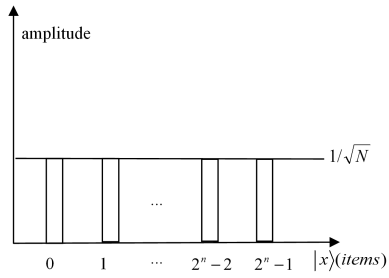

图 2　制备等权均匀叠加态

Fig. 2　Preparation of equal weight uniform superposition state

（2）构造 Oracle。通过构造一个映射 $\boldsymbol{U}_w$，该映射使得目标项的相位反转，但对于任何与目标项正交的其他项的符号不变，即若 $|\boldsymbol{a}\rangle$ 为目标项，$\langle \boldsymbol{a}|\boldsymbol{v}\rangle = 0$，则 $\boldsymbol{U}_w|a\rangle = -|a\rangle$，$U_w|\boldsymbol{v}\rangle = |\boldsymbol{v}\rangle$。图 3 给出了 $\boldsymbol{U}_w$ 作用后各项的状态，其中深色为目标项。

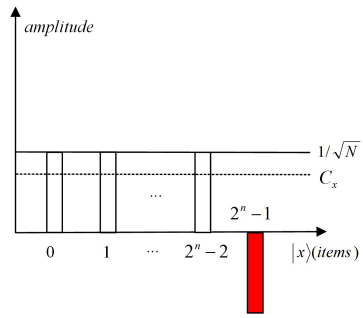

图 3　经 $\boldsymbol{U}_w$ 作用后将目标状态相位反转

Fig. 3　Inverting the phase of target state after $\boldsymbol{U}_w$ action

（3）构造平均反演算子。构造一个幺正矩阵 $\boldsymbol{U}_s$，该幺正矩阵可将目标状态振幅相对于平均振幅 C_x 做翻转，从而达到增大搜索到目标项概率的目的，其中 C_x 是所有态的平均振幅。图 4 给出了经 $\boldsymbol{U}_s$ 作用后各个状态的变化。

$$\boldsymbol{U}_s = 2|\boldsymbol{s}\rangle\langle\boldsymbol{s}| - \boldsymbol{I} \tag{2}$$

$$C_x = \frac{1}{N}\sum_x C_x \tag{3}$$

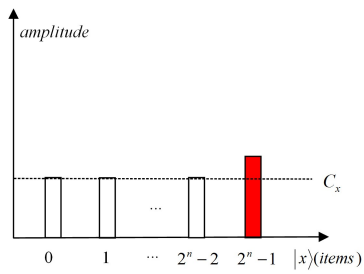

图 4　经 $\boldsymbol{U}_s$ 作用后将目标项相较于平均振幅做翻转

Fig. 4　Reversing the target relative to average amplitude after $\boldsymbol{U}_s$ action

（4）重复迭代。步骤（2）和（3）合称 G 变换，随着 G 迭代次数的增加，搜索到目标项的概率也会发生改变，当迭代至最优时能够以较高的概率搜索到目标项。

2.2 VQF 算法的主要步骤

VQF 是由 Zapata 公司研究人员开发出的一种经典加量子的混合算法。首先利用经典方法简化方程个数，然后量子部分是利用量子近似优化算法(Quantum Approximate Optimization Algorithm，QAOA)[15-16]求哈密顿量的基态，成功地将分解问题转化为优化问题，通过哈密顿量方程求出的近似解。量子近似优化算法是门线路下优化问题的求解算法，有利于在嘈杂中型量子(Noisy Intermediate Scale Quantum，NISQ)背景下投入实用。

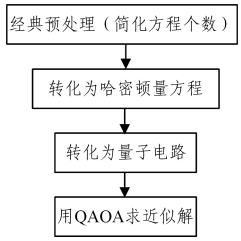

图 5 VQF 算法主要过程框架图

Fig. 5 Main process frame diagram of VQF algorithm

(1)首先将整数分解问题转化为优化问题，将需要分解的整数 N 及其因子 P，Q 用二进制表示，构建二进制乘法表。此处以表 1 中的分解整数 143 为例，根据初始条件假设 P，Q 两个因子的二进制位等长且等于 N 二进制位长的一半，因为 P，Q 两个因子均为质数，故将 P 和 Q 二进制的最高位和最低位置 1。表 1 前两行为因子 P 和 Q 的二进制表示，由于整数 143 的二进制表示需要 8 位，故 P 和 Q 需要 4 位二进制表示。z_{ij} 表示二进制相乘求和过程中从第 i 位向第 j 位的进位。

表 1 143 的二进制乘法表

Table 1 Binary multiplication table of 143

P					1	p_2	p_1	1
Q					1	q_2	q_1	1
					1	p_2	p_1	1
				q_1	p_2q_1	p_1q_1	q_1	
			q_2	p_2q_2	p_1q_2	q_2		
		1	p_2	p_1	1			
	z_{67}	z_{56}	z_{45}	z_{34}	z_{23}	z_{12}		
	z_{57}	z_{46}	z_{35}	z_{24}				
N	1	0	0	0	1	1	1	1

(2)根据二进制相乘得到的方程组，引入文献[17]提出的约束条件来进一步减少方程组的个数。最终将方程组化简为式(4)－式(6)这 3 个方程。

$$p_1+q_1=1 \tag{4}$$

$$p_2+q_2=1 \tag{5}$$

$$p_2q_1+p_1q_2=1 \tag{6}$$

(3)构造伊辛哈密顿量 $\boldsymbol{H}_c$，并利用 QAOA 计算 $\boldsymbol{H}_c$ 的基态。

$$\boldsymbol{H}_c=(\hat{p}_1+\hat{q}_1-1)^2+(\hat{p}_2+\hat{q}_2-1)^2+(\hat{p}_2\hat{q}_1+\hat{p}_1\hat{q}_2-1)^2 \tag{7}$$

(4)对近似基态进行测量，得到哈密顿量方程的最终近似解。

2.3 Grover 算法在求解 P 和 Q 中的应用

(1)制备等权叠加态，通过 Hadamard 门将量子基态变换为叠加态。

(2)根据 VQF 的步骤(2)中得到的简化方程可以构建 Grover 算法中的 Oracle。简化后式(4)－式(6)中的变量 p_1，p_2，q_1，q_2 都属于二元域。首先将方程转化为布尔逻辑关系，如式(8)所示，并根据式(8)中的逻辑关系构造 Oracle(具体量子线路模块如第 3 节图 8 的第一、第二虚线之间区域所示)。为便于理解布尔逻辑关系，可将式(8)进一步简化得到易理解的式(9)，从式(9)容易看出通过 Oracle 构造的 2 个目标项。

$$(p_1 \vee q_1) \wedge (p_2 \vee q_2) \wedge [(p_1 \wedge q_2) \vee (p_2 \wedge q_1)] \tag{8}$$

$$(p_1 \wedge \neg p_2 \wedge \neg q_1 \wedge q_2) \vee (\neg p_1 \wedge p_2 \wedge q_1 \wedge \neg q_2) \tag{9}$$

(3)构造反演算子($\boldsymbol{U}_s$)来增加搜索到目标项的概率，其中反演算子的数学公式如式(2)所示。然后根据式(2)来构建量子电路($\boldsymbol{U}_s$电路模块的具体构建如第 3 节图 8 第二、第三虚线之间区域所示)。

(4)Grover 算法中 Oracle($\boldsymbol{U}_w$)和反演算子($\boldsymbol{U}_s$)合称为 G 迭代(如图 8 中第一、第三虚线之间模块)。通过重复 G 迭代来改变搜索到目标项的概率。理论上，当 G 迭代的次数在 $\left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil$ 附近时(其中 N 为待搜索元素的总个数，M 为目标项元素的个数)，Grover 算法搜索到目标项的概率达到最优。在本文分解 143 的 Grover 搜索线路中，当迭代次数为 2 时，搜索到目标项的成功概率达到最优。

3 基于 IBMQ 的 Grover 算法模拟

IBMQ 是一个云应用程序，用于对真实的量子硬件和高性能模拟器进行编程，可通过两种方式在量子计算机上运行。第一种是使用 Circuit composer 对经典量子算法进行可视化创建，Circuit composer 是一种图形量子编程工具，可让用户通过拖放指令来构建量子电路并在真实的量子硬件上运行。第二种是使用 Qiskit[18]，Qiskit 是一个用于编程量子计算机的开源框架，可以通过 Qiskit 代码实现量子算法。本文首先使用 Circuit composer 对 Grover 算法进行创建。然后利用 Qiskit 探究多次迭代下搜索概率与线路深度、量子比特的关系。文中实验所使用的元器件均为通用门，如 H 门、X 门、C-Z 门、C-NOT(又称 C-X)门、Toffoli(又称 CCX)门。

本节通过 IBMQ 的相关门电路对 Grover 算法不同量子比特进行仿真模拟。首先基于 2 qubits Grover 搜索线路，从 4 个状态中搜索 1 个目标项(本文以目标项$|00\rangle$为例构造 Oracle，进行一次 G 变换)。实验线路图如图 6 所示。

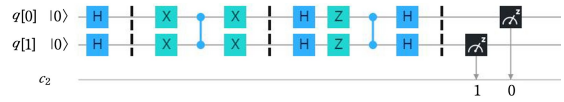

图 6 2 qubits 的 Grover 搜索线路

Fig. 6 Grover search circuit of 2 qubits

然后将 2 qubits 搜索线路扩展至 3 qubits 的 Grover 搜索线路，从$|000\rangle$，$|001\rangle$，…，$|111\rangle$ 8 个状态中搜索 2 个目标项(本文以目标项$|101\rangle$和$|110\rangle$为例构造 Oracle，同样进行一次 G 变换)，3 qubits Grover 算法对应的实验线路图如图 7 所示。

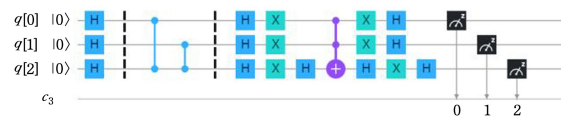

图 7 3 qubits 的 Grover 搜索线路

Fig. 7 Grover search circuit of 3 qubits

本文重点在于实现 Grover 算法求解因子 P 和 Q，并以分解整数 143 为例设计量子搜索线路。图 8 给出了该算法进行一次 G 迭代的 9 qubits Grover 搜索线路，通过布尔逻辑关系式(9)，在 Oracle 中(第一、二条虚线之间的区域)构造两个目标项(即待分解的解 p_1，q_1，p_2，q_2)。值得注意的是，在此处构造 Oracle 时引入了 5 个辅助比特来实现布尔关系式(9)。然后构造平均反演算子改变搜索到目标项的概率(见图 8 中第二、三条虚线之间的区域)。两个黑框合称为一次 G 变换。本文通过增加 G 迭代的次数来观察所用量子比特数、线路深度、搜索到目标项的概率的变化，从而对实验结果进行分析。

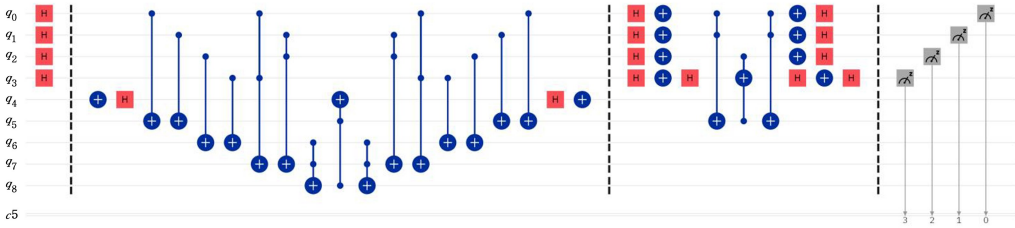

图 8　9 qubits 的 Grover 搜索线路(含 5 个辅助比特)

Fig. 8　9 qubits Grover search circuit(including 5 auxiliary qubits)

4　实验结果

图 9 给出了 2 qubits Grover 算法的运行结果，该算法进行 4 选 1，线路深度为 8，仅通过一次 G 迭代就可以使搜索到目标项|00⟩的概率趋向于 1，其他非目标项概率趋近于 0(默认以下实验结果后端均是基于 ibmq_qasm_simulator，运行次数设定为 8 192)。

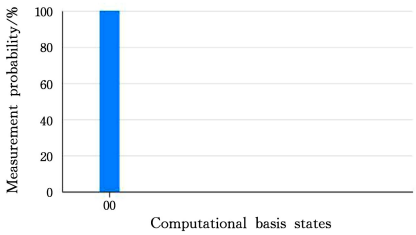

图 9　2 qubits Grover 算法运行结果

Fig. 9　Running results of Grover algorithm with 2 qubits

图 10 给出了在搜索空间为 8 时查找 2 个目标项的运行结果，线路深度为 10，即仅通过一次 G 迭代就能以 100%的成功概率搜索到目标项|101⟩，|110⟩中的一个。

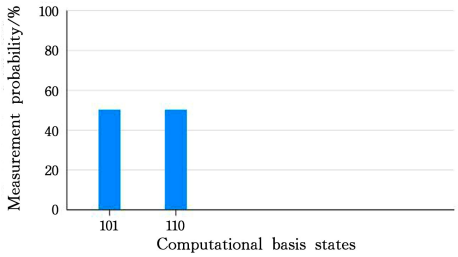

图 10　3 qubits Grover 算法运行结果

Fig. 10　Running results of Grover algorithm with 3 qubits

接下来使用 Grover 算法搜索 $p_1\,q_1\,p_2\,q_2$ 的运行结果图。伴随着 G 迭代次数的增加，在 Grover 算法中搜索到目标项的概率、量子线路深度也相应地发生变化。

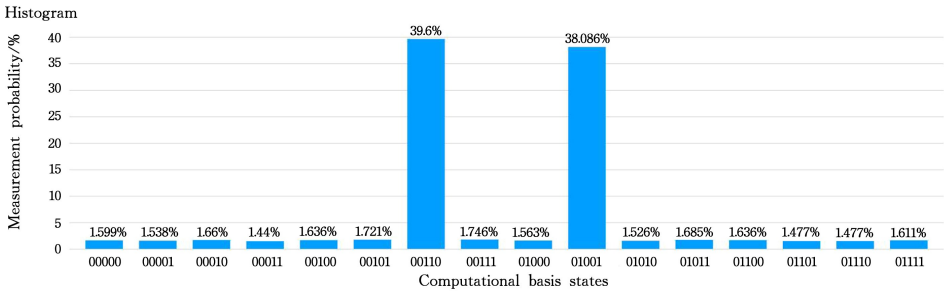

图 11　Grover 算法一次迭代的运行结果

Fig. 11　Running results of Grover algorithm with one iteration

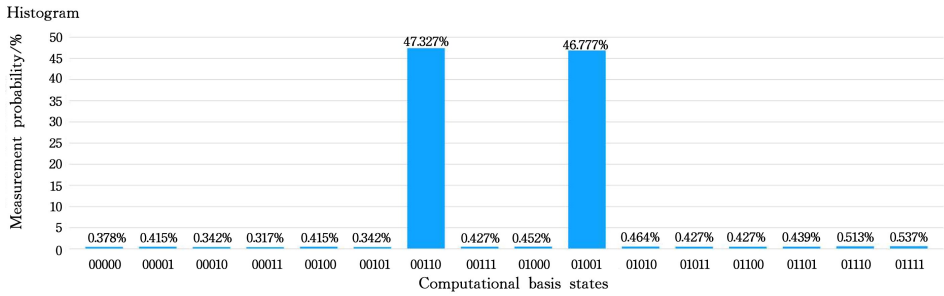

图 12　Grover 算法两次迭代的运行结果

Fig. 12　Running results of Grover algorithm with two iterations

图 11 和图 12 分别是 Grover 算法一次 G 迭代和二次 G 迭代的运行结果。由实验结果可知，该算法分别以近 78%，94%的概率搜索到 $p_1q_2p_2q_2$ 的解。为充分观察搜索概率与迭代次数间的内在关系，通过 Qiskit 进行多次迭代并记录实验结果。表 2 详细列出了 Grover 算法搜索因子时成功概率与迭代次数之间的关系，以及随着迭代次数的增加对应量子比特数、量子线路深度的变化，同时对该 Grover 搜索算法的理论概率和实际概率进行比较。由实验结果可知，随着 Grover 算法迭代次数的增加，线路所需要的量子比特数不变，但是线路深度会越来越深。由于该算法实验是基于 ibmq_qasm_simulator(理想模拟器)的，故得到的概率与理论计算概率几乎一致。当 Grover 算法迭代两次后，搜索到目标项的概率达到最大(近 94%)，然后随着迭代的继续搜索概率出现下降。当迭代次数为 4 时，搜索成功概率甚至低于直接搜索概率(2/16)。从表 2 中的数据可以看出，在不考虑量子计算机水平受限的情况下，选择两次迭代可以使搜索到目标项的成功概率(近 94%)最优。实际上仅一次迭代所达到的近 78%的成功概率已经比较可观。

表 2 Grover 算法不同迭代次数搜索概率和线路深度的关系

Table 2 Relationship between search probability and circuit depth with different iteration times of Grover algorithm

迭代次数	比特数	深度	理论概率	实际概率
1	9	22	0.78126	0.77686
2	9	42	0.94531	0.94104
3	9	62	0.33001	0.32900
4	9	82	0.01221	0.01200

图 11、图 12 中成功概率最高的两项都是 $p_1q_1p_2q_2$ 对应的解，不难发现解分别为 0110 和 1001(即 p_1，q_1，p_2，q_2 可取任意一个)，故 $N=143$ 的两个因子为 $P=1p_1p_21$，$Q=1q_1q_21$(或 $P=1q_1q_21$，$Q=1p_1p_21$)，容易得到两个因子分别为 11 和 13。该线路不仅可对 143 进行分解，还可以对能化简成式(4)—式(6)的任意大数进行分解。

表 3 列出了一些经验证符合求解 143 Grover 算法线路的数字，并对比分解不同数字时 Shor 算法和 Grover 算法所需的量子比特数及对应的复杂度。

表 3 用两种算法分解不同规模数字所用量子比特数和时间复杂度

Table 3 Qubits and time complexity used to decompose numbers of different sizes by two algorithms

N	Short 算法		Grover 算法	
	量子比特数	时间复杂度	量子比特数	时间复杂度
143	18		9	
3599	26		9	
25217	32		9	
110633	36	$O(\log N)$	9	$O(\sqrt{N})$
731021	42		9	
1520273	44		9	
16850989	52		0	

Shor 算法[19]在分解数字时加速效果明显，能将问题规模降至 $O(\log N)$。Shor 算法在文献[20]中将所用量子比特数优化至 $2n+2$(其中 n 为待分解整数的二进制位数)。表 3 中 Shor 算法所用量子比特数随着整数的变大增速明显，当分解 16850989(25 位)时需要 52 qubits。经过预处理后的 Grover 算法在处理符合 143 线路大数时所用的量子比特数(9 qubits)不发生改变，相比 Shor 算法在处理此类数字时所用的量子比特数目更少，因此在量子计算机水平受限的今天更容易实现。

结束语 量子计算是现代理论物理和计算机科学相结合的一个前沿领域，其依靠纠缠和叠加的量子现象来进行运算，相较于经典计算在许多方面都具有明显的优势。量子算法是量子处理器硬件充分发挥计算能力的神经中枢，与量子计算的加速能力息息相关。量子计算速度快的优势也为处理复杂经典问题提供了新的方向，从而实现性能上的飞跃。考虑到受当前量子计算机硬件发展水平的限制，本文利用 IBMQ 提供的量子模拟器 ibmq_qasm_simulator 对结合经典预处理的 Grover 算法在求解 P 和 Q 的问题上进行模拟，通过分析不同迭代次数下该算法所需量子比特数、线路深度、搜索到目标项的概率，验证了 Grover 算法在该问题上的可行性。文中还对比了分解不同规模数字时 Shor 算法和结合了经典预处理的 Grover 搜索算法所用到量子比特数目的差异，说明了应用 Grover 算法分解因子的现实意义。Grover 算法在实际模拟中，由于依赖于核心模块的多次迭代来提高概率幅，故而核心模块具体实现所耗的量子资源对整个算法的模拟影响巨大。对于 Grover 来说，用于区分目标态的 Oracle 往往需要较深的线路，如何优化其线路深度，使其能在资源受限的量子平台上高效执行是目前各界关注的一大难题。经实验证明，量子线路的深度改变对其实验结果的影响大于其宽度的变化。目前的一个优化方向是在构建 Oracle 时通过引入辅助量子比特来减少线路的深度，即以线路宽度的增加来降低其整体的深度，从而达到优化实验线路、降低噪声的影响、提高实验结果中搜索成功概率的目的。未来工作可以从以下两个方面着手：1)实现 Grover 算法分解整数所用量子比特数随着经典步骤中方程的进一步简化而减少；2)通过线路优化降低量子线路深度。

参 考 文 献

[1] GROVER L K. A Fast Quantum Mechanical Algorithm for Database Search [C]// Proceedings 28th ACM Symposium on Theory of Computation. New York, 1996: 212-219.

[2] YOUNES A, ROWE J, MILLER J. A Hybrid Quantum Search Engine: A Fast Quantum Algorithm for Multiple Matches[C]// Proceedings of ICENCO. 2006.

[3] YOUNES A, ROWE J, MILLER J. Quantum Search Algorithm with More Reliable Behavior Using Partial Diffusion[C]// Proceedings of the seventh International Conference on Quantum Communication, Measurement and Computing. 2004: 171-174.

[4] AARONSON S, RALL P. Quantum Approxim- ate Counting, Simplified[J]. arXiv: 1908. 10846.

[5] YODER T J,LOW G H,CHUANG I L. Fixed-Point Quantum Search with an Optimal Number of Queries[J]. Physical Review Letters,2014,113(21):210501.

[6] ZALKA C. Grover's Quantum Searching Algori- thm is Optimal [J]. Physical Review A,1999,60(4):2746-2751.

[7] GILLIAM A,WOERNER S,GONCIULEA C. Grover Adaptive Search for Constrained Polynomial Binary Optimization[J]. arXiv:1912.04088,2019.

[8] RUAN Y,CHEN H W,LIU Z H,et al. Quantum Principal Component Analysis Algorithm[J]. Chinese Journal of Computers,2014,37(3):666-676.

[9] JAQUES S,NAEHRIG M,ROETTELER M,et al. Implementing Grover Oracles for Quantum Key Search on AES and LowMC [M]// Advances in Cryptology—EUROCRYPT 2020. 2020.

[10] WANG P,TIAN S P,SUN Z W,et al. Quantum Algorithms for Hash Preimage Attacks[J]. Quantum Engineering,2020,2(2).

[11] VIKRAM M. Quantum String Comparison Method[J]. arXiv: 2005.08950,2020.

[12] AMIT S,DEBASRI S,AMLAN C. Circuit Design for K-coloring Problem and It's Implementation on Nearterm Quantum Devices [J]. arXiv:2009.06073,2020.

[13] ANSCHUETZ E R,OLSON J P,ASPURU-GUZIK A,et al. Variational Quantum Factoring [J]. arXiv:1808.08927,2018.

[14] GILLIAM A,VENCI C,MURALIDHA-RAN S,et al. Foundational Patterns for Efficient Quan-tum Computing[J]. arXiv: 1907.11513,2019.

[15] ALAM M,ASH-SAKI A,GHOSH S. Analysis of Quantum Approximate Optimization Algorithm under Realistic Noise in Superconducting Qubits [J]. arXiv:1907.09631,2019.

[16] WILLSCH M,WILLSCH D,JIN F,et al. Benchmarking the Quantum Approximate Optimization Algorithm[J]. Quantum Information Processing,2020,19(7):197.

[17] XU N Y,ZHU J,LU D W,et al. Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System[J]. Physical Review Letters,2012,108(13):130501.

[18] CROSS A. The IBM Q Experience and QISKit Open-Source Quantum Computing Software[C]// APS March Meeting 2018. American Physical Society,2018.

[19] SHOR P W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer[J]. Siam Review,1999,41(2):303-332.

[20] YASUHIRO T,NOBORU K. AQuantum Circuit for Shor's Factoring Algorithm Using $2n+2$ Qubits [J]. Quantum Information and Computation 2006,6(2):184-192.

SONG Hui-chao, born in 1996, postgraduate. His main research interests include quantum algorithm and so on.

LIU Xiao-nan, born in 1977, Ph.D, associate professor, master's supervisor, is a member of China Computer Federation. His main research interests include quantum algorithm and high-performance parallel computation.