文章编号:1005-4642(2022)04-0007-06

基于量子计算原理的 Shor 算法优越性验证

刘安航†,李浩昱†,关　佳,张志华,方　恺,赫　丽,沈　军
(同济大学 物理科学与工程学院,上海 200092)

摘　要:从理论上分析了分解大数质因子的量子算法——Shor 算法,将大数的质因子分解问题转换为求解函数的周期问题. 设计了基于 Shor 算法的实验,并通过比较应用于求解同一函数时量子计算方法和经典计算方法分别需要的运算次数. 实验结果表明:量子计算方法在函数的周期求解问题中仅需要多项式级别的复杂度,从而证明了量子计算在大数的质因子分解问题中具有明显的优越性.

关键词:Shor 算法;量子并行计算;量子傅里叶变换
中图分类号:O413　　**文献标识码**:A　　DOI:10.19655/j.cnki.1005-4642.2022.04.002

经典计算机需要信息的载体、逻辑操作、状态读出等一系列基本元素. 量子计算机用量子比特作为量子信息的载体,对量子比特进行初始化、操控和读出等,再通过一系列的逻辑操作构成量子算法,从而实现特定的计算目的. 比特是经典计算和经典信息中的基本概念,量子计算和量子信息则建立在类似的概念——量子比特的基础上. 经典计算机中,比特有 0 和 1 两种状态,利用 0 和 1 构成的比特串编码分别表示不同的信息. 而在量子计算机中,信息单元被称为量子比特,除了可以处于 0 态或 1 态外,还可以处于叠加态. 借助叠加态,可以实现利用较少的量子比特储存更多的信息.

Shor 算法由 P. W. Shor 在 1994 年提出,是针对整数分解问题在量子计算机上运作的算法[1],该算法可以解决如下问题:给定整数 N,找出其质因数. 现有的经典算法还无法有效地解决该问题[1-2],因此 Shor 算法展示了量子计算的优越性. 此外,Shor 算法的存在也直接威胁到经典通讯的 Rivest-Shamir-Adleman(RSA)加密算法. 所以关于 Shor 算法的相关研究一直备受瞩目,2019 年 Aidan Dang 等人详细介绍了优化 Shor 算法的高阶经典模拟技术,利用检查电路的纠缠特性,有效地将其映射到矩阵乘积状态的一维结构中并对其进行了优化[3];2020 年在 IEEE 第 5 届计算通信与自动化国际会议上,Vaishali Bhatia 等人提出了用 Shor 算法破解 RSA 的高效量子计算技术[4].

目前我国在量子计算领域也颇有建树,2017 年中国科学技术大学杜江峰院士团队基于核磁共振系统和绝热量子计算模型在 Shor 算法中实现了 6 位数 291 311 的因式分解[5];2020 年,段兆臣等人使用量子点单光子源成功编译了 Shor 算法[6];2021 年,中国科学院量子信息与量子科技创新研究院潘建伟、朱晓波、彭承志等人组成的研究团队成功研制了 62 比特可编程超导量子计算原型机“祖冲之号”[7].

本文的设计思路来自于近代物理实验课程中的量子密钥分发虚拟仿真实验[8],并参考了一些与量子纠缠和量子保密通信相关的实验[9-13]. 设计出了基于 Shor 算法的实验,首先将质因数分解问题转换为求函数的周期问题,然后通过拟定已

“第 11 届全国高等学校物理实验教学研讨会“论文
收稿日期:2021-07-09;修改日期:2021-11-15
基金项目:教育部产学合作协同育人项目(No. 202002123019);同济大学实验教学改革项目(No. 202149)
作者简介:刘安航(2001—),男,辽宁锦州人,同济大学物理科学与工程学院 2018 级本科生. E-mail:1853725@tongji.edu.cn
李浩昱(2000—),男,江西南昌人,同济大学物理科学与工程学院 2018 级本科生. E-mail:1852468@tongji.edu.cn
通讯作者:关　佳(1992—),女,山西忻州人,同济大学物理科学与工程学院助教,博士,主要从事物理实验教学和量子光学研究. E-mail:227guanjia@tongji.edu.cn
†:共同第一作者,对本文贡献相同.

知函数和未知函数，从理论上对这 2 个函数进行实验与分析，得出实验次数 n（该实验次数是指为了获得正确的周期结果所需要的运算次数或者选取次数）. 通过实验发现量子方法需要的实验次数仅仅正比于要分解的大数 N，而经典计算方法需要的实验次数为 n^n. 因此，由于量子算法的并行性，Shor 算法在质因子分解问题中存在显著的优势.

1 实验原理

1.1 量子比特

在量子计算机中，信息单元被称为量子比特，除了可以处于 0 态或 1 态外，还可处于叠加态. 用$|0\rangle$和$|1\rangle$表示量子比特可取的状态基矢，单个量子比特可取的值为

$$|\Psi\rangle=\alpha|0\rangle+\beta|1\rangle, \tag{1}$$

其中，α 和 β 为复数. 因为存在约束条件 $\alpha\alpha^*+\beta\beta^*=1$，量子比特可写成

$$|\Psi\rangle=\cos\frac{\theta}{2}|0\rangle+\mathrm{e}^{\mathrm{i}\varphi}\sin\frac{\theta}{2}|1\rangle, \tag{2}$$

其中，θ 和 φ 为实数且 $-\pi\leqslant\theta\leqslant\pi$，$0\leqslant\varphi\leqslant2\pi$.

1.2 量子逻辑门

经典计算中用到很多的基本逻辑门，包括与门、或门、非门、与非门、或非门、异或门等，这些元件组合在一起可以构成用来计算函数的电路. 量子计算机也由一系列的量子逻辑门组合而成，并以此来完成复杂的计算任务. 但是量子计算机利用的是量子态的相干叠加性、纠缠性以及量子态演化的幺正性等，因此量子逻辑门与经典逻辑门存在较大的差异. 其中，哈达玛门（Hadamard gate，简写为 H 门）可对单个量子比特进行操作，使其处于叠加态，即将基态$|0\rangle$转变为$\frac{|0\rangle+|1\rangle}{\sqrt{2}}$（等概率的所有态的集合），基态$|1\rangle$转变为$\frac{|0\rangle-|1\rangle}{\sqrt{2}}$；泡利-X 门（Pauli-X gate）相当于经典的逻辑非门，可将基态$|0\rangle$转变为$|1\rangle$，或将基态$|1\rangle$转变为$|0\rangle$；泡利-Y 门（Pauli-Y gate）可使单量子比特绕布洛赫球 y 轴使目标基态旋转 180°；泡利-Z 门（Pauli-Z gate）可保留基态$|0\rangle$不变，将基态$|1\rangle$转变为$|-1\rangle$；可控非门（C-Not gate）可操作 2 个量子比特，实心表示控制量子比特，空心圆表示目标量子比特，当控制量子比特为$|1\rangle$时，目标量子比特将发生翻转，否则保持不变. 此外，量子傅里叶变换门等也可以实现复杂运算.

1.3 量子并行计算

量子并行性使得量子计算机可以在同一时间计算函数 $f(x)$ 在多个不同 x 值处的函数值. 对于 b 位的量子存储器而言，可以同时存储 2^b 个数字（态），在量子力学中，对 b 个量子位的寄存器的一般态可表示为

$$|\Psi\rangle=\sum_{x=0}^{2^b-1}c_b\,|x\rangle, \tag{3}$$

其中，$|c_b|^2$ 表示取得对应值的概率. 由于储存了 2^b 个不同的态，使用 1 次量子逻辑门可以同时改变 2^b 个态的 c_b 值，改变了 2^b 个信息，即为量子并行计算[14].

1.4 量子傅里叶变换

在函数的周期求解问题中，量子傅里叶变换（Quantum Fourier transform，QFT）为

$$F(|x\rangle)=\frac{1}{\sqrt{2^b}}\sum_{k=0}^{2^b-1}\exp\left(\mathrm{i}\frac{2\pi x}{2^b}k\right)|k\rangle. \tag{4}$$

式(4)表示对任意量子态$|x\rangle$做傅里叶变换，得到以波矢 k 展开的表达形式，其中，$k=0,1,\cdots,2^b-1$.

QFT 同样可以构成逻辑门，其 QFT 门矩阵表示为

$$QFT_N=\frac{1}{\sqrt{2^b}}\begin{pmatrix}1&1&1&\cdots&1\\1&\omega&\omega^2&\cdots&\omega^{(2^b-1)}\\1&\omega^2&\omega^4&\cdots&\omega^{2(2^b-1)}\\\vdots&\vdots&\vdots&\ddots&\vdots\\1&\omega^{(2^b-1)}&\omega^{2(2^b-1)}&\cdots&\omega^{(2^b-1)(2^b-1)}\end{pmatrix}, \tag{5}$$

其中，$\omega=\exp\left(\frac{2\pi\mathrm{i}}{2^b}\right)$[15]. 当输入如式(3)所示 1 个存储器中的量子态时，通过该量子逻辑门可以完成对 2^b 个态的同时变换，因此 QFT 体现了量子并行计算的特点.

1.5 素数因子分解问题转换为求周期问题

已知大数 N，存在唯一的质因子分解 $N=P_1P_2$，求 P_1 和 P_2. 求解质因子分解问题的步骤包括：

1）随机取大于 1 的正整数 y，使得 $y<N$，且 y 和 N 互质，即 $\gcd(y,N)=1$，其中 gcd 表示最大公约数. 定义使 $y^r\equiv1(\mathrm{mod}\ N)$的最小正整数 r 称为 y 关于 N 的阶数，其中 mod 表示同余运算.

2）若 r 为奇数，则另取 1 个大于 1 的正整数 y，继续求 r，直到 r 为偶数.

3）若 r 为偶数，取 $x\equiv y^{r/2}(\mathrm{mod}\ N)$，则 $x^2\equiv 1(\mathrm{mod}\ N)$，进而有

$$x^2-1\equiv 0(\mathrm{mod}\ N), \tag{6}$$

即

$$(x+1)(x-1)\equiv 0(\mathrm{mod}\ N). \tag{7}$$

于是可设

$$(x+1)(x-1)=tN=tP_1P_2=uvP_1P_2, \tag{8}$$

其中，t,u,v 为正整数，进而有

$$(x+1)(x-1)=(uP_1)(vP_2). \tag{9}$$

式(7)解为

$$x+1\equiv 0(\mathrm{mod}\ P_1), \tag{10}$$

$$x-1\equiv 0(\mathrm{mod}\ P_2), \tag{11}$$

即

$$P_1=\gcd(x+1,N), \tag{12}$$

$$P_2=\gcd(x-1,N). \tag{13}$$

其中，$\gcd(x,N)$ 可由辗转相除法求得. 因此，若求得大于 1 的正整数 y 关于 N 的阶数 r，则可求出 P_1 和 P_2.

令 $y^x\equiv z(\mathrm{mod}\ N)$，因 $y^r\equiv 1(\mathrm{mod}\ N)$，则对任意正整数 h 有

$$y^{x+hr}\equiv z(\mathrm{mod}\ N), \tag{14}$$

即以 N 为模的函数 $f(x)=y^x$ 的周期就是 y 关于 N 的阶数 r. 素数因子分解问题，转换为求函数 $f(x)\equiv a^x(\mathrm{mod}\ N)$ 的周期问题，其中 a 为大于 1 的正整数[16].

2　实验内容

Shor 算法原理的装置图如图 1 所示，图中的 2 个寄存器负责储存数字信息.

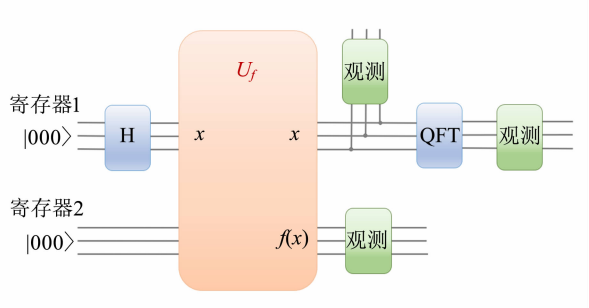

图 1　Shor 算法实验装置图

H 门的特点是当输入为零（基态）时，例如 $|000\rangle$，H 门会将其转变为等概率的所有态的集合，即 $\frac{1}{\sqrt{2^3}}\sum_{x=0}^{2^3-1}|x\rangle$. U_f 门表示通过一系列幺正变换将 x 与 $f(x)$ 之间建立纠缠，当 x 被观测到时，另一侧 $f(x)$ 的观测值也随之确定. 观测门表示读出寄存器此时所储存的数字信息.

算法流程为寄存器 1 作为 $|x\rangle$，在经过 H 门后储存所有的数字信息，寄存器 2 经过幺正变换与存储器 1 中的 x 建立纠缠并储存函数信息. 完成上述流程后得到

$$|\psi_0\rangle=\frac{1}{\sqrt{2^b}}\sum_{x=0}^{2^b-1}|x\rangle\,|f(x)\rangle, \tag{15}$$

式(15)表明经过变换后，若对初态 $|\psi_0\rangle$ 进行观测，将得到 2^b 个出现概率相同的态，而当每个态的 $|x\rangle$ 确定后，相应的 $|f(x)\rangle$ 值也随之确定.

观测 $f(x)$ 时将使其坍缩为 $f(x_0)$，由于存在周期性，这时 x 会坍缩成 x_0+jT_0（T_0 为周期，$j=0,1,2,\cdots,m_0-1$），需要指出的是此处总的周期数 $m_0=N/T_0$，如不满足则需做进一步处理[1]. 这里只讨论 $m_0=N/T_0$ 的情况，可得

$$|\psi\rangle=\frac{1}{\sqrt{m_0}}\sum_{j=0}^{m_0-1}|x_0+jT_0\rangle\,|f(x_0)\rangle. \tag{16}$$

由于观测到 $f(x_0)$ 会使得 x 坍缩成只与正整数 j 有关的值 x_0+jT_0，此时 x 与 $f(x)$ 之间不再存在函数关系（量子纠缠关系），即式(16)可分离（两寄存器之间退相干）.

寄存器 1 在分离后可以表示为

$$|\phi\rangle=\frac{1}{\sqrt{m_0}}\sum_{j=0}^{m_0-1}|x_0+jT_0\rangle, \tag{17}$$

对寄存器 1 进行 QFT，即经过 QFT 门可得到

$$F(|x_0+jT_0\rangle)=\frac{1}{\sqrt{2^b}}\sum_{k=0}^{2^b-1}\exp\left[\mathrm{i}\frac{2\pi k}{2^b}(x_0+jT_0)\right]|k\rangle. \tag{18}$$

所以有

$$F(|\phi\rangle)=\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\exp\left(\mathrm{i}\frac{2\pi k}{N}x_0\right)|k\rangle\cdot\left[\frac{1}{\sqrt{m_0}}\sum_{j=0}^{m_0-1}\exp\left(\mathrm{i}\frac{2\pi k}{m_0}j\right)\right], \tag{19}$$

最终可以得到

$$F(|\phi\rangle)=\frac{1}{\sqrt{T_0}}\sum_{k=0}^{T_0-1}\exp\left(\mathrm{i}\frac{2\pi k}{T_0}x_0\right)|km_0\rangle. \tag{20}$$

此时进行测量，将得到等概率的 T_0 个 $|km_0\rangle$，将其与 N 进行约分，得到的约分式分母将恰好为待求解的周期 T_0. 可能存在 k 与 T_0 有公约数的情况，分式可继续约分，这一情况将在第 3 部分进行讨论.

$$\frac{km_0}{N}=\frac{k}{T_0}\ (k=0,1,2,\cdots,T_0-1). \tag{21}$$

经典计算方法同样可以按照图 1 装置图进行实验，仅需要在 QFT 门前对 x 进行观测.

3 实验结果与讨论

3.1 周期测定

3.1.1 已知函数

假定已知函数为

$$f(x)=\begin{cases}0, x\text{ 为偶数};\\ 1, x\text{ 为奇数},\end{cases} \tag{22}$$

即函数周期为 2.

设寄存器 1 为 3 位量子比特，即 $b=3$. 寄存器 2 根据 $f(x)$ 的值设置为 1 位量子比特. 根据式(15)初始化赋予两寄存器纠缠态，对式(15)中的 $f(x)$ 进行测量，假设得到 $f(x)=0$，由于两寄存器处于纠缠态，此时寄存器 1 坍缩为

$$|\psi_1\rangle=\frac{1}{\sqrt{4}}(|0\rangle+|2\rangle+|4\rangle+|6\rangle). \tag{23}$$

对式(23)进行 QFT，可以得到的结果为

$$|\psi_2\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|4\rangle). \tag{24}$$

实际上在 $f(x)=1$ 时进行 QFT 能够得到同样的结果，±号对应 $f(x)=1$ 和 $f(x)=0$ 的 2 种情况，即各有 1/2 的概率得到 $|0\rangle$ 或 $|4\rangle$，当得到 $|0\rangle$ 时，应舍去，当得到 $|4\rangle$ 时，根据

$$\frac{km}{N}=\frac{4}{8}=\frac{1}{2}, \tag{25}$$

可得最终周期为 2.

3.1.2 未知函数

在实际的质因数分解中，已知条件仅为函数存在周期. 假定函数周期为 $T=16$，选择 $b=6$，即 $N=2^6=64$. 进行 QFT，可以得到结果为

$$|\psi_2\rangle=\frac{1}{\sqrt{T}}(|0\rangle\pm|4\rangle\pm|8\rangle\pm|12\rangle\pm\cdots\pm|60\rangle), \tag{26}$$

在所有的 $f(x)$ 值下进行 QFT 都能得到相同结果，即等概率得到以上的 T 个解，注意 T 为未知量，需要多次测量来确定 T 的实际取值，该计算将在 3.2 节中展开. 对所得数据进行处理运算，约分得到下列值

$$\frac{k}{T}=\left[0,\frac{1}{16},\frac{1}{8},\frac{3}{16},\frac{1}{4},\frac{5}{16},\cdots,\frac{15}{16}\right]. \tag{27}$$

由式(27)可知有些值与周期并不相符，可推断在测量次数较少时，并不能正确分辨待测定的周期值. 所以需要多次测量，并选取最大的分母，作为最终的周期值，即 16. 由此可见该算法并不能在单次测量中得到 100%正确的周期值.

3.2 测量次数的确定

3.2.1 经典计算方法

经典计算方法的运算流程为：在通过 U_f 门后，直接观测 x 和 $f(x)$ 的值. 假定函数周期为 T，由于 x 与 $f(x)$ 之间存在纠缠关系，多次重复观测可发现，当观测到相同的 $f(x)$ 时，对应的观测量 x 之间的差值必定是 T 的整数倍. 这样观测相同的 $f(x)$ 值下 x 之间的差值，取最小值作为周期 T.

在经典计算方法中使正确率达到 99%的运算次数，可以分为 2 个步骤：

1)选择相同的 $f(x)$，由于 $N=mT$，则单次实验的选取成功率为 $P(1)=1/m$.

2)在相同的 $f(x)$ 中，选取相邻的 x 值，根据排列组合，并做相应简化，得到成功率达到 99%时，对应的选取次数为 $\frac{2}{\lg[m/(m-2)]}$.

返回 1)，为进行 $\frac{2}{\lg[m/(m-2)]}$ 次测量，需要取得 $\frac{2}{\lg[m/(m-2)]}$ 次相同的 $f(x)$ 值. 最终选取次数为 $\frac{2}{\lg[m/(m-1)]}^{\frac{2}{\lg[m/(m-2)]}}$ 时，选取成功率为 $99\%^{\frac{2}{\lg[m/(m-2)]}}$，可将其近似认为是 99%，但需注意该选取次数实际上仍不能使正确率达到 99%.

由于 m 不能确定，将 m 用 N 来表示，运算结果如图 2 所示，其中横坐标为要选取的大数 N，纵坐标表示在对数坐标下的选取次数，红色点是对应大数 N 下计算得到的运算次数在坐标空间内的点，对应的选取次数在对数坐标下与 N 基本呈正相关，当 N 在 10^4 附近时，就需要 $10^{1.2\times10^5}$ 次选取，这样计算量巨大，难以达到要求. 如果分别计算两步骤的选取次数，就可以得到 2 次的选取次数均与 N 呈正比例关系，即最终的表达式为 $c_0N^{d_0N}$（c_0 和 d_0 均为比例系数）. 因此，在经典计

算方法下，大数质因子分解问题的复杂度为指数级别 $O(n^n)$.

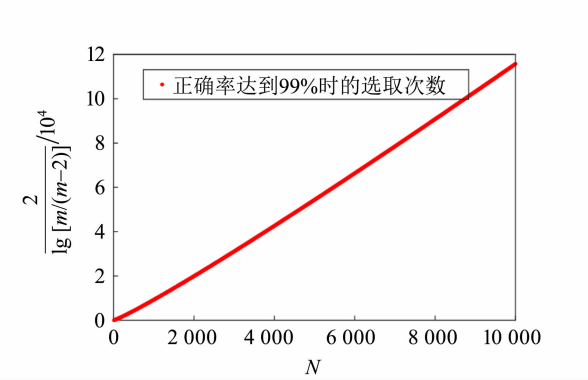

图 2　对数坐标系下选取次数与大数 N 的散点图

3.2.2　量子方法

根据上面的计算，进行 QFT 后共存在等概率的 T 个结果，一定能够保持分母为 T 值的 2 个量分别为 $1/T$ 和 $(T-1)/T$. 所以每次测量至少有 $P=2/T$ 概率得到想要的值. 在 n 次测量后得到该值的概率为

$$P=1-\left(\frac{T-2}{T}\right)^n, \tag{28}$$

由于式(28)中的周期并不能事先确定，因此需要选取更大的大数 N 值. 为了保证结果的准确性，需要从理论上分析选取次数与正确率的关系，如图 3 所示.

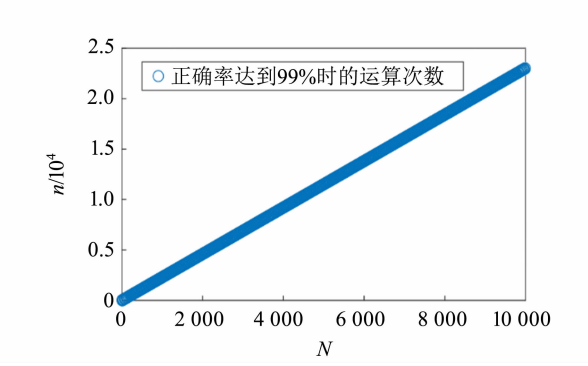

图 3　运算次数与大数 N 的散点图

图 3 中横坐标为选择的大数 N，纵坐标为在正确率为 99%时需要的运算次数，蓝色圆圈是对应周期下计算得到的运算次数在坐标空间内的点. 由图 3 可知对应的运算次数 n 与大数 N 呈正相关. 这说明在量子计算方法下，仅需要多项式级别的复杂度 $O(n)$ 就可以解决大数的质因子分解问题.

4　结束语

将量子计算方法与经典计算方法进行比较，得出在量子算法中分解质因数的复杂度为多项式级别 $O(n)$，而经典计算方法中分解质因数的复杂度为指数级别 $O(n^n)$. 因为量子计算具有并行性，即在量子算法中，1 个量子门可以对其储存的 2^b 个数据同时进行运算，省去了经典计算方法中逐个进行计算的过程. 本实验中，量子傅里叶变换门同时对 2^b 个数据展开运算，直接得到了包含 T 个数字的等概率的波函数，降低了计算的复杂程度. 本文对设计的实验进行了数值上的模拟和计算，验证和解释了 Shor 算法的运行机制以及量子计算的优越性.

参考文献：

[1] Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring [C]//Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994:124-134.

[2] Shor P W. Polynomial-time algorithm for prime factorization and discrete logarithms on a quantum computer [J]. SIAM Journal on Computing, 1997, 26(5):1484-1509.

[3] Dang A, Hill C D, Hollenberg L, et al. Optimising matrix product state simulations of Shor's algorithm [J]. Quantum, 2019,3:116.

[4] Bhatia V, Ramkumar K R. An efficient quantum computing technique for cracking RSA using Shor's algorithm [C]//2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA), 2020:89-94.

[5] Li Z K, Dattani N S, Chen X, et al. High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311 [J/OL]. [2021-06-30]. https://arxiv.org/pdf/1706.08061.pdf.

[6] Duan Z C, Li J P, Qin J, et al. Proof-of-principle demonstration of compiled Shor's algorithm using a quantum dot single-photon source [J]. Optics Express, 2020,28(13):18917-18930.

[7] Gong M, Wang S Y, Zha C, et al. Quantum walks on a programmable two-dimensional 62-qubit superconducting processor [J]. Science, 2021, 372(6545):948-952.

[8] 国家虚拟仿真实验教学课程共享平台. 量子秘钥分发虚拟仿真实验[EB/OL]. (2017-04-16)[2021-06-30]. http://www.ilab-x.com/details/v5?id=4297&isView=true.
[9] 齐雅静,车修平,孙梦琳,等. 基于液晶电光效应的量子密钥分发演示实验[J]. 物理实验,2020,40(6):1-8.
[10] 孙文博,王合英,陈宜保,等. Ⅰ类量子纠缠实验教学系统[J]. 物理实验,2016,36(6):1-5.
[11] 许穆岚,刘乃乐. 基于 BB84 协议的量子保密通信实验[J]. 物理实验,2014,34(11):27-29,33.
[12] 孙文博,王合英,陈宜保,等. 量子纠缠实验中 SPDC 光谱分布的计算分析与实验研究[J]. 物理实验,2014,34(11):1-5.
[13] 王合英,孙文博,陈宜宝,等. 光量子纠缠态的制备和测量实验[J]. 物理实验,2009,29(3):1-5,13.
[14] 莫露洁. 量子计算机的研究与应用综述[J]. 桂林航天工业高等专科学校学报,2008,13(1):29-31.
[15] 彭卫丰. Shor 量子算法的优化及模拟实现[D]. 无锡:江南大学,2008.
[16] 霍红卫,潘征. 大数质因子分解的量子算法[J]. 计算机工程与科学,2003,25(1):23-25.

Verifying the superiority of Shor algorithm based on the principle of quantum computing

LIU An-hang†, LI Hao-yu†, GUAN Jia,
ZHANG Zhi-hua, FANG Kai, HE Li, SHEN Jun
(School of Physics Science and Engineering, Tongji University, Shanghai 200092, China)

Abstract: The quantum algorithm for decomposing the prime factors of large numbers, that is the Shor algorithm, was analyzed theoretically, and the problem of decomposing the prime factors of large numbers was transformed into the problem of solving the period of a function. Experiments based on Shor algorithm were designed. By comparing the number of operations required to solve the quantum computational method and the classical computational method respectively when applied to the same function, it could be concluded that the quantum computational method requires only polynomial-level complexity in the problem of solving the period of a function. This conclusion demonstrated the obvious superiority of quantum computing in the problem of decomposition of large numbers by prime factors.

Key words: Shor algorithm; quantum parallel computation; quantum Fourier transform
[责任编辑:任德香]