第25卷 第2期 湖 南 工 业 大 学 学 报 Vol.25 No.2
2011年3月 Journal of Hunan University of Technology Mar. 2011

Shor 算法的腔 QED 实现

吴琴琴

（湖南理工学院 物理与电子学院，湖南 岳阳 414000）

摘　要：基于阶梯形三能级原子与经典和量子腔场之间的共振相互作用，提出了一个在腔量子电动力学（QED）系统中实现Shor算法的方案，并具体介绍了实现Shor算法的操作方法。

关键词：Shor 算法；腔量子电动力学；幺正变换

中图分类号：O431.2　　**文献标志码**：A　　**文章编号**：1673-9833(2011)02-0001-04

Implementation of Shor′s Algorithm in Cavity QED

Wu Qinqin

（Department of Physics and Electronics, Hunan Institute of Science and Technology, Yueyang Hunan 414000, China）

Abstract: Based on the resonant interaction of three-level ladder-shaped atom and classic quantum cavity, proposes an implementation of Shor′s algorithm via a cavity QED scheme and introduces the operational method to achieve the algorithm.

Keywords: Shor′s algorithm; cavity quantum electrodynamics; unitary transformation.

0　引言

量子算法使得量子计算机的计算速度大幅度提高，可以快速地求解某些问题，其中最典型的例子就是Shor分解大数质因子量子算法[1-3]。与已知的经典算法相比，运用该算法进行大数分解能获得指数加速。该算法中最简单的情况（整数N=15的分解）已经在核磁共振系统中得到了实现[4]，但在实现过程中退相干问题较为严重。最近在文献[5]中提出了一个在腔量子电动力学（QED）系统中实现控制非（CNOT）门的方法，该方法可以极大地减少腔场退相干因素的影响。基于这种实现方法，通过控制阶梯形三能级原子和腔肠的相互作用，笔者提出一个在腔QED系统中实现Shor算法的理论方案。

1　Shor 分解大数质因子的量子算法

Shor算法的具体过程在文献[1-3]中已有详细介绍。算法将分解大数N的质因子转化为求一个小于N且与N互质的随机数a的阶。数a的阶定义为使

$$a^r(\mathrm{mod}\ N)=1(\mathrm{mod}\ N) \quad (1)$$

成立的最小非零整数r，这里$a^r(\mathrm{mod}\ N)$表示a^r除以N的余数。式（1）表示相对模N，a^r和1同余。构造函数$f(x)=a^x(\mathrm{mod}\ N)$，则数$a$的阶就是函数$f(x)$的周期。假设求得函数$f(x)$的周期$r$，并假设$r$是偶数，且$a(\mathrm{mod}\ N)\neq -1$（否则需另取$a$值重新计算），那么$N$的因子可通过计算$N$和$(a^{r/2}\pm 1)$的最大公约数获得。

求随机数a的阶在经典领域是难解问题，Shor的发现就在于他找到了求数a阶的有效量子算法。量

收稿日期：2011-01-11

基金项目：湖南省教育厅科研基金资助项目（10A026）

作者简介：吴琴琴（1979-），女（土家族），湖南常德人，湖南理工学院讲师，博士，主要从事量子信息方面的研究，

E-mail：wu_qinqin1979@yahoo.com.cn

子计算机可通过在2个量子处理器W和A上进行一系列量子操作，有效地找到a的阶r，其中W表示有n个量子位的工作处理器，用来存放初始输入的x值，而函数值$f(x)$储存在有m个量子位的辅助处理器A中。工作处理器和辅助处理器中的量子比特个数分别为满足关系$N^2<q=2^n<2N^2$和$2^{m-1}<N<2^m$的整数，其中q是工作处理器希尔伯特空间的维数。要将整数N=15进行分解，所需进行的量子操作如图1中线路所示[3]。

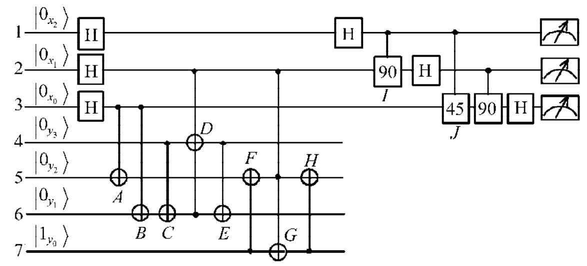
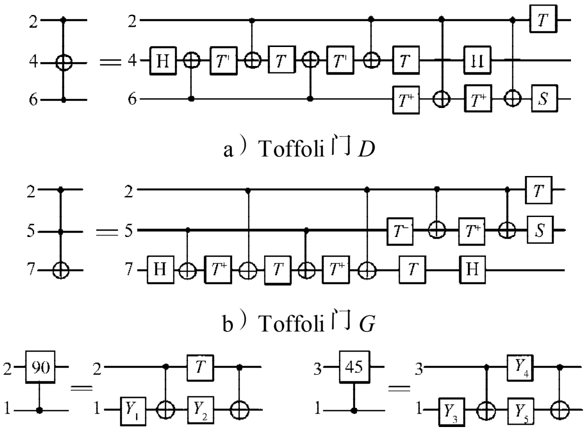


图1 Shor算法的实现线路图(N=15, a=7)

Fig. 1 Quantum circuit for implementing Shor's algorithm (N=15, a=7)

2 Shor算法的腔QED实现

下面给出当N=15，a=7时，Shor算法在腔QED中的实现方案。在腔QED中实现Shor算法需完成图1线路中的Toffoli门操作D和G，控制相移操作I和J及单量子逻辑门操作，其中单量子比特门操作可简单地通过原子和经典场的相互作用来实现。经分析知道每个Toffoli门可分解成为6个CNOT门、2个Hadamard操作、7个π/8(T)门和1个相位(S)门的组合[2]; 控制相位门I可分解成2个CNOT门，2个$Y_i(i=1, 2)$操作和1个T门的组合; 控制相位门J可分解成2个CNOT门和3个$Y_i(i=3, 4, 5)$操作的组合，如图2所示。



a）Toffoli门D

b）Toffoli门G

c）控制相位门I

d）控制相位门J

图2 Shor算法的腔QED实现线路图

Fig. 2 Quantum circuit for implementing Shor's algorithm in cavity QED

图2中的操作$T, T^\dagger, Y_i(i=1, 2, 3, 4, 5)$和$S$可表示为下面的矩阵形式，即

$$\boldsymbol{T}=\begin{pmatrix}1 & 0\\ 0 & \mathrm{e}^{\mathrm{i}\frac{\pi}{4}}\end{pmatrix},\ \boldsymbol{T}^\dagger=\begin{pmatrix}1 & 0\\ 0 & \mathrm{e}^{-\mathrm{i}\frac{\pi}{4}}\end{pmatrix},\ \boldsymbol{Y}_1=\begin{pmatrix}0 & 1\\ \mathrm{e}^{\mathrm{i}\frac{\pi}{4}} & 0\end{pmatrix},$$

$$\boldsymbol{Y}_2=\begin{pmatrix}0 & \mathrm{e}^{-\mathrm{i}\frac{\pi}{4}}\\ 1 & 0\end{pmatrix},\ \boldsymbol{Y}_3=\begin{pmatrix}0 & 1\\ \mathrm{e}^{\mathrm{i}\frac{\pi}{8}} & 0\end{pmatrix},\ \boldsymbol{Y}_4=\begin{pmatrix}1 & 0\\ 0 & \mathrm{e}^{\mathrm{i}\frac{\pi}{8}}\end{pmatrix},$$

$$\boldsymbol{Y}_5=\begin{pmatrix}0 & \mathrm{e}^{-\mathrm{i}\frac{\pi}{8}}\\ 1 & 0\end{pmatrix},\ \boldsymbol{S}=\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix},$$

它们又可以进一步表示成单比特绕z-和y-轴的旋转操作的组合，即

$$\boldsymbol{T}=\mathrm{e}^{\mathrm{i}\frac{\pi}{8}}\boldsymbol{R}_z^{\frac{\pi}{4}},\ \boldsymbol{S}=\mathrm{e}^{\mathrm{i}\frac{\pi}{4}}\boldsymbol{R}_z^{\frac{\pi}{2}},\ \boldsymbol{Y}_1=\mathrm{e}^{-\mathrm{i}\frac{3\pi}{8}}\boldsymbol{R}_y^{\pi}\boldsymbol{R}_z^{-\frac{5\pi}{4}},$$

$$\boldsymbol{Y}_2=\mathrm{e}^{-\mathrm{i}\frac{5\pi}{8}}\boldsymbol{R}_y^{\pi}\boldsymbol{R}_z^{-\frac{5\pi}{4}},\ \boldsymbol{Y}_3=\mathrm{e}^{-\mathrm{i}\frac{7\pi}{16}}\boldsymbol{R}_y^{\pi}\boldsymbol{R}_z^{-\frac{9\pi}{8}},\ \boldsymbol{Y}_4=\mathrm{e}^{\mathrm{i}\frac{\pi}{16}}\boldsymbol{R}_z^{\frac{\pi}{8}},$$

$$\boldsymbol{Y}_5=\mathrm{e}^{-\mathrm{i}\frac{9\pi}{16}}\boldsymbol{R}_y^{\pi}\boldsymbol{R}_z^{-\frac{9\pi}{8}},$$

式中的旋转操作定义为：

$$\boldsymbol{R}_z^{\frac{\pi}{4}}=\mathrm{e}^{-\mathrm{i}\frac{\pi\boldsymbol{\sigma}_z}{8}},\ \boldsymbol{R}_z^{\frac{\pi}{2}}=\mathrm{e}^{-\mathrm{i}\frac{\pi\boldsymbol{\sigma}_z}{4}},\ \boldsymbol{R}_z^{-\frac{5\pi}{4}}=\mathrm{e}^{\mathrm{i}\frac{5\pi\boldsymbol{\sigma}_z}{8}},$$

$$\boldsymbol{R}_z^{-\frac{9\pi}{8}}=\mathrm{e}^{\mathrm{i}\frac{9\pi\boldsymbol{\sigma}_z}{16}},\ \boldsymbol{R}_z^{\frac{\pi}{8}}=\mathrm{e}^{-\mathrm{i}\frac{\pi\boldsymbol{\sigma}_z}{16}},\ \boldsymbol{R}_y^{\pi}=\mathrm{e}^{-\mathrm{i}\frac{\pi\boldsymbol{\sigma}_y}{2}}。$$

利用图2中Toffoli门操作和控制相移操作的实现线路，可仅利用单比特操作和CNOT操作来实现图1中的Shor算法。

下面将指出Shor算法线路中的所有幺正操作都可以在腔QED系统中得到实现。为实现幺正操作，需使用7个阶梯形三能级原子，其能级分别用$|g\rangle_j$，$|e\rangle_j$和$|i\rangle_j$表示，其中下标$j(j=1, 2, \cdots, 7)$表示第j个原子。图3所示为原子的能级结构图。

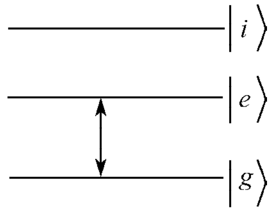


图3 阶梯形三能级原子的能级图

Fig. 3 The level diagram of the ladder-type three-level atom

2.1 Hadamard变换的实现

让原子j通过2个经典电磁场，这2个电磁场的频率与原子$|g\rangle_j \leftrightarrow |e\rangle_j$的转换频率相同。在相互作用表象中，场和原子的相互作用哈密顿量为

$$\boldsymbol{V}(t)=-\frac{\hbar\Omega}{2}\left(\mathrm{e}^{-\mathrm{i}\phi}|e\rangle_{jj}\langle g|+\mathrm{e}^{\mathrm{i}\phi}|g\rangle_{jj}\langle e|\right),$$

式中：$|e\rangle_j$和$|g\rangle_j$分别表示第j个原子的激发态和基态。调节经典场的振幅和频率以及原子和场的相互作用时间，使得原子在场中依次经历如下转换

$$|g\rangle_j\xrightarrow[\phi=0]{\Omega t=\pi}\mathrm{i}|e\rangle_j\xrightarrow[\phi=-\pi/2]{\Omega t=\pi/2}\mathrm{i}\left[\frac{1}{\sqrt{2}}\left(|g\rangle_j+|e\rangle_j\right)\right],$$

$$|e\rangle_j\xrightarrow[\phi=0]{\Omega t=\pi}\mathrm{i}|g\rangle_j\xrightarrow[\phi=-\pi/2]{\Omega t=\pi/2}\mathrm{i}\left[\frac{1}{\sqrt{2}}\left(|g\rangle_j-|e\rangle_j\right)\right],$$

若用原子态$|e\rangle$和$|g\rangle$分别编码量子比特$|1\rangle$和$|0\rangle$，上式就代表Hadamard变换。

2.2 操作$\boldsymbol{R}_y^{\pi}$的实现

通过与2.1节相同的方法，调节经典场的振幅和频率以及原子和场的相互作用时间，使得原子j经历如下转换

$$|g\rangle_j\xrightarrow[\phi=-\pi/2]{\Omega t=\pi}|e\rangle_j,\quad |e\rangle_j\xrightarrow[\phi=-\pi/2]{\Omega t=\pi}-|g\rangle_j,$$

这个转换对应于单量子比特旋转门$\boldsymbol{R}_y^{\pi}$。

2.3 操作$\boldsymbol{R}_Z^{\theta_k}$的实现

绕z轴的旋转操作$\boldsymbol{R}_Z^{\theta_k}$定义为

$$\boldsymbol{R}_Z^{\theta_k}=\begin{pmatrix}\exp(-\mathrm{i}\theta_k/2) & 0\\ 0 & \exp(\mathrm{i}\theta_k/2)\end{pmatrix},$$

式中：$\theta_k=\frac{\pi}{4},\frac{\pi}{2},-\frac{5\pi}{4},-\frac{9\pi}{8}$和$\frac{\pi}{8}$。

为了实现这些旋转操作$\boldsymbol{R}_Z^{\theta_k}$，需要让第$j$个原子依次通过3个经典场，调节经典场的振幅和频率以及原子和场的相互作用时间，使得原子j经历如下转换

$$|g\rangle_j\xrightarrow[\phi=\pi/2]{\Omega t=\pi/2}\frac{1}{\sqrt{2}}\left(|g\rangle_j+|e\rangle_j\right)\xrightarrow[\phi=\pi]{\Omega t=\theta_k}$$
$$\frac{1}{\sqrt{2}}\mathrm{e}^{-\mathrm{i}\theta_k/2}\left(|g\rangle_j+|e\rangle_j\right)\xrightarrow[\phi=-\pi/2]{\Omega t=\pi/2}\mathrm{e}^{-\mathrm{i}\theta_k/2}|g\rangle_j,$$

$$|e\rangle_j\xrightarrow[\phi=\pi/2]{\Omega t=\pi/2}\frac{1}{\sqrt{2}}\left(|e\rangle_j-|g\rangle_j\right)\xrightarrow[\phi=\pi]{\Omega t=\theta_k}$$
$$\frac{1}{\sqrt{2}}\mathrm{e}^{\mathrm{i}\theta_k/2}\left(|e\rangle_j-|g\rangle_j\right)\xrightarrow[\phi=-\pi/2]{\Omega t=\pi/2}\mathrm{e}^{\mathrm{i}\theta_k/2}|e\rangle_j。$$

若用原子态$|e\rangle$和$|g\rangle$分别编码量子比特$|1\rangle$和$|0\rangle$，上式就对应于单量子比特旋转门$\boldsymbol{R}_Z^{\theta_k}$。

2.4 CNOT门的实现

假定原子3和1分别充当控制比特和目标比特，通过如下3个步骤即可实现两者之间的CNOT门操作[5]。

第1步：让原子1通过2个经典场，这2个电磁场的频率分别与原子$|g\rangle\leftrightarrow|e\rangle$和$|e\rangle\leftrightarrow|i\rangle$的转换频率相同。调节经典场的振幅和相位使得原子1和3组成的系统经历如下转换

$$\begin{cases}|g\rangle_3|g\rangle_1\xrightarrow[\phi=-\pi/2]{\Omega t=\pi/2}\frac{1}{\sqrt{2}}|g\rangle_3\left(|g\rangle_1-|e\rangle_1\right)\cdot\\ \qquad\xrightarrow[\phi=\pi/2]{\Omega t=\pi}\frac{1}{\sqrt{2}}|g\rangle_3\left(|g\rangle_1-|i\rangle_1\right),\\ |g\rangle_3|e\rangle_1\xrightarrow[\phi=-\pi/2]{\Omega t=\pi/2}\frac{1}{\sqrt{2}}|g\rangle_3\left(|e\rangle_1+|g\rangle_1\right)\cdot\\ \qquad\xrightarrow[\phi=\pi/2]{\Omega t=\pi}\frac{1}{\sqrt{2}}|g\rangle_3\left(|i\rangle_1+|g\rangle_1\right),\\ |e\rangle_3|g\rangle_1\xrightarrow[\phi=-\pi/2]{\Omega t=\pi/2}\frac{1}{\sqrt{2}}|e\rangle_3\left(|g\rangle_1-|e\rangle_1\right)\cdot\\ \qquad\xrightarrow[\phi=\pi/2]{\Omega t=\pi}\frac{1}{\sqrt{2}}|e\rangle_3\left(|g\rangle_1-|i\rangle_1\right),\\ |e\rangle_3|e\rangle_1\xrightarrow[\phi=-\pi/2]{\Omega t=\pi/2}\frac{1}{\sqrt{2}}|e\rangle_3\left(|e\rangle_1+|g\rangle_1\right)\cdot\\ \qquad\xrightarrow[\phi=\pi/2]{\Omega t=\pi}\frac{1}{\sqrt{2}}|e\rangle_3\left(|i\rangle_1+|g\rangle_1\right)。\end{cases}\qquad(2)$$

第2步：让原子1和3同时进入单模量子化腔场。原子$|e\rangle\leftrightarrow|i\rangle$的转换频率与腔场频率大失谐，因此原子能级$|i\rangle$在原子–腔场相互作用过程中不受影响。原子1和3同时与腔场相互作用，相互作用表象中的哈密顿量为

$$\boldsymbol{H}_1=g\sum_{j=1,3}\left(\mathrm{e}^{-\mathrm{i}\delta t}\boldsymbol{a}^{\dagger}\boldsymbol{S}_j+\mathrm{e}^{\mathrm{i}\delta t}\boldsymbol{S}_j^{\dagger}\boldsymbol{a}\right),$$

式中：$\boldsymbol{a}^{\dagger}$和$\boldsymbol{a}$分别为腔场的产生和湮灭算符；

$\boldsymbol{S}_j^{\dagger}=|e\rangle_{jj}\langle g|$，$\boldsymbol{S}_j=|g\rangle_{jj}\langle e|$；

g为原子和腔场的耦合系数；

δ为原子转换频率ω_0和腔场频率ω之间的失谐量。

在$\delta\gg g$的情况下，原子和腔场之间没有能量交换。如果腔场初始处于真空态，有效哈密顿量可写为

$$\boldsymbol{H}=\lambda\left[\sum_{j=1,3}|e\rangle_{jj}\langle e|+\left(\boldsymbol{S}_1^{\dagger}\boldsymbol{S}_3+\boldsymbol{S}_3^{\dagger}\boldsymbol{S}_1\right)\right],$$

式中：$\lambda=g^2/\delta$。

这样态$|g\rangle_1|g\rangle_3$和$|i\rangle_1|g\rangle_3$不会随着时间演化。系统经过一段时间$\lambda t=\pi$的演化，可得到

$$\begin{cases}|g\rangle_3|g\rangle_1\to|g\rangle_3|g\rangle_1,|g\rangle_3|i\rangle_1\to|g\rangle_3|i\rangle_1,\\ |e\rangle_3|g\rangle_1\to|e\rangle_3|g\rangle_1,|e\rangle_3|i\rangle_1\to-|e\rangle_3|i\rangle_1。\end{cases}\qquad(3)$$

若将第1步的输出态作为第2步的输入态，即将式（2）和式（3）中的原子态矢转化相结合，可得如下转化

$$\begin{cases}|g\rangle_3|g\rangle_1\to\frac{1}{\sqrt{2}}|g\rangle_3\left(|g\rangle_1-|i\rangle_1\right),\\ |g\rangle_3|e\rangle_1\to\frac{1}{\sqrt{2}}|g\rangle_3\left(|i\rangle_1+|g\rangle_1\right),\\ |e\rangle_3|g\rangle_1\to\frac{1}{\sqrt{2}}|e\rangle_3\left(|g\rangle_1+|i\rangle_1\right),\\ |e\rangle_3|e\rangle_1\to\frac{1}{\sqrt{2}}|e\rangle_3\left(-|i\rangle_1+|g\rangle_1\right)。\end{cases}\qquad(4)$$

第3步：将第2步的输出态作为输入，让原子1经过2个经典场，其频率分别与原子$|e\rangle \leftrightarrow |i\rangle$和$|g\rangle \leftrightarrow |e\rangle$的转换频率相同。通过适当调节经典场的振幅和相位使得原子1在场中经历如下转换

$$\begin{cases} |i\rangle_1 \xrightarrow[\phi=-\pi/2]{\Omega t=\pi} |e\rangle_1 \xrightarrow[\phi=\pi/2]{\Omega t=\pi/2} \frac{1}{\sqrt{2}}\left(|e\rangle_1 - |g\rangle_1\right), \\ |g\rangle_1 \xrightarrow[\phi=\pi/2]{\Omega t=\pi/2} \frac{1}{\sqrt{2}}\left(|e\rangle_1 + |g\rangle_1\right)。 \end{cases} \quad (5)$$

由方程（4）和（5），就能实现2个原子比特之间的CNOT门操作

$$|g\rangle_3|g\rangle_1 \rightarrow |g\rangle_3|g\rangle_1, |g\rangle_3|e\rangle_1 \rightarrow |g\rangle_3|e\rangle_1,$$
$$|e\rangle_3|g\rangle_1 \rightarrow |e\rangle_3|g\rangle_3, |e\rangle_3|e\rangle_1 \rightarrow |e\rangle_3|g\rangle_1。$$

这样就已经在腔QED系统中实现了图1中Shor算法的所有逻辑门操作。当完成整个线路操作之后，工作处理器的输出态为

$$|x\rangle \rightarrow |x_0x_1x_2\rangle_W = |k2^n/r\rangle_W,$$

因此，通过测量原子j(j=1, 2, 3)的量子态，就能够确定x_0, x_1和x_2的值，从而可确定r的值。也就是说，若测量第j个原子的态为基态，则对应x_j的输出为0；若测量第j个原子的态为激发态，则对应x_j的输出为1。

3 结语

本文给出了Shor算法在腔QED系统中的实现方案，讨论了当N=15，a=7时算法的具体操作实现。在本文的方案中，量子比特被编码在阶梯形三能级原子的能级中，对原子比特的操作是通过原子和经典（量子）场之间的控制相互作用实现的。随着腔场QED技术的发展，本文方案在实验上将是可行的，该方案的提出也为研究少数量子比特的量子信息处理提供了一种实际的方法。我们可期待利用该方法来实现Shor算法的更为普遍的情形。

参考文献：

[1] Shor P W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer[J]. SIAM J. Sci. Statist. Comput.，1997，26：1484-1509.

[2] Nielsen M A，Chuang I L. Quantum Computation and Quantum Information[M]. Cambridge：Cambridge University Press，2000：28-42.

[3] 李承祖，黄明球，陈平形，等. 量子通信和量子计算[M]. 长沙：国防科技大学出版社，2000：171-184.
Li Chengzu，Huang Mingqiu，Chen Pingxing，et al. Quantum Computation and Quantum Information[M]. Changsha: National University of Defense Technology Press，2000：171-184.

[4] Vandersypen L M K，Steffen M，Breyta G，et al. Experimental Realization of Shor′s Quantum Factoring Algorithm Using Nuclear Magnetic Resonance[J]. Nature，2001，414：883-887.

[5] Zheng S B，Guo G C. Efficient Scheme for Two-Atom Entanglement and Quantum Information Processing in Cavity QED[J]. Phys. Rev. Lett.，2000，85：2392-2395.

[6] 刘　丽. 用分组法改进Shor算法的可能性[J]. 清华大学学报：自然科学版，2008，48(8)：1233-1235.
Liu Li. Possibility to Improve Shor Algorithm with Grouping Algorithm[J]. Journal of Tsinghua University：Science and Technology，2008，48(8)：1233-1235.

[7] 付向群，鲍皖苏，周　淳. Shor整数分解量子算法的加速实现[J]. 科学通报，2010，55(4/5)：322-327.
Fu Xiangqun，Bao Wansu，Zhou Chun. Speeding up Implementation for Shor's Factorization Quantum[J]. Chinese Science Bulletin，2010，55(4/5)：322-327.

[8] 张永德. 量子信息物理原理[M]. 北京：科学出版社，2005.
Zhang Yongde. The Physics Principle of Quantum Information[M]. Beijing：Science Press，2005.

（责任编辑：李玉珍）