科学通报 2011 年 第 56 卷 第 26 期: 2250 ~ 2255
论 文 www.scichina.com csb.scichina.com
《中国科学》杂志社 SCIENCE CHINA PRESS

t 比特半经典量子 Fourier 变换

付向群, 鲍皖苏*, 周淳, 宋震

解放军信息工程大学电子技术学院, 郑州 450004
* 联系人, E-mail: 2010thzz@sina.com

2011-06-13 收稿, 2011-07-21 接受

摘要 针对目前大维数量子寄存器生成的困难性, 研究了基于小维数量子寄存器实现大维数量子 Fourier 变换的方法. 首先, 定义了 t 比特半经典量子 Fourier 变换, 从几率幅的角度证明该变换可以实现量子 Fourier 变换, 且所需 2 位量子门的规模显著降低, 并设计了该变换的量子实现线路. 然后基于 t 比特半经典量子 Fourier 变换, 将经典固定窗口法与 Shor 算法实现方法相融合, 重新设计了 Shor 整数分解量子算法的实现线路, 与 Parker 等人的实现线路相比, 计算资源大体相同(所需的基本量子门均为 $O\left(\lceil \log N \rceil^3\right)$, 所需量子寄存器的维数前者较后者多 $t-1$ 维), 而实现速度提高了 t^2 倍, t 是窗口宽度.

关键词
量子 Fourier 变换
Shor 量子算法
窗口法

量子计算机具有强大的并行计算能力, 对现代密码的安全性带来了严峻的挑战. 1994 年, Shor[1]提出了量子计算机上多项式时间的大数质因子分解算法, 该算法对基于大数质因子分解、离散对数问题的公钥密码如 RSA 等公钥密码体制产生了巨大威胁. 1996 年, Grover[2]提出了未加整理数据库的量子搜索算法, 该算法用于对称密码的密钥穷尽攻击时, 计算复杂度可以得到开平方根级的降低. 自此之后, 量子计算和量子密码的研究引起了国内外学者的广泛关注[3~11].

尽管量子计算和 Shor 量子算法的原理的正确性已得到验证[12], 但将量子计算机真正应用于实际, 破译目前实用的 2048 比特的 RSA 或 191 比特的 ECC 还很困难, 主要的原因在于目前人们还无法研制千比特级的量子计算机. 因此, 长期以来如何减少 Shor 量子算法实现时所需的计算资源一直是人们关注的难点和热点.

1996 年, Vedral 等人[13]首次设计了一个 Shor 算法实现的量子线路, 该线路需要规模为 $7n+1$ 维量子寄存器和 $O\left(n^3\right)$ 基本量子门就可以实现模幂运算(n 是所分解整数的比特长), 如果利用 Toffoli 门代替用于存储运算过程中产生的中间态的 n 维量子寄存器, 可将所需量子寄存器的维数降为 $4n+3$, 同年, Beckman 等人[14]对此作了进一步分析, 如果所需的 Toffoli 门数量不受限制, 那么实现模幂运算需要 $4n+1$ 维量子寄存器. 1998 年, Zalka[15]给出一个需要 $3n+O(\log n)$ 维量子寄存器实现 Shor 算法的量子线路. 这些研究结果都是从减少模幂运算所需量子寄存器维数方面优化 Shor 算法的实现线路.

一般情况下, 在原始的量子 Fourier 变换实现中, 需要 n 维量子寄存器, 且 n 位量子态是一次输入, 在实现线路中共需要 $n^2/2$ 个 2 位量子门、n 个 1 位量子门[16]. 对于较大的 n, 在现有技术条件下还无法实现 n 维量子 Fourier 变换. 1996 年, Griffiths 等人[17]提出了单比特半经典量子 Fourier 变换, 由于该变换的 n 比特信息是按逐比特方式输入的, 其实现量子 Fourier 变换所需量子寄存器维数仅为 1 且只需要 1 个 1 位量子门, 不再需要 2 位量子门. 也正是有了 Griffiths 等人的工作, 2000 年, Parker 等人[18]基于单比特半经典量子 Fourier 变换设计了 Shor 算法的新的

英文版见: Fu X Q, Bao W S, Zhou C, et al. *t*-bit semiclassical quantum Fourier transform. Chinese Sci Bull, 2011, 56, doi: 10.1007/s11434-011-4692-8

实现线路，所需的量子寄存器为$n+1$维．因此，单比特半经典量子Fourier变换为大维数量子Fourier变换的实现提供了一种解决方案，对在量子计算资源有限的条件下将Shor算法应用于破译RSA，ECC等实用的公钥密码具有重要的现实意义和实用价值．

量子 Fourier 变换与单比特半经典量子 Fourier 变换相比，前者实现速度快但所需量子资源多，后者实现速度相对较慢但所需量子资源少．考虑到目前实际实现时 2 位量子门较 1 位量子门操控的困难性，因此，在量子计算的实现线路中应尽量减少2位量子门的使用．用单比特半经典量子 Fourier 变换代替量子 Fourier 变换虽是一个非常好的选择，但毕竟是以牺牲速度为代价的．针对量子 Fourier 变换的实现，基于目前大维数量子寄存器生成的困难性，如何既兼顾到实现所需的量子资源又兼顾到实现的速度，即基于小维数量子寄存器如何实现大维数量子Fourier变换的方法，还需进一步研究．

本文给出了t比特半经典量子 Fourier 变换的定义，基于几率幅证明了该变换也可以实现量子Fourier 变换，并设计了该变换的量子实现线路，与量子Fourier变换相比，所需2位量子门和1位量子门的规模分别降为原来的$1/l^2$, $2/l$ (n是量子 Fourier 变换的维数，如果t整除n，$l=[n/t]-1$，否则$l=[n/t]$)；与单比特半经典量子Fourier变换相比，实现速度提高了大约t倍．基于t比特半经典量子Fourier 变换，给出了经典的固定窗口法与 Shor 整数分解量子计算算法的融合方法，设计了基于该方法的 Shor 整数分解量子计算算法实现线路，与 Parker 等人的实现线路[18]相比，在计算资源大体相同的条件下实现速度提高了t^2倍，t是窗口宽度．

1 量子 Fourier 变换与单比特半经典量子 Fourier 变换

定义 1 (量子Fourier变换)[16] 如果在一组标准正交基$|0\rangle,|1\rangle,\cdots,|N-1\rangle$上的一个线性算子在基态上的作用$U_F$为

$$U_F:|j\rangle\mapsto\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\omega_N^{jk}|k\rangle,$$

那么对任意的状态的作用可以表示为

$$U_F:\sum_{j=0}^{N-1}x_j|j\rangle\mapsto\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}x_j\omega_N^{jk}|k\rangle,$$

称U_F为量子 Fourier 变换．其中，“$\mapsto$”表示该变换是可逆变换，$\omega_N=\mathrm{e}^{2\pi i/N}$．

如果$N=2^n$，那么对一个量子态$|a\rangle$作用量子Fourier 变换后有

$$U_F|a\rangle=\prod_{j=0}^{n-1}\otimes\left|p\left(\phi_j\right)\right\rangle_j,\qquad(1)$$

此时称量子 Fourier 变换为n维量子 Fourier 变换．其中，$a=\sum_{j=0}^{n-1}a_j2^j$是a的二进制表示，a_j为 0 或者 1，$\phi_j=\sum_{k=0}^{n-j}a_k2^{j+k-n-1}$，$j=0,1,\cdots,n-1$，$|p(\phi)\rangle=(|0\rangle+\mathrm{e}^{2\pi i\phi}|1\rangle)/\sqrt{2}$．

文献[16]指出实现一个量子 Fourier 变换需要$\lceil\log N\rceil$维量子寄存器. 1996 年, Griffiths 和 Niu 提出了只需1维量子寄存器且实现线路只需要1位门就可实现量子 Fourier 变换的方法，称为单比特半经典量子 Fourier 变换[17]，其量子实现线路如图 1 所示．

图 1 的相关说明:

(1) 方框代表一个黑盒，其变换可描述为

$$\begin{cases}|0\rangle\mapsto(|0\rangle+|1\rangle)/\sqrt{2}\\|1\rangle\mapsto\mathrm{e}^{2\pi i\phi}(|0\rangle-|1\rangle)/\sqrt{2}\end{cases}.\qquad(2)$$

(2) 单线表示量子态，双线表示经典值;

(3) 每个黑盒输出两个经典值：一个是测量的结果，另一个是相位$\phi'=\phi/2+c/4$，并做为下一个黑盒的输入，其中ϕ的初始值为 0;

(4) 最终的观测结果为$c=\sum_{k=0}^{n-1}2^kc_k$．

文献[16]指出，对量子态$|a\rangle$做完单比特半经典量子 Fourier 变换所得的某个量子态$|c\rangle$的几率幅与做完量子 Fourier 变换一样，因此利用单比特半经典量子 Fourier 变换可以实现量子 Fourier 变换，且$|a\rangle$是从高位至低位逐比特输入的，亦即单比特半经

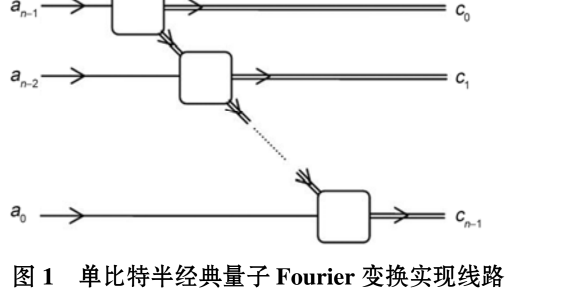

图 1 单比特半经典量子 Fourier 变换实现线路

典量子 Fourier 通过 n 步同样可以完成 2^n 个输入的并行计算. 两者的不同点在于单比特半经典量子 Fourier 变换的每个比特信息处理完都进行观测, 以此来减少所需量子资源.

2 t 比特半经典量子 Fourier 变换

在量子实现线路中, 利用单比特半经典量子 Fourier变换实现量子Fourier变换可以降低所需资源, 但速度慢, 而量子 Fourier 变换的原始实现方法速度快, 但所需资源多. 针对这两种实现方法各自存在的缺点, 本文设计了一个既兼顾到量子资源又兼顾到实现速度的量子 Fourier 变换的实现方法.

定义 2 设 t 是正整数, $l=\begin{cases}[n/t]\ ,\ t\nmid n\\ l=[n/t]-1\ ,\ t\mid n\end{cases}$, $|a\rangle=|a_{n-1},a_{n-2},\cdots,a_0\rangle$ 是标准正交基 $|0\rangle,|1\rangle,\cdots,|2^n-1\rangle$ 中的任意一个基态, 如果变换 U_{F_t} 对 $|a\rangle$ 的作用为

$$|a_{n-1},a_{n-2},\cdots,a_{lt}\rangle\mapsto$$

$$\frac{1}{2^{(n-lt)/2}}\sum_{c_0'=0}^{2^{n-lt}-1}\omega_{2^{n-lt}}^{a_0'c_0'}|c_{n-lt-1},c_{n-lt-2},\cdots,c_0\rangle,$$

$$|a_{lt-1},a_{lt-2},\cdots,a_{(l-1)t}\rangle\mapsto$$

$$\frac{1}{2^{t/2}}\sum_{c_1'=0}^{2^t-1}\omega_{2^t}^{a_1'c_1'}\mathrm{e}^{2\pi i(a_{lt-1}+\frac{a_{lt-2}}{2}+\cdots+\frac{a_{(l-1)t}}{2^{t-1}})\varphi_1}|c_{n-(l-1)t-1},c_{n-(l-1)t-2},\cdots,c_{n-lt}\rangle,$$

$$\vdots$$

$$|a_{t-1},a_{t-2},\cdots,a_0\rangle\mapsto$$

$$\frac{1}{2^{t/2}}\sum_{c_l'=0}^{2^t-1}\omega_{2^t}^{a_l'c_l'}\mathrm{e}^{2\pi i(a_{t-1}+\frac{a_{t-2}}{2}+\cdots+\frac{a_0}{2^{t-1}})\varphi_l}|c_{n-1},c_{n-2},\cdots,c_{n-t}\rangle,$$

其中, $a_0'=\sum_{r=lt}^{n-1}2^{r-lt}a_r$, $a_j'=\sum_{r=(l-j)t}^{(l-j+1)t-1}2^{r-(l-j)t}a_r$, $c_0'=\sum_{r=0}^{n-lt-1}2^rc_r$, $c_j'=\sum_{r=n-(l-j+1)t}^{n-(l-j)t-1}2^{r-n+(l-j+1)t}c_r$, $\varphi_1=\frac{c_0}{2^{n-lt+1}}+\cdots+\frac{c_{n-lt-1}}{2^2}$, $\varphi_k=\frac{\varphi_{k-1}}{2^t}+\frac{c_{n-(l-k+2)t}}{2^{t+1}}+\cdots+\frac{c_{n-(l-k+1)t-1}}{2^2}$ $(j=1,\cdots,l,\ k=2,\cdots,l)$, 则称变换 U_{F_t} 为量子态 $|a\rangle$ 的 t 比特半经典量子 Fourier 变换.

U_{F_t} 实际上是从高位至低位按块进行变换的, 其中第一块是 $n-lt$ 位的, 其余均为 t 位.

定理 1 设 $|0\rangle,|1\rangle,\cdots,|N-1\rangle$ 是一组标准正交基, U_F 是量子 Fourier 变换, U_{F_t} 是 t 比特半经典量子 Fourier 变换, 则对基态中的任意一个量子态 $|a\rangle=|a_{n-1},a_{n-2},\cdots,a_0\rangle$ 做 U_F 和 U_{F_t} 变换之后, 得到结果 $|c\rangle=|c_{n-1},c_{n-2},\cdots,c_0\rangle$ 的概率相等.

证明 要证明定理成立, 只需证明对 $|a\rangle$ 分别做 U_F 和 U_{F_t} 变换之后, 得到结果 $|c\rangle$ 的几率幅一样.

根据定义 2 和 $\mathrm{e}^{2\pi i}=1$ 可得

$$\omega_{2^{n-lt}}^{a_0'c_0'}=\omega_{2^{n-lt}}^{a_0'c}=\mathrm{e}^{\pi i\left(\frac{ca_{n-1}}{2^0}+\frac{ca_{n-2}}{2^1}+\cdots+\frac{ca_{lt}}{2^{n-lt-1}}\right)},$$

故 $|c_{n-lt-1},c_{n-lt-2},\cdots,c_0\rangle$ 的几率幅为

$$\frac{1}{2^{(n-lt)/2}}\mathrm{e}^{\pi i\left(\frac{ca_{n-1}}{2^0}+\frac{ca_{n-2}}{2^1}+\cdots+\frac{ca_{lt}}{2^{n-lt-1}}\right)}.$$

又由于

$$\omega_{2^t}^{a_1'c_1'}\mathrm{e}^{2\pi i\left(a_{lt-1}+\frac{a_{lt-2}}{2}+\cdots+\frac{a_{(l-1)t}}{2^{t-1}}\right)\varphi_1}$$

$$=\mathrm{e}^{\frac{2\pi i a_1'c_1'}{2^t}}\mathrm{e}^{2\pi i\left(a_{lt-1}+\frac{a_{lt-2}}{2}+\cdots+\frac{a_{(l-1)t}}{2^{t-1}}\right)\left(\frac{c_0}{2^{n-lt+1}}+\cdots+\frac{c_{n-lt-1}}{2^2}\right)}$$

$$=\mathrm{e}^{\frac{\pi i a_{lt-1}}{2^{n-lt}}\left(c_0+2c_1+\cdots+2^{n-(l-1)t-1}c_{n-(l-1)t-1}\right)}$$

$$\bullet\cdots\bullet\mathrm{e}^{\frac{\pi i a_{(l-1)t}}{2^{n-(l-1)t-1}}\left(c_0+2c_1+\cdots+2^{n-(l-1)t-1}c_{n-(l-1)t-1}\right)}$$

$$=\mathrm{e}^{\pi i\left(\frac{ca_{lt-1}}{2^{n-lt}}+\frac{ca_{lt-2}}{2^{n-lt+1}}+\cdots+\frac{ca_{(l-1)t}}{2^{n-(l-1)t-1}}\right)},$$

即

$$|c_{n-(l-1)t-1},c_{n-(l-1)t-2},\cdots,c_{n-lt}\rangle \text{ 的几率幅为 } \frac{1}{2^{t/2}}\mathrm{e}^{\pi i\left(\frac{ca_{lt-1}}{2^{n-lt}}+\frac{ca_{lt-2}}{2^{n-lt+1}}+\cdots+\frac{ca_{(l-1)t}}{2^{n-(l-1)t-1}}\right)}.$$

同理可得

$$|c_{n-(l-2)t-1},c_{n-(l-2)t-2},\cdots,c_{n-(l-1)t}\rangle \text{ 的几率幅为 } \frac{1}{2^{t/2}}\mathrm{e}^{\pi i\left(\frac{ca_{(l-1)t-1}}{2^{n-(l-1)t}}+\frac{ca_{(l-1)t-2}}{2^{n-(l-1)t+1}}+\cdots+\frac{ca_{(l-2)t}}{2^{n-(l-2)t-1}}\right)},$$

$$\vdots$$

$|c_{n-1},c_{n-2},\cdots,c_{n-t}\rangle$ 的几率幅为 $\frac{1}{2^{t/2}}\mathrm{e}^{\pi i\left(\frac{ca_{t-1}}{2^{n-t}}+\frac{ca_{t-2}}{2^{n-t+1}}+\cdots+\frac{ca_0}{2^{n-1}}\right)}$.

因此, 对 $|a\rangle$ 做 U_{F_t} 变换之后, 任意基态 $|c\rangle=|c_{n-1},c_{n-2},\cdots,c_0\rangle$ 的几率幅为

$$A=\frac{1}{2^{n/2}}\mathrm{e}^{\pi i\left(\frac{ca_{n-1}}{2^0}+\frac{ca_{n-2}}{2^1}+\cdots+\frac{ca_{lt}}{2^{n-lt-1}}\right)}\bullet\mathrm{e}^{\pi i\left(\frac{ca_{lt-1}}{2^{n-lt}}+\frac{ca_{lt-2}}{2^{n-lt+1}}+\cdots+\frac{ca_{(l-1)t}}{2^{n-(l-1)t-1}}\right)}\bullet\cdots\bullet\mathrm{e}^{\pi i\left(\frac{ca_{t-1}}{2^{n-t}}+\frac{ca_{t-2}}{2^{n-t+1}}+\cdots+\frac{ca_0}{2^{n-1}}\right)},$$

经过化简可得, $A=\frac{1}{2^{n/2}}\omega_{2^n}^{ac}$.

由定义 1 可知, 对量子态 $|a\rangle$ 做量子 Fourier 变换 U_F, 可得

$$U_F|a\rangle = \frac{1}{2^{n/2}}\sum_{c=0}^{2^n-1}\omega_{2^n}^{ac}|c\rangle.$$

因此，对量子态$|a\rangle$做变换U_F变换之后，任意基态$|c\rangle = |c_{n-1}, c_{n-2}, \cdots, c_0\rangle$的几率幅为

$$\frac{1}{2^{n/2}}\omega_{2^n}^{ac}.$$

故结论成立.

证毕.

由定理1可知，t比特半经典量子Fourier变换可以实现量子Fourier变换，其实现线路可以按图2方式设计.

图2的相关说明.

(1) 图中每个粗线虚框记为虚框1、含E_1的细线虚框记为虚框2、含E_2的每个细线虚框记为虚框3，其中E_1是$n-lt$维量子Fourier变换，E_2是t维量子Fourier变换，E_1、E_2的具体实现线路可参见文献[16]；

(2) 虚框2的输出值为$n-lt+1$个，分别为$c_{n-lt-1}, c_{n-lt-2}, \cdots, c_0$和$\varphi' = \frac{c_0}{2^{n-lt+1}} + \cdots + \frac{c_{n-lt-1}}{2^2}$，如果虚框3输入为$a'_{t-1}, a'_{t-2}, \cdots, a'_0$，则其输出$t+1$个经典值$c'_{t-1}, c'_{t-2}, \cdots, c'_0$和$\varphi' = \frac{\varphi}{2^t} + \frac{c'_0}{2^{t+1}} + \cdots + \frac{c'_{t-1}}{2^2}$，且$R_j = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i\varphi/2^{j-1}} \end{bmatrix}$，其中$\varphi'$是下一个虚框1的输入值，$j = 1, 2, \cdots, t$，$\varphi$是虚框1输入的经典值且$\varphi$的初始值为0；

(3) 最终观测结果$c = \sum_{j=0}^{n-1} 2^j c_j$.

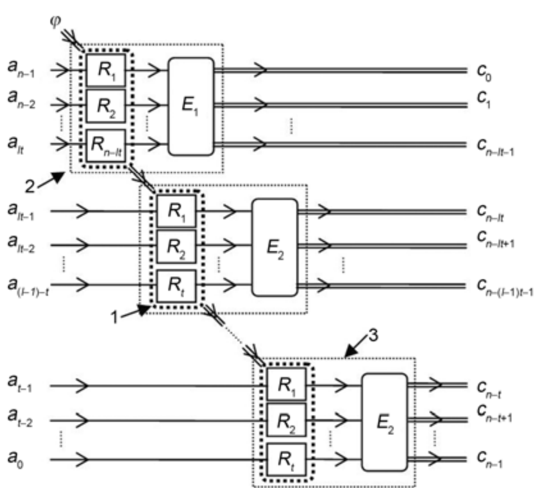

图2 t比特半经典量子Fourier变换的实现线路图

下面对t比特半经典量子Fourier变换的实现线路所需资源进行分析.

从图2可以看出，t比特半经典量子Fourier变换只需要t维量子寄存器. 由于实现n维量子Fourier变换需要$n^2/2$个2位量子门、n个1位量子门[16]，因此，在图2中需要$t^2/2$个2位量子门、t个1位量子门用于实现t维量子Fourier变换且需t个1位量子门用于实现R_j ($j = 1, 2, \cdots, t$)，亦即t比特半经典量子Fourier变换所需2位量子门和1位量子门的规模是量子Fourier变换的$1/l^2$，$2/l$；与单比特半经典量子Fourier变换相比，由于t比特半经典量子Fourier变换需要进行1次$\frac{1}{2^{(n-l't)/2}}\sum_{c=0}^{2^{n-l't}-1}|c\rangle$叠加态和$l'$次$\frac{1}{2^{t/2}}\sum_{c=0}^{2^t-1}|c\rangle$叠加态的制备，单比特半经典量子Fourier变换需要进行L次$(|0\rangle+|1\rangle)/\sqrt{2}$叠加态的制备，因此，实现速度提高了大约$t$倍.

3 Parker的Shor整数分解量子算法的实现线路

2000年，Parker等人提出了一个Shor整数分解量子算法的实现线路，其具体实现线路如图3所示[18]. 其中，H为Hadamard门[16]，$R'_j = \begin{pmatrix} 1 & 0 \\ 0 & \phi_j \end{pmatrix}$，$\phi_j = e^{-2\pi i\sum_{k=2}^{j} m_{j-k}/2^k}$，$U_a$由一个控制比特控制，其变换为$cU_a|r\rangle|x\rangle = |r\rangle|a^r x \bmod N\rangle$，最终观测到的结果$c = \sum_{i=0}^{L} 2^{L-i} m_i$，$L = 2\lceil \log N \rceil + 1$，$\lceil \log N \rceil$是比$\log N$大的最小整数，图3中的量子态$|0\rangle+|1\rangle$实际上是量子态$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$，是$|0\rangle$态通过Hadamard变换得到的，此处简写为$|0\rangle+|1\rangle$.

Parker的Shor整数分解量子算法的实现线路需要$\lceil \log N \rceil+1$维量子寄存器，并且需要$O(\lceil \log N \rceil^3)$基

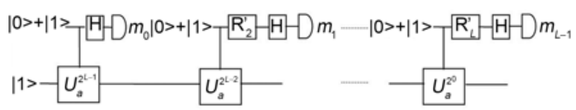

图3 Parker等人的Shor整数分解量子算法实现线路

本量子门[18]. 文献[19]中进一步指出该线路需要 nL 次加法运算(加法运算是两个 n 比特的数相加, $n=\lceil \log N \rceil$), 其预计算为 $\alpha \bmod N, \alpha^2 \bmod N, \cdots, \alpha^{2^{L-1}} \bmod N$.

4 基于窗口法的 Shor 整数分解量子算法实现方案及分析

文献[16]中指出模幂运算 $\alpha^k \bmod N$ 是 Shor 算法实现中最耗时的. 在经典计算机上, 提高模幂运算的实现速度通常有两种方法: 一种是研究整数整数 k 的表示法; 另外一种是通过增加预计算量来提高模幂运算的实现速度, 比如窗口法[20]. 窗口法是以空间换时间来提高模幂运算的实现速度, 其大体思想是: 对 k 的二进制表示式, 用固定长度 t , 按一定的规则进行划分, 即将 k 表示为如下形式

$$k=\sum_{i=0}^{v-1} 2^{ti} u_i \,, \quad 0 \leqslant k_i \leqslant 2^t-1, \quad 0 \leqslant i \leqslant v-1 .$$

这样, 如果计算模幂运算之前先将 $\alpha, \alpha^{2^t}, \alpha^{2^{2t}} \cdots$, $\alpha^{2^{(v-1)t}}$ 求解并存储起来, 则在计算模幂运算时就可以减少加法运算的次数, 而且每次进行运算时 u_i 的所有比特信息均已输入. 如果要将窗口法与量子实现线路相融合, 那么每个 u_i 的所有比特信息需同时输入.

以下基于窗口法和 t 比特半经典量子 Fourier 变换重新设计 Shor 整数分解量子算法实现线路, 其具体量子实现线路如图 4 所示.

图 4 的相关说明:

(1) 最终观测结果为 $c=\sum_{i=0}^{L-1} 2^i m_i$, 如果 t 不能整除 L , 那么 $l'=[L/t]$, 否则 $l'=[L/t]-1$;

(2) 虚框 2 和虚框 3 的结构、上方的输出值均与图 2 一样, 虚框 2 的输入比特是 $L-l't$ 比特, 虚框 3 的输入是 t 比特, φ 的初始值为 0;

(3) 假设 $U_\alpha^{u_i 2^{it}}$ 黑盒的左端输入是 A , 那么输出的结果是 $A \cdot \alpha^{u_i 2^{it}} \bmod N$, 其中 $\alpha^{u_i 2^{it}} \bmod N$ 是在经典算机上预计算, $u_i=\sum_j 2^j u_j'$ ($u_0', u_1', \cdots$ 分别为 $U_\alpha^{u_i 2^{it}}$ 黑盒从右至左的上端输入值);

(4) 图中的量子态 $|0\rangle+|1\rangle$ 实际上是量子态 $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, 是 $|0\rangle$ 态通过 Hadamard 变换得到的, 此处简写为 $|0\rangle+|1\rangle$;

(5) 图中的 $|1\rangle$ 是 $\lceil \log N \rceil$ 比特, $|0\rangle+|1\rangle$ 是 1 比特.

由图 4 易知, $\alpha^k \bmod N$ 是通过 $U_\alpha^{u_{l'} 2^{l't}}$, $U_\alpha^{u_{l'-1} 2^{(l'-1)t}}$, $\cdots$, $U_\alpha^{u_0 2^0}$ 黑盒计算出来的, 其输出的结果为 $\alpha^{\sum_{i=0}^{l'} u_i 2^{it}} \bmod N$ (u_i 为 $U_\alpha^{u_i 2^{it}}$ 黑盒的上端输入值), 即 $\sum_{i=0}^{l'} u_i 2^{it}$ 正好是整数 k 的窗口宽度为 t 的窗口表示. 也就是说, 窗口宽度与 t 比特半经典量子 Fourier 变换的输入维数相等.

该实现线路需要 $\lceil \log N \rceil + t$ 维量子寄存器. 因为运行 1 次 R_i 门需要 $O(1)$ 基本量子门, 而运行一次量子 Fourier 变换需要 $O(t^2)$ 基本量子门, 所以运行 1 次虚框 2, 1 次虚框 3 均需要 $O(t^2)$ 基本量子门, 又由于实现 1 次模幂运算需要 $O(\lceil \log N \rceil^3)$ 基本量子门, 因此, 新的量子线路整体需要 $O(\lceil \log N \rceil^3)$ 基本量子门. 与文献[18]相比, 所需的基本量子门均为 $O(\lceil \log N \rceil^3)$, 但所需量子寄存器的维数前者较后者多 $t-1$ 维.

Shor 整数分解量子算法实现线路的运行时间是通过模幂运算和量子 Fourier 变换运算运行时间刻画的[15]. 文献[19]中指出实现一次模幂运算需要 n 次加

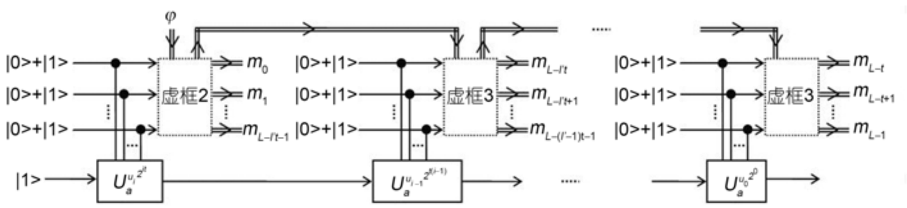

图 4 基于窗口法和 t 比特半经典量子 Fourier 变换的 Shor 整数分解量子算法实现线路

法运算，而新的量子线路需要进行 $l'+1$ 次模幂运算，因此，新量子线路的模幂运算需要 $(l'+1)n$ 次加法运算，且需要预计算 $\alpha^{1+2^{jt}} \bmod N$，$\alpha^{2+2^{jt}} \bmod N$，$\cdots$，$\alpha^{2^t-1+2^{jt}} \bmod N$ $(j=0,1,\cdots,l')$．文献[18]的 Shor 整数分解量子算法实现线路的模幂运算需要 nL 次加法运算，因此，新的量子线路的模幂运算实现速度比文献[18]提高了约 t 倍．又由第 2 节分析可知，t 比特半经典量子 Fourier 变换实现速度比单比特半经典量子 Fourier 变换大约快 t 倍，因此，总体而言，新的量子线路的实现速度比文献[18]提高约 t^2 倍，但预计算增加约 $2^t/t$ 倍．

5 结束语

本文针对目前大维数量子寄存器生成的困难性，深入研究了基于小维数量子寄存器实现大维数量子 Fourier 变换的方法．提出了 t 比特半经典量子 Fourier 变换，既兼顾了量子资源又兼顾了实现速度，设计了该变换的实现线路．给出了经典的固定窗口法与 Shor 整数分解量子计算算法的融合方法，设计了基于该方法的 Shor 整数分解量子计算算法实现线路，与 Parker 等人的实现线路相比，在计算资源大体相同的条件下实现速度提高了 t^2 倍，t 是窗口宽度．

参考文献

1 Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput, 1997, 26: 1484–1509

2 Grover L K. A fast quantum mechanics algorithm for database search. In: Proceeding of the 28th ACM Symposium on Theory of Computation. New York: ACM Press, 1996. 212–219

3 Long G L, Xiao L. Parallel quantum computing in a single ensemble quantum computer. Phys Rev A, 2004, 69: 052303

4 Zhong P C, Bao W S. Quantum mechanical meet-in-the-middle search algorithm for triple-DES. Chinese Sci Bull, 2010, 55: 321–325

5 Gao F, Guo F Z, Wen Q Y, et al. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. Sci China Ser G-Phys Mech Astron, 2008, 51: 559–566

6 Chen W, Han Z F, Mo X F, et al. Active phase compensation of quantum key distribution system. Chinese Sci Bull, 2008, 53: 1310–1314

7 Fang X M, Zhu X W, Hong M, et al. Realization of quantum discrete Fourier transform with NMR. Chinese Sci Bull, 2000, 45: 1071–1075

8 He Y G, Sun J G. Complete quantum circuit of HAAR wavelet based MRA. Chinese Sci Bull, 2005, 50: 1796–1798

9 Cao Y, Peng S G, Zgeng C, et al. Quantum Fourier transform and phase estimation in qudit system. Commun Theor Phys, 2011, 55: 790–794

10 Wang X, Bao W S, Fu X Q. A quantum algorithm for searching a target solution of fixed weight. Chinese Sci Bull, 2011, 56: 484–488

11 Zhou C, Bao W S, Fu X Q. Decoy-state quantum key distribution for the heralded pair coherent state photon source with intensity fluctuations. Sci China Infor Sci, 2010, 53: 2485–2494

12 Lieven M K V, Matthias S, Gregory B, et al. Experimental realization of Shor's quantum factorization algorithm using nuclear magnetic resonance. Nature, 2001, 414: 883–887

13 Vedral V, Barenco A, Ekert A. Quantum networks for elementary arithemetic operations. Phys Rev A, 1996, 54: 147–153

14 Beckman D, Chari A N, Devabhaktuni S, et al. Efficient networks for quantum factoring. Phys Rev A, 1996, 54: 1034–1063

15 Zalka C. Fast versions of Shor's quantum factoring algorithm. Arxiv: quant-ph/9806084v1, 1998

16 Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. London: Cambridge University Press, 2000

17 Griffiths R B, Niu C S. Semiclassical Fourier transform for quantum computation. Phys Rev Lett, 1996,76: 3228–3232

18 Parker S, Plenio M B. Efficient factorization with a single pure qubit and logN mixed qubits. Phys Rev Lett, 2000, 85: 3048–3052

19 Fu X Q, Bao W S, Zhou C. Speeding up implementation for Shor's factorization quantum algorithm. Chinese Sci Bull, 2010, 55: 3648–3653

20 Kenji K, Yukio T. Speeding up elliptic cryptosystems using a signed binary window method. In: Proceeding of the 12th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer-Verlag, 1993. 345–357