DOI: 10.3969/j.issn.1007-5461.2023.05.014

HHL 量子算法的普适量子线路设计

季 雯[1], 叶 宾[1,2*]

(1 中国矿业大学信息与控制工程学院, 江苏 徐州 221116;
2 地下空间智能控制教育部工程研究中心, 江苏 徐州 221116)

摘 要: HHL (Harrow-Hassidim-Lloyd) 量子算法实现了近似求解线性方程组 $\boldsymbol{Ax} = \boldsymbol{b}$, 是许多复杂量子算法的重要组成部分。尽管 HHL 量子算法相比于经典算法能够实现指数级加速, 但是目前 HHL 量子算法大多为抽象的算法描述或分析, 所设计出的量子线路规模很小, 且不具有普适性。在分析 HHL 量子算法原理的基础上, 使用通用量子门自上而下地设计了算法的关键模块, 包括酉矩阵的通用量子门分解模块、量子相位估计模块、量子全加器与乘法器模块、量子态条件旋转变换模块等, 从而实现了求解线性方程组的普适量子线路。利用 IBM qiskit 量子计算开发平台进行的量子仿真实验表明, 所设计的 HHL 量子线路能够求解一般形式的线性方程组, 且易于扩展为中大规模的量子线路。

关 键 词: 量子计算; HHL 量子算法; 量子线路; 量子相位估计; IBM qiskit 平台

中 图 分 类 号 : O431.2; TP301 **文 献 标 识 码 :** A **文章编号:** 1007-5461(2023)05-00747-12

A general quantum circuit design method for HHL quantum algorithm

JI Wen[1], *YE Bin*[1,2*]

(1 School of Information and Control Engineering, China University of Mining and Technology, Xuzhou 221116, China;
2 Engineering Research Center of Intelligent Control for Underground Space, Ministry of Education, Xuzhou 221116, China)

Abstract: Harrow-Hassidim-Lloyd (HHL) quantum algorithm has basically realized the function of solving linear equation $\boldsymbol{Ax} = \boldsymbol{b}$, and it is also the essential ingredient of many complex quantum algorithms. Although HHL quantum algorithm achieves exponential speedup over its classical counterpart, most of the current HHL quantum algorithms are abstract algorithm descriptions or their analyses. Especially, the HHL quantum circuits developed so far are small in scale and not general. By analyzing the basic units of HHL quantum algorithm, the key modules of HHL algorithm, including a unitary matrix decomposition module by general quantum gates, a quantum phase estimation module, a quantum full adder and

基金项目: 徐州市科技计划项目 (KC22286), 河南省网络密码技术重点实验室研究课题 (LNCT2019-S06)
作者简介: 季 雯 (1996 -), 女, 江苏徐州人, 研究生, 主要从事量子计算方面的研究。E-mail: ts19060065a31@cumt.edu.cn
导师简介: 叶 宾 (1980 -), 河南南阳人, 博士, 副教授, 硕士生导师, 主要从事量子计算和量子信息方面的研究。 E-mail: yebin@cumt.edu.cn
收稿日期: 2021-09-24; **修改日期:** 2021-11-22
*通信作者。

multiplier module, and a conditional rotation module of quantum state, etc, were designed from top to down using general quantum gates, thus achieving a general quantum circuit for solving linear equations. Quantum simulations on the IBM qiskit quantum computation development platform show that the designed quantum circuits are suitable for solving more general linear equations and can be easily extended to medium or large-scale quantum circuits.

Key words: quantum computation; HHL quantum algorithm; quantum circuit; quantum phase estimation; IBM qiskit platform

0 引 言

HHL量子算法是由Harrow、Hassidim及Lloyd[1]提出的一种求解量子线性系统问题的量子算法, 其利用量子态的相干叠加与纠缠等特性实现稀疏线性方程组 $\boldsymbol{Ax}=\boldsymbol{b}$ 的快速求解, 与经典的线性方程组求解算法相比, HHL量子算法可以达到指数级加速。对于一个 $N\times N$ 的矩阵 $\boldsymbol{A}$, 若 $\boldsymbol{A}$ 的条件数为 κ, 则HHL量子算法的时间复杂度为 $O\left(\frac{\kappa^2\log_2 N}{\varepsilon}\right)$(其中 ε 为计算精度)。HHL量子算法与Shor质因数分解量子算法和Grover量子搜索算法一样, 已成为许多复杂量子算法的基本组成部分, 且广泛应用于量子支持向量机[2]、量子判别分析[3]、量子线性回归[4]、量子无监督学习[5]、量子神经网络[6]等量子机器学习算法中。在当前的大数据时代, HHL量子算法带来的潜在加速收益非常明显[7, 8]。

基于HHL量子算法, Childs等[9]应用哈密顿量的快速模拟, 将HHL量子算法的计算复杂性由 $O\left(\frac{\kappa^2\log_2 N}{\varepsilon}\right)$ 降低为 $O(\kappa^2\log_2 N\log_2\frac{1}{\varepsilon})$; Wossnig等[10]提出了一种求解非稀疏线性系统的量子算法, 与经典算法相比带来了平方加速; Chen等[11]提出了用于求解布尔多项式方程组的量子算法。对于小规模的二元线性方程组, HHL量子算法已分别在光量子计算机和核磁共振量子信息处理器上得到了实现和验证[12, 13]。虽然目前HHL量子算法在算法分析与实验验证方面取得了以上成果, 但其仍处于较为抽象的算法描述阶段, 对于一般形式的线性方程组, 所设计出的量子线路规模非常小, 且没有完整和普适的量子线路设计方法。

为了在中等规模甚至大规模的量子计算机上实现HHL量子算法, 本文利用厄米矩阵的Pauli分解及乘积公式实现了一般哈密顿量的量子模拟线路, 分别设计了量子相位估计、量子加法与乘法运算、量子态的条件旋转变换等重要算法模块对应的量子线路, 经过IBM qiskit量子软件平台[14]的仿真验证, 构建了一种普适的求解线性方程组的量子线路。

1 HHL算法原理

线性方程组求解问题是对于已知矩阵 $\boldsymbol{A}\in\mathbb{R}^{N\times N}$ 和向量 $\boldsymbol{b}\in\mathbb{R}^N$, 求出使方程组 $\boldsymbol{Ax}=\boldsymbol{b}$ 成立的向量 $\boldsymbol{x}\in\mathbb{R}^N$。利用量子计算机求解线性方程组 $\boldsymbol{Ax}=\boldsymbol{b}$, 首先要进行量子态编码。假设 $\boldsymbol{A}$ 为厄米矩阵, 且 $\boldsymbol{A}$ 的维数 $N=2^{n_b}$(n_b为进行量子态编码所用量子比特数目)。对于归一化单位向量 $\boldsymbol{b}$(或者 $\boldsymbol{x}$), 将其第 i 个元素编码为量子叠加态 $|b\rangle$ (或者量子态 $|x\rangle$) 的第 i 个基态, 那么HHL量子算法就是求出 $|x\rangle$ 以满足 $\boldsymbol{A}|x\rangle=|b\rangle$。

HHL量子算法主要由三个基本模块组成, 即量子相位估计模块、量子态受控旋转模块和量子态反演解算模块, 如图1所示。图1共包含三个量子寄存器, 其中量子寄存器F是1位辅助量子比特寄存器, 寄存器L

用来存储矩阵 $\boldsymbol{A}$ 的特征值的二进制近似, 寄存器 B 用于存储量子态$|b\rangle$以及演化后所得量子态$|x\rangle$, 三个量子寄存器的每个量子比特初态都为$|0\rangle$。

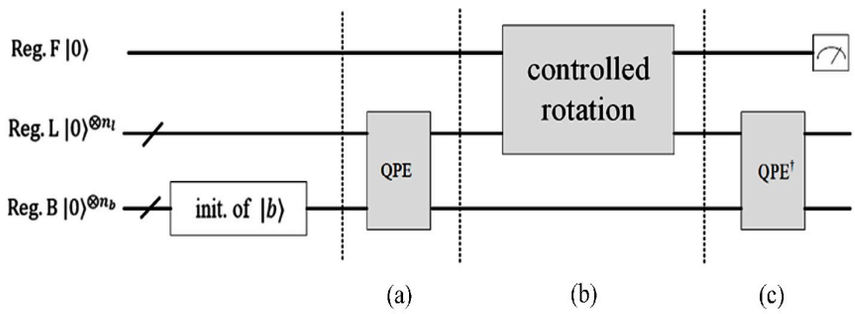

图 1　HHL 量子线路概图。(a) 量子相位估计模块 (QPE); (b) 量子态受控旋转模块; (c) 量子态反演解算模块 (QPE†)[15]

Fig. 1　Diagram of HHL quantum circuit. (a) Quantum phase estimation module (QPE); (b) Quantum state controlled rotation module; (c) Time-reversal of the QPE module (QPE†)[15]

HHL 量子算法的步骤如下[1, 15]: 1) 将量子寄存器 B 初始化为量子态 $|b\rangle$(量子寄存器 B 共有 n_b 个量子比特, 且 $2^{n_b}=N$); 2) 量子相位估计 [QPE, 如图 1(a)]。厄米矩阵 $\boldsymbol{A}$ 具有谱分解 $\boldsymbol{A}=\sum_{i=1}^{N}\lambda_i|u_i\rangle\langle u_i|$, 其中 $|u_i\rangle$ 为对应于实特征值 λ_i 的特征向量, 所以 $\boldsymbol{U}=\mathrm{e}^{\mathrm{i}2\pi\boldsymbol{A}}$ 为酉矩阵, 且具有特征值 $\mathrm{e}^{\mathrm{i}\lambda_i 2\pi}$ 和特征向量$|u_i\rangle$。如果量子寄存器 L 的初态为 $|0\rangle^{\otimes n_l}$, 量子寄存器 B 的状态为 $|u_i\rangle$, 则对矩阵 $\boldsymbol{U}$ 应用量子相位估计算法[16]可实现映射 $|0\rangle^{\otimes n_l}|u_i\rangle\mapsto|\lambda_i\rangle|u_i\rangle$, 其中 $|\lambda_i\rangle$ 为特征值 λ_i 在量子寄存器 L 中的二进制表示。更一般地, 若取矩阵 $\boldsymbol{A}$ 的特征向量 $|u_i\rangle$ 作为基向量, B 的状态 $|b\rangle$ 可表示为 $|b\rangle=\sum_{i=1}^{N}b_i|u_i\rangle$, $b_i\in\mathbb{R}$, 此时将量子态$|b\rangle=\sum_{i=1}^{N}b_i|u_i\rangle$ 输入到量子相位估计算法, 即可实现映射 $\sum_{i=1}^{N}b_i|0\rangle^{\otimes n_l}|u_i\rangle\mapsto\sum_{i=1}^{N}b_i|\lambda_i\rangle|u_i\rangle$; 3) 计算 λ_i 的倒数 $1/\lambda_i$, 并以存储 $|1/\lambda_i\rangle$ 的 L 作为控制寄存器, 对初态为 $|0\rangle$ 的辅助量子比特 F 施加受控旋转量子运算[如图 1(b)], 使 F 的状态近似为 $\sqrt{1-\frac{C^2}{\lambda_j^2}}|0\rangle+\frac{C}{\lambda_j}|1\rangle$ (其中 C 是归一化常数)。此时, 对量子寄存器 F、L 和 B 完成映射 $\sum_{i=1}^{N}b_i|0\rangle\otimes|\lambda_i\rangle\otimes|u_i\rangle\mapsto\sum_{i=1}^{N}b_i\left(\sqrt{1-\frac{C^2}{\lambda_i^2}}|0\rangle+\frac{C}{\lambda_i}|1\rangle\right)\otimes|\lambda_i\rangle\otimes|u_i\rangle$; 4) 对量子寄存器 L 和 B 进行量子相位估计的状态反演 [如图 1(c)], 可得 $\sum_{i=1}^{N}b_i\left(\sqrt{1-\frac{C^2}{\lambda_i^2}}|0\rangle+\frac{C}{\lambda_i}|1\rangle\right)\otimes|\lambda_i\rangle\otimes|u_i\rangle\mapsto\sum_{i=1}^{N}b_i\left(\sqrt{1-\frac{C^2}{\lambda_i^2}}|0\rangle+\frac{C}{\lambda_i}|1\rangle\right)\otimes|0\rangle^{\otimes n_l}\otimes|u_i\rangle$; 5) 对辅助量子寄存器 F 进行量子测量。若测量结果为 1, 则量子寄存器 L 和 B 在测量后的量子态为 $\sqrt{\frac{1}{\sum_{i=1}^{N}|b_i/\lambda_i|^2}}\sum_{i=1}^{N}\frac{b_i}{\lambda_i}|0\rangle^{\otimes n_l}\otimes|u_i\rangle$, 因此 B 的状态与线性方程组的解$|x\rangle=\boldsymbol{A}^{-1}|b\rangle=\sum_{i=1}^{N}(\lambda_i^{-1}|u_i\rangle\langle u_i|)\cdot(b_i|u_i\rangle)=\sum_{i=1}^{N}\frac{b_i}{\lambda_i}|u_i\rangle$ 相比只相差了一个归一化因子。

对于一般形式的线性方程组 $\boldsymbol{Ax}=\boldsymbol{b}$, 若 $\boldsymbol{A}$ 不是厄米矩阵, 则可以通过构造厄米矩阵 $\begin{bmatrix}0 & \boldsymbol{A}\\ \boldsymbol{A}^{\dagger} & 0\end{bmatrix}$, 将 $\boldsymbol{Ax}=\boldsymbol{b}$ 增广转化为一个维数更高的线性方程组 $\begin{bmatrix}0 & \boldsymbol{A}\\ \boldsymbol{A}^{\dagger} & 0\end{bmatrix}\begin{bmatrix}0\\ \boldsymbol{x}\end{bmatrix}=\begin{bmatrix}\boldsymbol{b}\\ 0\end{bmatrix}$, 并利用上述HHL量子算法进行求解。

2 HHL量子电路设计

2.1 量子相位估计模块

对于一个酉矩阵 $\boldsymbol{U}$, 它具有模为1的复特征值 $e^{i\theta}$ 和特征向量 $|u_i\rangle$, 量子相位估计算法的目的即是在一定的误差范围内估算相位 θ 的值[16]。量子相位估计算法的框架及概图如图2所示, 图中 $\boldsymbol{H}$ 表示Hadamard量子门, $\mathrm{QFT}^{\dagger}$ 表示量子傅里叶逆变换算法, $\boldsymbol{U}^j$ 表示逐次以量子寄存器L中的量子比特为控制比特且以寄存器B为目标量子寄存器的受控 $\boldsymbol{U}^j$ 运算。

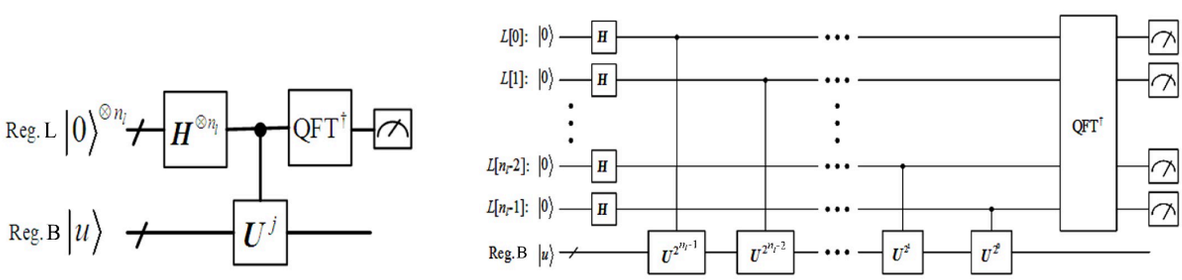

图2 量子相位估计算法的量子线路 (a) 框架和 (b) 概图

Fig. 2 (a) Quantum circuit framework and (b) diagram of quantum phase estimation algorithm

对于厄米矩阵 $\boldsymbol{A}$, 相应的酉矩阵 $\boldsymbol{U}=e^{i2\pi\boldsymbol{A}}$ 具有特征值 $e^{i2\pi\lambda}$ 和特征向量 $|u\rangle$, 其中 $|u\rangle$ 为对应于 $\boldsymbol{A}$ 的实特征值 λ 的特征向量。若将 $\boldsymbol{U}$ 的特征向量 $|u\rangle$ 载入到图2中的量子寄存器B, 且以受控 $\boldsymbol{U}^j$ 进行演化, 并经量子傅里叶逆变换之后, 量子相位估计算法最终对量子寄存器L进行量子测量, 将给出二进制串 $l_{n_l-1}l_{n_l-2}\cdots l_1l_0$。此时 $\boldsymbol{A}$ 对应于特征向量 $|u\rangle$ 的实特征值 λ 可被估算为 $(l_{n_l-1}l_{n_l-2}\cdots l_1l_0)_{\mathrm{bin}}/2^{n_l}$。

量子相位估计算法的具体步骤如下: 1) 将 $\boldsymbol{U}$ 的特征向量 $|u\rangle$ 载入到量子寄存器B; 2) 对量子寄存器L中的每个量子比特都执行Hadamard量子门运算 [如图2(b)], 得到量子态 $\frac{1}{\sqrt{2^{n_l}}}\left(|0\rangle+|1\rangle\right)^{\otimes n_l}\otimes|u\rangle$; 3) 从量子寄存器L的最低位 $L[0]$开始, 依次施加受控 $\boldsymbol{U}^j$ (其中 $j=2^{n_l-1},2^{n_l-2},\cdots,2^1,2^0$) 量子门作用于量子寄存器B上 [如图2(b)所示]。由于 $U^{2^{n_l-1}}|u\rangle=U^{2^{n_l-2}}UU|u\rangle=U^{2^{n_l-2}}e^{4\pi i\lambda}|u\rangle=\ldots=e^{2\pi i\lambda 2^{n_l-1}}|u\rangle$ 以及 $|0\rangle\otimes|u\rangle+|1\rangle\otimes e^{2\pi i\lambda}|u\rangle=(|0\rangle+e^{2\pi i\lambda}|1\rangle)\otimes|u\rangle$, 经过一系列受控 $\boldsymbol{U}^j$ 运算, 可得到量子态 $\frac{1}{\sqrt{2^{n_l}}}\sum_{k=0}^{2^{n_l}-1}e^{2\pi i\lambda k}|k\rangle\otimes|u\rangle$, 其中 k 为存储在量子寄存器L中的 n_l 位二进制数; 4) 对量子寄存器L进行量子傅里叶逆变换, 可得 $\frac{1}{\sqrt{2^{n_l}}}\sum_{k=0}^{2^{n_l}-1}e^{2\pi i\lambda k}|k\rangle\otimes|u\rangle\xrightarrow{\mathrm{QFT}^{\dagger}}\frac{1}{2^{n_l}}\sum_{x=0}^{2^{n_l}-1}\sum_{k=0}^{2^{n_l}-1}e^{\frac{-2\pi ik}{2^{n_l}}\left(x-2^{n_l}\lambda\right)}|x\rangle\otimes|u\rangle$, 由于 $|x\rangle$ 的幅值在 $x=2^{n_l}\lambda$ 时取得最大值, 因此若对量子寄存器L进行量子测量, 测量得到 $2^{n_l}\lambda$ 的概率是最大的。

2.1.1　酉矩阵$\boldsymbol{U}$的通用量子门分解

为了利用通用量子门设计HHL量子线路, 必须根据厄米矩阵$\boldsymbol{A}$实现图2(b) 中的一系列受控$\boldsymbol{U}^j$运算。将结合厄米矩阵$\boldsymbol{A}$的泡利矩阵分解以及积公式[17, 18], 设计和实现酉矩阵$\boldsymbol{U}$的量子线路。利用积公式设计的量子电路更具有直观性, 且易于集成。

基于泡利矩阵$\boldsymbol{X}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$、$\boldsymbol{Y}=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$、$\boldsymbol{Z}=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$和单位矩阵$\boldsymbol{I}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, 任意厄米矩阵$\boldsymbol{A}_{2^{n_b}\times 2^{n_b}}$都可以进行泡利矩阵分解, 即

$$\boldsymbol{A}_{2^{n_b}\times 2^{n_b}}=\sum_{G_1,G_2,\cdots,G_{n_b}\in\{\boldsymbol{I},\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}\}} a_{G_1,G_2,\cdots,G_{n_b}}(G_1\otimes G_2\otimes\cdots\otimes G_{n_b}), \tag{1}$$

式中: 系数$a_{G_1,G_2,\cdots,G_{n_b}}=\dfrac{1}{2^{n_b}}\mathrm{tr}[(G_1\otimes G_2\otimes\cdots\otimes G_{n_b})\boldsymbol{A}_{2^{n_b}\times 2^{n_b}}]$, tr(·)表示矩阵的迹。根据 (1) 式, 酉矩阵$\boldsymbol{U}=\mathrm{e}^{\mathrm{i}2\pi\boldsymbol{A}}$可写为$\boldsymbol{U}=\mathrm{e}^{\mathrm{i}2\pi\sum\limits_{G_1,G_2,\cdots,G_{n_b}} a_{G_1,G_2,\cdots,G_{n_b}}(G_1\otimes G_2\otimes\cdots\otimes G_{n_b})}$, 结合积公式的一阶近似[19], $\boldsymbol{U}$可进一步写为

$$\boldsymbol{U}=\lim_{m\to\infty}\left(\prod_{G_1,G_2,\cdots,G_{n_b}\in\{\boldsymbol{I},\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}\}}\mathrm{e}^{\mathrm{i}2\pi a_{G_1,G_2,\cdots,G_{n_b}}(G_1\otimes G_2\otimes\cdots\otimes G_{n_b})/m}\right)^m. \tag{2}$$

以下对 (2) 式中形如$\mathrm{e}^{\mathrm{i}2\pi a_{G_1,G_2,\cdots,G_{n_b}}(G_1\otimes G_2\otimes\cdots\otimes G_{n_b})/m}$的运算项 (简写为$\mathrm{e}^{\mathrm{i}2\pi a(G_1\otimes G_2\otimes\cdots\otimes G_{n_b})/m}$) 进行量子线路设计。对于多量子比特运算$\mathrm{e}^{\mathrm{i}2\pi a(G_1\otimes G_2\otimes\cdots\otimes G_{n_b})/m}$, 如果其中某个$G_i=I$, 则表明量子寄存器B的第$i$位无须进行任何运算; 反之, 如果$G_i\in\{\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}\}$, 则从所有$G_i$中选取$i$的最大值$i^*=\max\{i|G_i\in\{\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}\}\}$, 对量子寄存器B的第$i^*$位施加单比特旋转门$\mathrm{e}^{\mathrm{i}2\pi a\boldsymbol{X}/m}=R_x(-2\dfrac{2\pi a}{m})$, 相应的量子线路如图3(a) 所示。进一步, 根据Clifford量子线路和量子旋转门的性质, 可得$\mathrm{CNOT}\cdot\left(R_x(a)\otimes\boldsymbol{I}\right)\cdot\mathrm{CNOT}=\mathrm{e}^{-\mathrm{i}\frac{a}{2}\mathrm{CNOT}\cdot(\boldsymbol{X}\otimes\boldsymbol{I})\cdot\mathrm{CNOT}}=\mathrm{e}^{-\mathrm{i}\frac{a}{2}\boldsymbol{X}\otimes\boldsymbol{X}}$(其中CNOT为受控量子非门), 因此图3(a) 中的单量子比特运算$\mathrm{e}^{\mathrm{i}2\pi a\boldsymbol{X}/m}$扩展为双比特量子运算$\mathrm{e}^{\mathrm{i}2\pi a\boldsymbol{X}\otimes\boldsymbol{X}/m}$的量子线路, 如图3(b) 所示。类似地, 多量子比特运算$\mathrm{e}^{\mathrm{i}2\pi a\boldsymbol{X}\otimes\boldsymbol{X}\otimes\boldsymbol{X}/m}$的量子线路如图3(c) 所示。

以这些单量子比特或多量子比特状态绕X轴的旋转运算为基础, 结合$\boldsymbol{HXH}=\boldsymbol{Z}$以及$\boldsymbol{SXS}^\dagger=\boldsymbol{Y}$ (其中$\boldsymbol{H}=\dfrac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$为Hadamard门, $\boldsymbol{S}=\begin{bmatrix}1 & 0\\ 0 & \mathrm{e}^{\mathrm{i}\frac{\pi}{2}}\end{bmatrix}$为量子相位门), 可实现任意量子比特的旋转运算$\mathrm{e}^{\mathrm{i}2\pi a\cdot(G_1\otimes G_2\otimes\cdots\otimes G_{n_b})/m}$。例如, 图3(d)~(f)分别为量子比特运算$\mathrm{e}^{\mathrm{i}2\pi a\boldsymbol{Z}/m}$、双量子比特运算$\mathrm{e}^{\mathrm{i}2\pi a\boldsymbol{Y}\otimes\boldsymbol{X}/m}$和多量子比特运算$\mathrm{e}^{\mathrm{i}2\pi a\boldsymbol{Y}\otimes\boldsymbol{I}\otimes\boldsymbol{Z}/m}$的量子线路。将图3所示的典型量子线路与 (1)、(2) 式相结合, 即可构成酉算符$\boldsymbol{U}=\mathrm{e}^{\mathrm{i}2\pi\boldsymbol{A}}$的通用量子门近似分解线路。此时, 对酉算符$\boldsymbol{U}=\mathrm{e}^{\mathrm{i}2\pi\boldsymbol{A}}$的近似误差正比于$1/m$。

2.1.2　受控U^j运算的量子线路

当厄米矩阵$\boldsymbol{A}$的维数较大或者 (2) 式中m取值较大时, 酉算符$\boldsymbol{U}=\mathrm{e}^{\mathrm{i}2\pi\boldsymbol{A}}$对应的量子线路深度将非常大, 这不利于设计受控$\boldsymbol{U}^j$运算的量子线路。在第2.1.1节中详细介绍了$\boldsymbol{U}^j$的设计方法, 本研究使用的是IBM qiskit量子计算开发平台[20], 因此在设计受控$\boldsymbol{U}^j$的量子线路时调用量子线路对象的to_gate( )方法, 将酉算符$\boldsymbol{U}$封装为1个自定义的量子门U_gate; 然后对封装后的量子门U_gate调用U_gate.control( ), 并以寄存器L中的量子比特为控制位, 嵌入到量子线路中, 实现1次受控$\boldsymbol{U}$运算 [参考图2(b)]。需要注意的是, 由于全局相

位不可观测, 在第2.1.1节中设计酉矩阵 $\boldsymbol{U}$ 的量子线路时并不需要考虑 $e^{i2\pi a(\boldsymbol{I}\otimes\boldsymbol{I}\otimes\cdots\otimes\boldsymbol{I})/m}$ 的项; 但是在设计受控 $\boldsymbol{U}$ 运算量子线路时, $e^{i2\pi a/m}$ 成为相对相位, 是不可忽略的。因此需要利用Phase Kickback方法将相移 $e^{i2\pi a/m}$ 从目标寄存器B等价地转移到寄存器L的相应控制位 (如图4所示)。受控 $\boldsymbol{U}^j$ 运算由串联 j 个受控 $\boldsymbol{U}$ 运算的量子线路来实现。

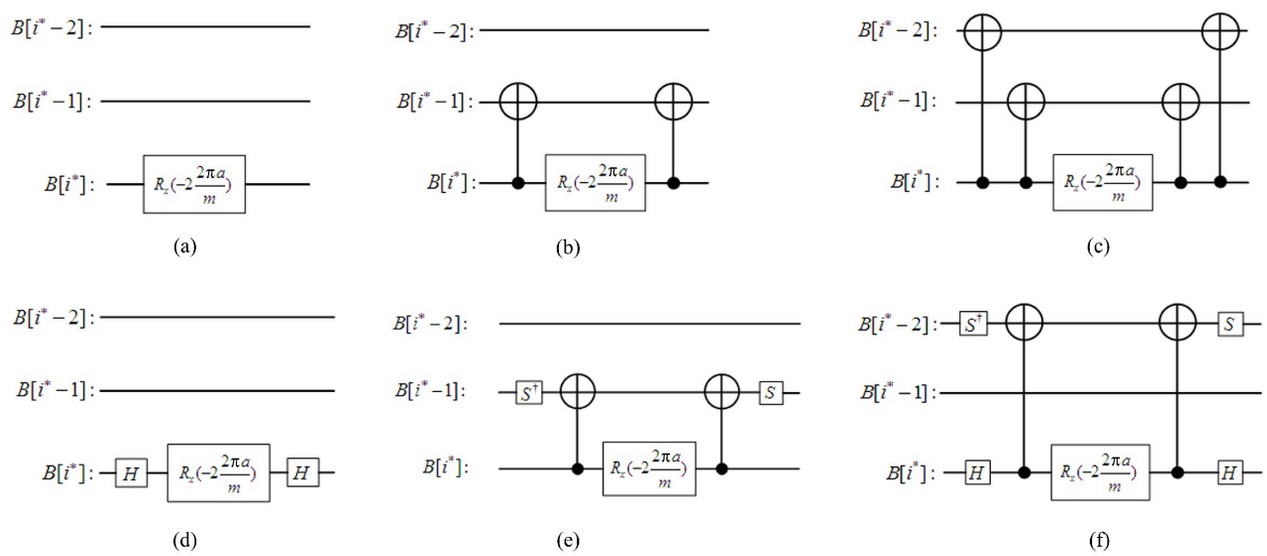

图3 酉矩阵 $\boldsymbol{U}$ 的通用量子门分解中部分量子线路图。(a) 单量子比特运算 $e^{i2\pi aX/m}$; (b) 双比特量子运算 $e^{i2\pi aX\otimes X/m}$; (c) 多量子比特运算 $e^{i2\pi aX\otimes X\otimes X/m}$; (d) 量子运算 $e^{i2\pi aZ/m}$; (e) 量子运算 $e^{i2\pi aY\otimes X/m}$; (f) 量子运算 $e^{i2\pi aY\otimes I\otimes Z/m}$

Fig. 3 Some quantum circuits in decomposition of unitary matrix $\boldsymbol{U}$. (a) Single qubit operation $e^{i2\pi aX/m}$; (b) Two qubits quantum operation $e^{i2\pi aX\otimes X/m}$; (c) Multi-qubit quantum operation $e^{i2\pi aX\otimes X\otimes X/m}$; (d) Quantum operation $e^{i2\pi aZ/m}$; (e) Quantum operation $e^{i2\pi aY\otimes X/m}$; (f) Quantum operation $e^{i2\pi aY\otimes I\otimes Z/m}$

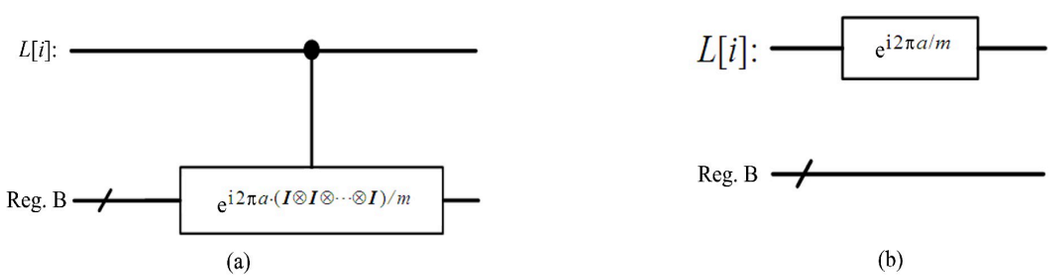

图4 受控 $e^{i2\pi a(\boldsymbol{I}\otimes\boldsymbol{I}\otimes\cdots\otimes\boldsymbol{I})/m}$ 运算经过Phase Kickback变换前 (a) 和变换后 (b) 的等价量子线路

Fig. 4 Equivalent quantum circuits of controlled $e^{i2\pi a(\boldsymbol{I}\otimes\boldsymbol{I}\otimes\cdots\otimes\boldsymbol{I})/m}$ before (a) and after (b) the Phase Kickback

2.1.3 量子傅里叶变换QFT

量子傅里叶变换是对量子态 $|\xi\rangle=\sum_{\zeta=0}^{N-1}\xi_i|i\rangle$ 实现映射 $|\xi\rangle=\frac{1}{\sqrt{N}}\sum_{\zeta=0}^{N-1}e^{\frac{2\pi i}{N}\zeta\zeta}|\zeta\rangle$, 对应的酉演化矩阵为 $U_{\mathrm{QFT}}=\frac{1}{\sqrt{N}}\sum_{\xi=0}^{N-1}\sum_{\zeta=0}^{N-1}e^{\frac{2\pi i}{N}\zeta\xi}|\zeta\rangle\langle\xi|$。量子傅里叶变换是许多复杂量子算法的子程序, 其逆变换在HHL量子算法中作用在

量子寄存器L上 [如图2(b)][16]。量子傅里叶变换线路如图5所示, 其中 $\boldsymbol{R}_k=\begin{bmatrix}1 & 0\\ 0 & \exp\left(\frac{2\pi \mathrm{i}}{2^k}\right)\end{bmatrix}$, 在线路最右端有多个量子交换门。量子傅里叶变换满足酉演化性质, 因此量子傅里叶逆变换的量子线路可以通过对图5所示的量子线路做左右镜像翻转而得到。

2.2　量子态受控旋转模块

量子态受控旋转运算模块主要对量子寄存器F和L完成映射: $\sum_{i=1}^{N}b_i|0\rangle\otimes|\lambda_i\rangle\mapsto\sum_{i=1}^{N}b_i\left(\sqrt{1-\frac{C^2}{\lambda_i^2}}|0\rangle+\frac{C}{\lambda_i}|1\rangle\right)\otimes|\lambda_i\rangle$, 主要由两部分构成: 1) 根据QPE给出的特征值 λ 的二进制近似 (存储在L中), 计算 $1/\lambda$; 2) 根据 $1/\lambda$, 对初态为$|0\rangle$的辅助量子比特F施加受控旋转运算, 得到 $\sqrt{1-\frac{C^2}{\lambda^2}}|0\rangle+\frac{C}{\lambda}|1\rangle$。

2.2.1　计算 $1/\lambda$

若已知$\boldsymbol{A}$的某个特征值 λ, 通常使用牛顿迭代法求取 $1/\lambda$, 即: 将 $f(x)=\frac{1}{x}-\lambda$ 以及 $f'(x)=-x^{-2}$ 同时代入牛顿迭代公式 $x_{n+1}=x_n-\frac{f(x_n)}{f'(x_n)}$, 可得 $x_{n+1}=x_n-\frac{x_n^{-1}-\lambda}{-x_n^{-2}}=-\lambda x_n^2+2x_n$。因此对于 $1/\lambda$ 的某个初值 x_0, 可以通过 $x_{n+1}=-\lambda x_n^2+2x_n$ 的多次迭代得到 $1/\lambda$ 的近似值。在设计量子线路中引入这种方法计算 $1/\lambda$, 该迭代运算主要由加法和乘法运算构成, 采用文献 [21] 提出的量子加法线路实现两个二进制串的加法运算, 其基于量子傅里叶变换实现量子加法运算, 无需辅助量子比特, 量子线路如图6所示。

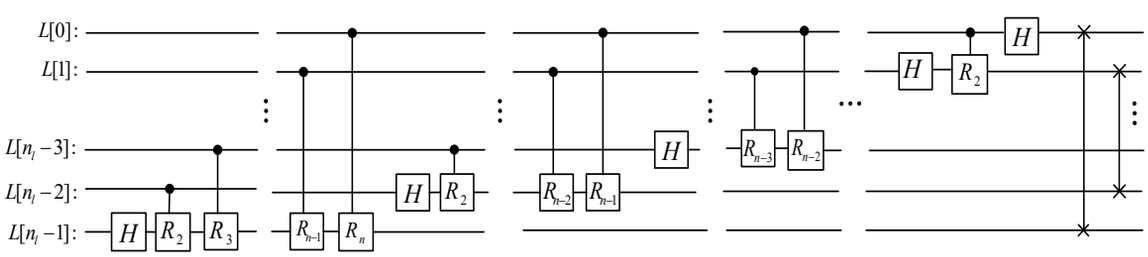

图5　量子傅里叶变换线路

Fig. 5　Circuit of quantum Fourier transform

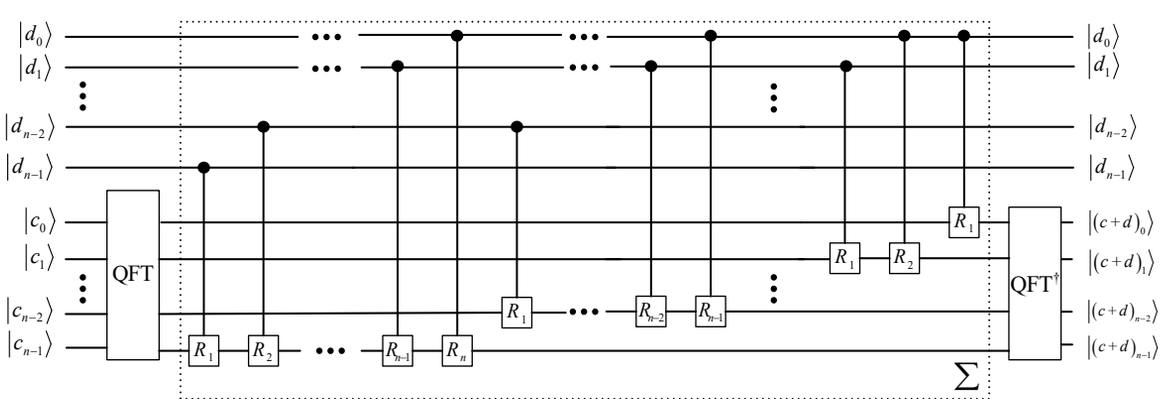

图6　两个二进制串 $|d_{n-1}d_{n-2}\cdots d_1d_0\rangle$ 和 $|c_{n-1}c_{n-2}\cdots c_1c_0\rangle$ 的量子加法线路

Fig. 6　Quantum adder of two binary strings $|d_{n-1}d_{n-2}\cdots d_1d_0\rangle$ and $|c_{n-1}c_{n-2}\cdots c_1c_0\rangle$

量子乘法运算线路有基于经典数字逻辑算法的量子乘法器[22, 23]和基于QFT的量子乘法器[24, 25]等, 其中基于QFT的量子乘法器通过累加来实现乘法运算, 可看做图6所示量子加法线路的扩展, 其不需要辅助量子位, 且很容易推广到定点数的乘法运算, 因此使用图7所示基于QFT的量子乘法器进行乘法运算。在图7中, c 和 d 都是 n 位的二进制数, 因此 cd 需要使用 $2n$ 个量子比特存储, 它们被初始化为 $|0\rangle^{\otimes 2n}$。

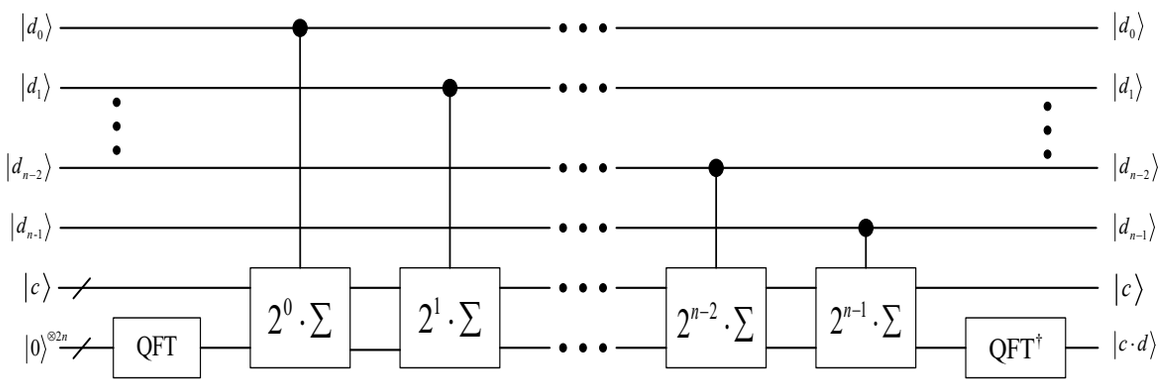

图7 二进制串 $|d_{n-1}d_{n-2}\cdots d_1d_0\rangle$ 和 $|c_{n-1}c_{n-2}\cdots c_1c_0\rangle$ 相乘的量子线路, 其中 Σ 为图6中虚框包含的相位叠加部分

Fig. 7 Quantum multiplier of two binary strings $|d_{n-1}d_{n-2}\cdots d_1d_0\rangle$ and $|c_{n-1}c_{n-2}\cdots c_1c_0\rangle$ where Σ corresponds to the quantum phase addition module in Fig. 6

2.2.2 受控旋转

在第2.2.1节计算出 λ^{-1} 后, 假设量子寄存器L中给出的二进制串为 $\phi_1\phi_2\cdots\phi_{n_l-1}\phi_{n_l}$, $\phi_j\in\{0,1\}$, $j=1, 2, \ldots, n_l$, 则它表示 $\boldsymbol{A}$ 的某个特征值 λ 的倒数 λ^{-1} 可近似为 $\frac{\left(\phi_1\phi_2\cdots\phi_{n_l-1}\phi_{n_l}\right)}{2^{n_l}}=0$, $\phi_1\phi_2\cdots\phi_{n_l-1}\phi_{n_l}=\sum_{j=1}^{n_l}\phi_j2^{-j}$。将 $2\lambda^{-1}\approx\sum_{j=1}^{n_l}\frac{\phi_j}{2^{j-1}}$ 代入旋转算子 $R_y(\theta)=\mathrm{e}^{-\frac{\mathrm{i}\theta Y}{2}}=\begin{bmatrix}\cos(\theta/2) & -\sin(\theta/2)\\ \sin(\theta/2) & \cos(\theta/2)\end{bmatrix}$ 可得

$$R_y\left(2\lambda^{-1}\right)=\mathrm{e}^{-\mathrm{i}\lambda^{-1}Y}=\mathrm{e}^{-\mathrm{i}Y\sum_{j=1}^{n_l}\phi_j2^{-j}}=\prod_{j=1}^{n_l}\mathrm{e}^{-\frac{\mathrm{i}Y\phi_j}{2^j}}=\prod_{j=1}^{n_l}R_y\left(\frac{\phi_j}{2^{j-1}}\right),\tag{3}$$

此外

$$R_y\left(\frac{\phi_j}{2^{j-1}}\right)|0\rangle=\begin{bmatrix}\cos(\phi_j/2^j) & -\sin(\phi_j/2^j)\\ \sin(\phi_j/2^j) & \cos(\phi_j/2^j)\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}=\cos\left(\frac{\phi_j}{2^j}\right)|0\rangle+\sin\left(\frac{\phi_j}{2^j}\right)|1\rangle\approx\cos\left(\frac{\phi_j}{2^j}\right)|0\rangle+\frac{\phi_j}{2^j}|1\rangle.\tag{4}$$

(3) 和 (4) 式表明如果以 $\phi_1\phi_2\cdots\phi_{n_l-1}\phi_{n_l}$ 中各个二进制位作为控制比特, 以初态为 $|0\rangle$ 的量子比特 F 为目标量子比特, 进行如图8所示的一系列受控 $R_y\left(\frac{\phi_j}{2^{j-1}}\right)$ 旋转运算, 则可在辅助量子比特 F 上得到量子叠加态 $\sqrt{1-\frac{C^2}{\lambda^2}}|0\rangle+\frac{C}{\lambda}|1\rangle$。

量子线路的时间复杂性通常以实现该量子线路的基本量子门的数量来度量[26]。本研究设计的HHL算法量子线路可分为四个模块 (如图1所示), 即量子态初始化模块、量子相位估计模块、量子态受控旋转模块和量子态反演解算模块, 其计算复杂度分别为 $O(n)$、$O(2^n)$、$O(2^{n+1})$ 和 $O(2^n)$, 因此HHL量子线路的计算复杂度为 $O(2^{n+2})$。此外, 还可用受控量子门的数量来度量量子线路的时间复杂性[27], 由于HHL量子线路

中QPE模块及其反演模块的受控量子门数量都为 $O\left(2^{n-3}\right)$, 量子态受控旋转模块的受控量子门数量为 $O\left(2^{n-2}\right)$, 据此计算HHL量子线路的时间复杂度为 $O\left(2^{n-1}\right)$。

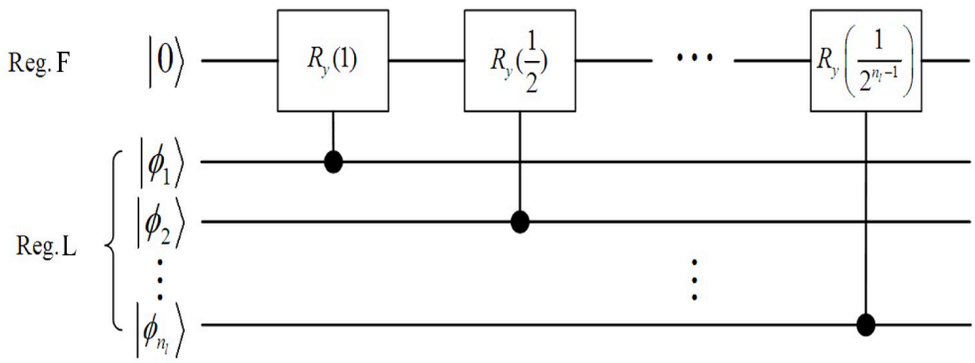

图8　受控旋转运算量子线路图

Fig. 8　Quantum circuit of the controlled rotation operation

3　一个 $\boldsymbol{A}\in\mathbb{R}^{4\times4}$ 的示例

在线性方程组 $\boldsymbol{Ax}=\boldsymbol{b}$ 中, 取 $\boldsymbol{A}=\begin{bmatrix}4.25 & -0.25 & -1.75 & 1.75\\ -0.25 & 4.25 & 1.75 & -1.75\\ -1.75 & 1.75 & 3.25 & -1.25\\ 1.75 & -1.75 & -1.25 & 3.25\end{bmatrix}$, $\boldsymbol{b}=[0.5,\ 0.5,\ 0.5,\ 0.5]^{\mathrm{T}}$, 易得 $\boldsymbol{A}$ 的特征值分别为 $\lambda_j=1,2,4,8, j=1,2,3,4$。图9(a) 给出了在IBM qiskit中求解该线性系统的量子线路, 与图1中量子线路的结构相似, 在图9(a) 中首先将量子寄存器B初始化为 $[0.5,\ 0.5,\ 0.5,\ 0.5]^{\mathrm{T}}$, 为了使量子线路结构清晰, 在qiskit中对QPE模块进行了封装, 该模块的具体线路如图9(c) 所示 (其中的酉算符 $\boldsymbol{U}=\mathrm{e}^{\mathrm{i}2\pi\boldsymbol{A}}$ 采用第2.1.1节的通用量子门分解方法进行近似, 且 (2) 式中 $m=20$)。在求取倒数 $\lambda_j^{-1}=1,\frac{1}{2},\frac{1}{4},\frac{1}{8}$ 时, 由于它们依次对应量子寄存器L中计算得到的二进制串 0001, 1000, 0100, 0010 (都扩大了 $2^4=16$ 倍, 不会改变算法运算结果), 将这些二进制串与 $\boldsymbol{A}$ 的特征值 $\lambda_1=1=(0001)_{\mathrm{bin}}$, $\lambda_2=2=(0010)_{\mathrm{bin}}$, $\lambda_3=4=(0100)_{\mathrm{bin}}$, $\lambda_4=8=(1000)_{\mathrm{bin}}$ 相比较可知, 在保持L中 $L[0]$ 和 $L[2]$ 不变的情况下, 交换 $L[1]$ 与 $L[3]$ 位, 即可实现求取倒数的运算 [如图9(a) 中的第1个量子交换门所示]。在图9(a) 第1个量子交换门之后依次为量子受控旋转、量子交换门、量子相位估计的反演以及量子测量部分。量子相位估计整体上是酉运算, 所以量子相位估计反演部分的量子线路可以由图2量子相位估计线路的水平镜像得到。

图9(b) 给出了该量子线路在qiskit仿真平台上运行10000次后的统计直方图, 其中横坐标上的3位二进制串的第1位表示辅助量子比特 F 的测量结果, 后2位为寄存器B 的测量结果。从图9(b) 可以看出, 当 F 的测量结果为“1” 时[对应于图 9(b) 横轴上后4组数据), 在B中得到这4个状态的概率分别为0.119、0.124、0.244和0.246, 这与该线性方程组的真实解 $(0.125,\ 0.125,\ 0.25,\ 0.25)^{\mathrm{T}}$ 较为接近。图9(b) 所示的求解结果与真实解存在偏差有两方面的原因: 一方面是由于酉矩阵 $\boldsymbol{U}=\mathrm{e}^{\mathrm{i}2\pi\boldsymbol{A}}$ 采用了近似分解, 另一方面是由于量子测量结果本身就是概率性的, 存在一定的偏差。

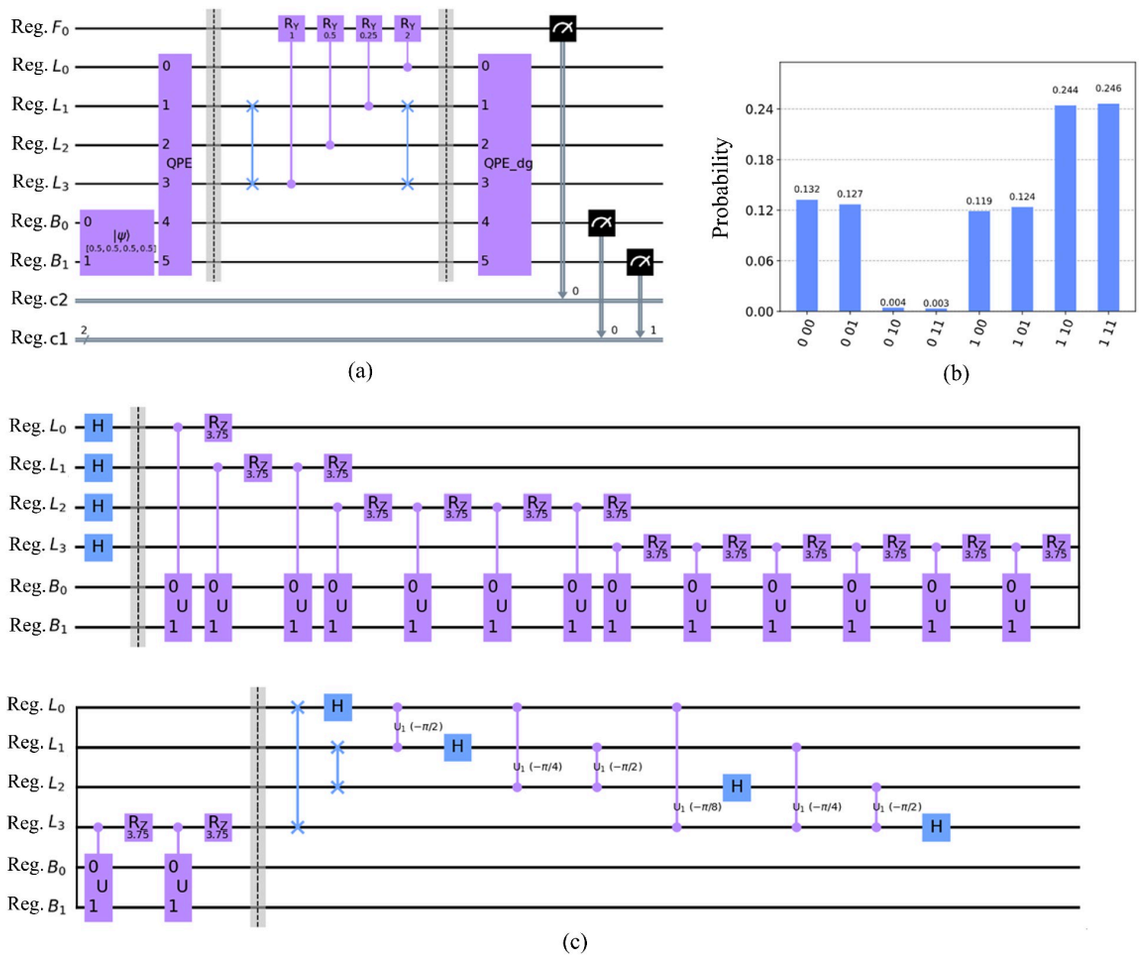

图9 IBM qiskit设计的HHL量子线路示例及其仿真结果。(a) 求解线性方程组的量子线路概图; (b) 量子测量结果的概率直方图; (c) 图 (a) 中封装的QPE模块

Fig. 9 An example of HHL quantum circuit designed by IBM qiskit and its simulation results. (a) Quantum circuit diagram for solving linear equations; (b) Probability histogram of the quantum measurement; (c) QPE module encapsulated in diagram (a)

4 结 论

HHL量子算法在量子数值计算和量子机器学习算法等方面有着广泛的应用价值, 但是目前仍然处在抽象的算法分析与描述阶段, 使用IBM qiskit量子计算平台对HHL量子算法的通用量子线路进行了设计和仿真。该量子线路采用了模块化设计方法, 便于在中等或大规模量子计算硬件上实现。仿真结果验证了所设计量子线路的正确性。尽管所设计量子线路使用辅助量子比特数目很少, 量子线路宽度也较小, 但是整个量子线路的深度很大, 这对整体抗噪性能非常不利, 后续将进一步优化量子线路的结构, 以降低线路深度。

参考文献:

[1] Harrow A W, Hassidim A, Lloyd S. Quantum algorithm for linear systems of equations [J]. *Physical Review Letters*, 2009, 103 (15): 150502.

[2] Saini S, Khosla P, Kaur M, *et al*. Quantum driven machine learning [J]. *International Journal of Theoretical Physics*, 2020, 59 (12): 4013-4024.

[3] Cong I, Duan L M. Quantum discriminant analysis for dimensionality reduction and classification [J]. *New Journal of Physics*, 2016, 18(7): 073011.

[4] Yu C H, Gao F, Wen Q Y. An improved quantum algorithm for ridge regression [J]. *IEEE Transactions on Knowledge and Data Engineering*, 2021, 33(3): 858-866.

[5] Wiebe N, Kapoor A, Svore K M. Quantum algorithms for nearest-neighbor methods for supervised and unsupervised learning [J]. *Quantum Information & Computation*, 2015, 15(3-4): 316-356.

[6] Amin M H, Andriyash E, Rolfe J, *et al*. Quantum Boltzmann machine [J]. *Physical Review X*, 2018, 8(2): 021050.

[7] Huang Y M, Lei H, Li X Y. A survey on quantum machine learning [J]. *Chinese Journal of Computers*, 2018, 41(1): 145-163.
黄一鸣, 雷 航, 李晓瑜. 量子机器学习算法综述 [J]. 计算机学报, 2018, 41(1): 145-163.

[8] Lu S C, Zheng Y, Wang X T, *et al*. Quantum machine learning [J]. *Control Theory & Applications*, 2017, 34(11): 1429-1436.
陆思聪, 郑 昱, 王晓霆, 等. 量子机器学习 [J]. 控制理论与应用, 2017, 34(11): 1429-1436.

[9] Childs A M, Kothari R, Somma R D. Quantum algorithm for systems of linear equations with exponentially improved dependence on precision [J]. *SIAM Journal on Computing*, 2017, 46(6): 1920-1950.

[10] Wossnig L, Zhao Z K, Prakash A. Quantum linear system algorithm for dense matrices [J]. *Physical Review Letters*, 2018, 120: 050502.

[11] Chen Y A, Gao X S. Quantum algorithm for Boolean equation solving and quantum algebraic attack on cryptosystems [J]. *Journal of Systems Science and Complexity*, 2022, 35(1): 373-412.

[12] Zhang X, Yang Z W, Zhang X D. Simplified experimental scheme of quantum algorithm for solving linear equations with single photons [J]. *Optics Express*, 2019, 27(3): 3369-3378.

[13] Pan J, Cao Y D, Yao X W, *et al*. Experimental realization of quantum algorithm for solving linear systems of equations [J]. *Physical Review A*, 2014, 89(2): 022313.

[14] Dai J, Li Z Q, Pan S H, *et al*. Deutsch-Jozsa algorithm realized on IBM Q [J]. *Chinese Journal of Quantum Electronics*, 2020, 37(2): 202-209.
戴 娟, 李志强, 潘苏含, 等. 基于IBM Q的Deutsch-Jozsa算法实现 [J]. 量子电子学报, 2020, 37(2): 202-209.

[15] Duan B J, Yuan J B, Yu C H, *et al*. A survey on HHL algorithm: From theory to application in quantum machine learning [J]. *Physics Letters A*, 2020, 384(24): 126595.

[16] Nielsen M A, Chuang I L. 量子计算和量子信息-量子信息部分 [M]. 赵千川, 译. 北京: 清华大学出版社, 2006: 198-223.

[17] Low G H, Chuang I L. Optimal Hamiltonian simulation by quantum signal processing [J]. *Physical Review Letters*, 2017, 118: 010501.

[18] Low G H, Chuang I L. Hamiltonian simulation by qubitization [J]. *Quantum*, 2019, 3: 163.

[19] Lloyd S. Universal quantum simulators [J]. *Science*, 1996, 273(5278): 1073-1078.

[20] Koch D, Wessing L, Alsing P M. Introduction to coding quantum algorithms: A tutorial series using qiskit [OL]. 2019, arXiv: 1903.04359. https://arxiv.org/abs/1903.04359.

[21] Draper T G. Addition on a quantum computer [OL]. 2000, arXiv: quant-ph/0008033.

[22] Li H S, Fan P, Xia H Y, *et al*. Efficient quantum arithmetic operation circuits for quantum image processing [J]. *Science China Physics*, Mechanics & Astronomy, 2020, 63(8): 280311.

[23] Babu H M H. Cost-efficient design of a quantum multiplier-accumulator unit [J]. *Quantum Information Processing*, 2017, 16 (1): 30.

[24] Ruiz-Perez L, Garcia-Escartin J C. Quantum arithmetic with the quantum Fourier transform [J]. *Quantum Information Processing*, 2017, 16(6): 152.

[25] Pavlidis A, Gizopoulos D. Fast quantum modular exponentiation architecture for Shor's factoring algorithm [J]. *Quantum Information and Computation*, 2014, 14(7&8): 649-682.

[26] Saeedi M, Markov I L. Synthesis and optimization of reversible circuits-a survey [J]. *ACM Computing Surveys*, 2013, 45(2): 1-34.

[27] Wei L H, Zhu P C, Guan Z J. Quantum linear logic synthesis algorithm based on L-ESOP reduction [J]. *Journal of Computer-Aided Design & Computer Graphics*, 2018, 30(8): 1579-1588.
卫丽华, 朱鹏程, 管致锦. 基于L-ESOP约简的量子线性电路逻辑综合算法 [J]. 计算机辅助设计与图形学学报, 2018, 30 (8): 1579-1588.