中国科学: 信息科学　2017 年　第 47 卷　第 10 期: 1277–1299
SCIENTIA SINICA Informationis　中国科学院学部　科学与技术前沿论坛
《中国科学》杂志社 SCIENCE CHINA PRESS
量子计算专题 • 评述

量子算法的一些进展

魏世杰[1,2], 王涛[1], 阮东[1,2], 龙桂鲁[1,2,3*]

1. 清华大学物理系低维量子物理国家重点实验室, 北京 100084
2. 量子物质科学协同创新中心, 北京 100084
3. 清华信息科学技术国家实验室 (筹), 北京 100084

* 通信作者. E-mail: gllong@tsinghua.edu.cn

收稿日期: 2017–09–11; 接受日期: 2017–09–18; 网络出版日期: 2017–10–16
国家重点基础研究发展计划 (973) (批准号: 2011CB9216002)、国家重点研发计划 (批准号: 2017YFA0303700) 和国家自然科学基金 (批准号: 91221205, 11175094) 资助项目

摘要　量子计算机利用量子力学原理进行计算, 具有量子并行计算能力, 有比经典计算机更加强大的数据处理能力. 量子计算机可以指数加速量子体系模拟, 加速一些重要的经典算法. 传统的量子计算运算是通过酉算子对信息进行处理, 其计算过程是对量子计算机体系的初始量子态进行一系列的酉算子的乘积运算. 20 世纪 90 年代中期, 量子算法取得重大突破, 1994 年 Shor 提出了大数分解量子算法, 指数加快了大数分解, 1996 年 Grover 提出了量子搜索算法, 平方根地加速了无序数据库的搜索. 量子算法的重大突破推动量子计算成为国际的持续研究热点领域. 之后量子算法的后续发展缓慢, Shor 在 2003 年提出了著名的 Shor 之问, 询问为什么没有发现更多的量子算法. 2009 年以后, 多个重要的新量子算法被发现, 如求解线性方程组的量子算法, 稀疏 Hamiltonian 体系的酉算符线性叠加算法, 取得计算精度的指数改进的量子系统的新模拟算法. 本文首先简单介绍量子算法的基本原理, 然后描写 Shor 算法和 Grover/Long 搜索算法. 这些算法都是传统的量子算法, 计算的过程就是一系列酉算子的乘积. 接着介绍了 2002 年提出的对偶量子计算, 不同于传统的酉量子算法, 对偶量子算法允许酉算子的线性组合. 过去的量子计算只能使用酉算子的乘和除, 而对偶量子计算可以使用酉算子的加减乘除四则运算. 对偶量子计算为构造量子算法提供了方便, 可以将经典算法中的技巧直接用于量子算法的构造. 我们最近的研究证明 2009 年以来的几个新量子算法都属于对偶量子计算. 本文还介绍开放量子系统的对偶量子模拟算法, 该算法不仅降低了计算复杂度, 而且指数提高了精度. 最后我们给出总结和展望.

关键词　量子计算, 量子算法, 龙算法, 对偶量子计算

1　引言

量子计算是国际上的热点研究领域, 是结合了计算机科学、数学、物理学和工程技术等诸多学科的交叉学科, 具有重要的科学意义和战略意义. 量子计算利用量子纠缠、量子干涉等独特的量子力学

引用格式: 魏世杰, 王涛, 阮东, 等. 量子算法的一些进展. 中国科学: 信息科学, 2017, 47: 1277–1299, doi: 10.1360/N112017-00178
Wei S-J, Wang T, Ruan D, et al. Quantum Computing (in Chinese). Sci Sin Inform, 2017, 47: 1277–1299, doi: 10.1360/N112017-00178

© 2017《中国科学》杂志社

原理进行计算. 它的主要的研究目标是打破传统的硅芯片电子计算机不可避免的发展极限, 利用量子态的相干叠加特性, 产生超越经典计算机的数据处理能力.

量子计算的物理实体是量子计算机. 1980 年 Benioff [1] 和 Manin [2] 等先后提出了量子计算的概念, 1982 年费曼设想利用量子计算机进行高效的量子模拟 [3], Deutsch 于 1985 年完善了量子计算机的概念, 并提出了量子平行计算的概念 [4]. 然而 1985~1994 的十年里, 量子计算没有引起世界上的重视. 直到 1994~1996 年, 量子算法取得突破. 最著名的两个量子算法, Shor 质因数分解算法和 Grover 搜索算法相继被提出 [5,6], 显示了量子计算的强大功能, 大大推动了量子计算的研究, 使得量子计算成为国际上的持续研究热点. Shor 算法对经典公开密码系统形成严重的威胁, Grover 算法加速了对称密码的求解, 量子算法还可能在大数据领域起到重要作用 [7]. 但在此后的十多年里, 量子算法的进展缓慢, 以至于有了著名的 Shor 之问 [8]. 在这段时间里, 一个值得注意的发展是对偶量子计算的提出 [9] 和发展 [10~27], 这种新的量子计算模式采用了酉算符的线性组合进行信息处理. 虽然其数学结构和理论已经建立并发展成熟, 但该算法模式的应用却没有重大进展. 2009 年开始, 求解线性方程组的量子算法 [28,29], 封闭量子体系的新量子模拟算法 [30~32], 开放量子系统的对偶量子算法 [33] 陆续被发现, 量子算法又开始了一个新的发展阶段. 而这些新量子算法就是利用了非酉演化的, 即采用了酉算子的线性组合的对偶量子算法 [29,32,33].

量子计算机的硬件研制已经成为世界主要国家和著名大公司的重点研究方向. 在 2000 年, Divincenzo 通过研究和总结提出了著名的量子计算机物理体系的 5 个标准, 即一个量子计算机的候选物理体系必须符合以下 5 个标准: (1) 具有很好定义且可扩展的量子比特; (2) 量子比特可初始化; (3) 可保持长时间的量子相干特性; (4) 可执行通用量子门操作; (5) 可对量子态进行测量. 尽管建造量子计算机是十分困难的, 但是已经没有了研制量子计算机的理论上的障碍. 世界上的大公司诸如谷歌、IBM、微软等都对量子计算机进行了巨大的投入并取得显著进展. 根据乐观的估计, 实用化的量子计算机可在 2025~2035 年的 10~20 之间研制成功[1)]. 在最近的 1~2 年里, 可以在一些特定问题中超越现在最强大的经典计算机的量子计算机雏形机就有可能诞生, 运行在其上的量子算法的研究和发展变得越来越迫切和重要.

2 量子计算的基本原理

经典信息中, 一个比特的状态只能是确定的 0 或者 1, 而量子比特可以是两个线性无关的态所构成的二维 Hilbert 空间的任意一个态:

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

其中 α 和 β 满足归一化条件 $|\alpha|^2 + |\beta|^2 = 1$. 对于一个 n 量子比特组成的量子体系, 其量子态一般可以写成

$$|\psi\rangle = \sum_{i_1 \ldots i_n = 0 \ldots 0 = 0}^{1 \ldots 1 = 2^n - 1} C_{i_1 \ldots i_n} |i_1 \ldots i_n\rangle. \tag{2}$$

量子比特的上述特性体现了量子力学基本假设的态叠加原理, 而这正是量子并行性的根源, 提供了同时处理多种任务的可能性, 使量子算法比经典算法高效. 当有 n 个量子比特的时候, 量子并行计算可

1) http://www.baselinemag.com/innovation/why-should-business-care-about-quantum-computing.html.

表述的态为 2^n, 相对于经典的 n 个比特是指数级的提升. 比如一个 n 量子比特的量子计算机, 具有巨大的平行计算功能. 在处理某些问题中, 相当于 2^n 个 n 比特的经典计算机同时工作. 在量子计算中, 通常有多个量子存储器, 我们取两个存储器来说明量子并行计算, 其中第 1 个 n 量子比特组成的存储器表示自变量, 而第 2 个存储器用于存储函数值, 函数 f 对应于一个量子酉操作 U_f. 对于初始态,

$$|\Psi\rangle = \sum_{i_1...i_n=0...0=0}^{1...1=2^n-1} C_{i_1...i_n}|i_1...i_n\rangle|0\rangle, \tag{3}$$

在量子计算机上只需要对这个态做一次操作就能同时将所有的自变量所对应的函数值 $f(x)$ 计算出来并存储在 m 个量子比特的第 2 个量子存储器中, 即

$$U_f|\Psi\rangle = \sum_{i_1...i_n=0...0=0}^{1...1=2^n-1} C_{i_1...i_n}|i_1...i_n\rangle|f(i_1...i_n)\rangle. \tag{4}$$

而同样的工作在经典计算机上需要进行 2^n 次操作, 并且使用 $2^n(n+m)$ 个量子比特资源, m 是用于存储函数值的第 2 个存储器的比特数目. 不仅操作次数是量子计算的指数倍, 而且所需资源也是量子计算的指数倍.

在量子计算和量子信息研究中, 还有一个重要的概念是量子纠缠. 考虑一个包含了多个量子比特组成的符合量子系统, 如果它的量子态可以分解为子系统状态的直积, 则该复合系统为可分离态. 如果它的量子态不能表示为子系统状态的直积, 那么子系统之间存在纠缠, 该复合系统称为纠缠态. 量子纠缠是完全区别于经典物理的具有奇妙特性的新的状态, 它在量子计算和量子通信中占有重要地位, 是量子信息的重要资源. 最广为人知的量子纠缠态就是 Bell 态, 以下是其 4 种不同形式:

$$\begin{aligned}
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}|0_A0_B\rangle + |1_A1_B\rangle, \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}|0_A0_B\rangle - |1_A1_B\rangle, \\
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}|0_A1_B\rangle + |1_A0_B\rangle, \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}|0_A1_B\rangle - |1_A0_B\rangle.
\end{aligned} \tag{5}$$

这里的 A 和 B 表示两个粒子, $|0\rangle$ 和 $|1\rangle$ 分别表示自旋向上和自旋向下, 是 Pauli 矩阵 σ_z 的本征态. 当我们对 A 粒子进行测量时, 体系的状态发生突变, B 粒子的自旋状态会随之确定.

通用量子算法是由一系列的酉算子的顺序乘积完成的, 量子计算操作也叫作量子计算门操作、量子门、量子逻辑门等. 而任意的酉算子都可以通过一些简单的基本量子逻辑门的组合来实现 [34], 其解析公式可见文献 [35]. 以下是几个基本的单量子比特门:

$$\begin{aligned}
I &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \\
\sigma_x &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix},
\end{aligned}$$

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},\ T=\begin{pmatrix}1 & 0\\ 0 & e^{\frac{\mathrm{i}\pi}{4}}\end{pmatrix}. \tag{6}$$

能够实现不同比特相互作用的基本量子门称为量子受控非门 (CNOT 门), 也叫做与或门, 其矩阵表示为

$$\mathrm{CNOT}=\begin{pmatrix}1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0\end{pmatrix}. \tag{7}$$

量子算法通过一系列量子逻辑门的顺序乘积来实现, 从量子态的初始化 (数据输入) 开始到量子测量 (即数据输出) 结束. 以这种酉算子乘积实现的量子算法中最著名的有 3 个, 即量子模拟、量子搜索算法和傅立叶变换. 量子搜索算法和傅立叶变换两个算法是构造其他量子算法的基石 [36]. 而量子体系模拟算法是用来模拟量子体系动力学演化过程的算法, 分为相似量子模拟和数字量子模拟两类. 量子模拟的想法来源于费曼 1982 年提出来的利用量子计算机模拟一个量子系统 [3]. 在 Lloyd [37] 具体给出利用通用量子计算机实现量子模拟器的普适方法后, 量子模拟取得了快速的发展, 吸引了越来越多研究者的关注.

3 Shor 大数分解算法

虽然 20 世纪 80 年代初期人们就提出了量子计算的概念, 然而量子计算的强大计算功能直到 1994 年随着 Shor 大数质因子分解的量子算法提出, 人们才重视到了量子计算的巨大潜能. 它能够解决一些在经典计算方法上具有指数复杂度的和有效时间内不可快速解决的问题. 从实用性上来看, Shor 大数质因子分解的算法意义重大, 它使得目前广泛使用的公钥加密体系变得不再安全.

大数质因子分解是指给定一个能因数分解的整数 N, 寻找其质因子的过程. Shor 算法大致分为两个过程, 首先可以将质因子分解过程简化成周期寻找问题. 然后, 对量子态做量子傅里叶变换来完成周期的寻找. 周期寻找问题是, 对于没有共同的质因子两个正整数 x 和 N, $x<N$, 寻找满足 $x^r=1(\mathrm{mod}\,N)$ 的最小正整数 r. 在经典算法里, 周期寻找被认为是一个没法在多项式复杂度 $O(L)$, $L=[\log(N)]$ 内有效解决的问题, 而借助量子傅里叶变换能够在 $O(L^3)$ 步骤内快速解决.

Shor 大数质因子分解算法的核心是对一个大数 N 求解它的一个函数的周期 [5,36]. 随机选择 1 个整数 $x<N$, 与 N 互质. Shor 算法就是来计算 $x^z \bmod N$ 的周期 r. 具体步骤是:

(a) 首先系统需要两个寄存器, 第 1 个寄存器要 t 个量子比特, 初始化为 $|0\rangle$ 态. 第 2 个寄存器要 L 个量子比特, 均初始化为 $|1\rangle$ 态.

(b) 用连续的多种受控旋转门, 构造一个受控的 U^{2^j} 算符, 使得满足变换 $|z\rangle|y\rangle\to|z\rangle|x^z y(\mathrm{mod}\,N)\rangle$. 容易验证其本征态是 $|u_s\rangle=\frac{1}{\sqrt{r}}\sum_{j=0}^{r-1}\mathrm{e}^{-2\pi\mathrm{i}sj/r}|x^j \mathrm{mod}\,N\rangle$, 因而有 $U|u_s\rangle=\frac{1}{\sqrt{r}}\sum_{j=0}^{r-1}\mathrm{e}^{-2\pi\mathrm{i}sj/r}|x^{j+1}\bmod N\rangle=\mathrm{e}^{2\pi\mathrm{i}s/r}|u_s\rangle$.

(c) 用 Hadmard 门 $H^{\otimes t}$ 作用在第一个寄存器的初始 $|0\rangle$ 态上, 得到叠加态 $\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|1\rangle$.

(d) 在第 2 个寄存器进行操作 U^{2^j}, 得到

$$\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|x^j \mathrm{mod}\,N\rangle\approx\frac{1}{\sqrt{r2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1}\mathrm{e}^{2\pi\mathrm{i}sj/r}|j\rangle|u_s\rangle. \tag{8}$$

(e) 对第 1 个量子寄存器做量子反傅里叶变换, 得到 $\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|s/r\rangle|u_s\rangle$.

(f) 测量第 1 个量子寄存器, 得到 s/r, 使用连续分式分解算法得到 r.

(g) 如果 r 是奇数, 则重新开始.

(h) 如果 $x^{r/2}=-1(\mathrm{mod}\,N)$, 则重新开始.

得到了 r 之后, $\gcd(x^{r/2}+1,N)$ 和 $\gcd(x^{r/2}-1,N)$ 中的一个是要求的质因子. 这一过程可以在经典计算机上以多项式的步骤完成.

4 Grover 量子搜索算法

1996 年, 针对无序数据库搜索问题, Grover 提出时间复杂度为 $O(\sqrt{N})$ 的量子搜索算法 [6]. 假定有一个数据规模为 N 的无序数据库, 我们需要从其中搜索一个特定的数据. 对于经典计算机, 通常采用在数据库依次寻找, 直到找到目标数据. 这种遍历法平均需要 $N/2$ 次搜索, 时间复杂度为 $O(N)$. 量子搜索算法通过一系列量子门操作, 将特定数据的几率逐步放大, 直到目标信息的几率几近为 1, 然后对量子数据库进行测量, 得到数据. 询问次数的复杂度为 $O(\sqrt{N})$, 平方根量级地加快了无序数据库的搜索速度.

考虑包含 n 个量子比特的无序数据库, 共有 $N=2^n$ 个量子态 $|i\rangle(i=1,2,\ldots,\tau,\ldots,N)$, 其中的 $|\tau\rangle$ 是目标态, 满足查询函数 $Q(\tau)=1$ ($Q(i)=0, i\neq\tau$). 量子搜索算法的目的就是以尽可能大的概率搜索得到目标态 τ. Grover 搜索算法的过程可以归纳为以下步骤:

首先, 进行数据初始化. 通过 Hadamard 操作 $H^{\otimes n}$ 作用在处于 $|0\rangle$ 态的 n 个量子比特的寄存器上, 就可以得到满足数据库要求的均匀线性叠加量子态:

$$|\psi_0\rangle=H^{\otimes n}|0\rangle=\sqrt{\frac{1}{N}}\sum_i|i\rangle=\cos\beta|c\rangle+\sin\beta|\tau\rangle, \tag{9}$$

其中

$$|c\rangle=\sqrt{\frac{1}{N-1}}\sum_{i\neq\tau}|i\rangle,\ \beta=\arcsin(\sqrt{\frac{1}{N}}). \tag{10}$$

然后, 我们进行 Grover 量子算法的搜索迭代. 其迭代过程包括 4 个步骤.

(1) 保持其他态不变, 反转目标态 $|\tau\rangle$ 的相位, 相应的操作可以表示为 $I_\tau=I-2|\tau\rangle\langle\tau|$, 其中目标态 $|\tau\rangle$ 的相位反转是通过查询函数 $Q(\tau)=1$ 完成的;

(2) 对 n 比特系统作用 $H^{\otimes n}$ 变换;

(3) 其他基矢态的相位不变, 反转 $|0\rangle$ 态, 可表述为 $I_0=I-2|0\rangle\langle 0|$;

(4) 再次进行 n 比特系统的 $H^{\otimes n}$ 变换.

Grover 迭代过程可以用一个整体的 G 操作实现:

$$G=WI_0WI_\tau=(2|\psi\rangle\langle\psi|-I)(I-2|\tau\rangle\langle\tau|). \tag{11}$$

上述操作在几何化的角度来看, 相当于在以 $|\tau\rangle$ 和 $|c\rangle$ 张开的二维 Hilbert 空间中的如下操作:

$$G=\begin{bmatrix}\cos 2\beta & \sin 2\beta\\ -\sin 2\beta & \cos\beta\end{bmatrix}. \tag{12}$$

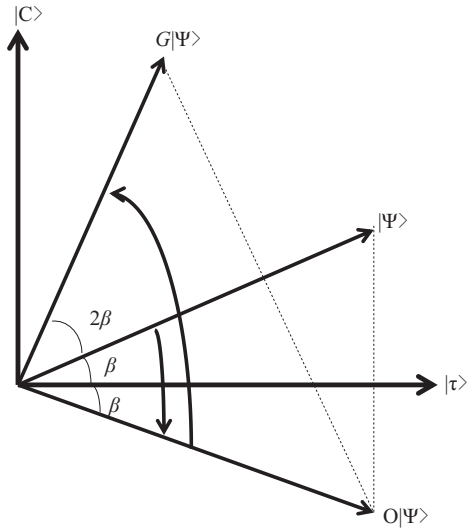

图 1　Grover 搜索算法的几何示意图, 修改自参文 [36]
Figure 1　Geometrical illustration of Grover algorithm, modified from [36]

由此可以清晰地看出 Grover 搜索迭代的几何图像, 即每次 Grover 迭代可以看作是在二维 Hilbert 空间沿逆时针方向旋转 2β. 整个过程如图 1 所示 [36]. 在连续 k 次迭代后, 数据库的量子态演化为

$$|\psi_k\rangle = \cos[(2k+1)\beta]|c\rangle + \sin[(2k+1)\beta]|\tau\rangle. \tag{13}$$

当我们进行 $O(\sqrt{N})$ 次 Grover 迭代后, 测量那时量子系统的状态便以几乎 100% 的几率得到目标量子态 $|\tau\rangle$.

由于对于搜索问题的数据库不一定满足 $\sin[(2k+1)\beta] = 1$, 所以 Grover 算法的搜索成功概率不一定是 100%, 而是一个以迭代步数为周期的函数, 只有在一个有四个数据的数据库中找一个标记态 (四中找一) 时成功率才是 100%. 这导致 Grover 算法在小数据样本和在大数据库时满足搜索条件的数据较多时 (目标态数量较大), Grover 搜索的成功率变低. 这就限制了 Grover 算法的应用. 如在对结构性数据进行搜索时, 如一个字符串, 对每一个字符进行搜索, 而对整个字符串进行搜索的成功率则是每一个搜索成功率的乘积, 这样就会导致成功率迅速下降, 限制了字符串长度 [38].

5　量子搜索算法的相位匹配

在 Grover 量子算法的 4 个步骤中, 有两个相位取反, 即对标记态的系数取反和对 $|0\rangle$ 态的系数取反. Grover 认为任意的相位转动都可以用来进行量子搜索, 但是相位取反, 即 180° 的相位转动是最优的, 其他角度的相位转动都需要使用更多的搜索步骤 [39]. 1999 年, 龙桂鲁课题组首先发现任意相位转动不能构造量子搜索算法 [40], 并提出了量子搜索算法的相位匹配理论 [41, 42], 利用相位匹配理论构造了一个成功率总是 100% 的量子精确搜索算法 [43]. 量子搜索相位匹配和量子精确搜索算法详见文献 [44]. 对于如果将 Grover 算法中的两个相位取反换成一般角度的相位转动, 其量子搜索操作为

$$G = -UR_0U^{-1}R_\tau,$$
$$R_0 = I + (\mathrm{e}^{\mathrm{i}\theta} - 1)|0\rangle\langle 0|,$$

$$R_\tau = I + (\mathrm{e}^{\mathrm{i}\phi} - 1)\sum_k |\tau_k\rangle\langle\tau_k|, \tag{14}$$

其中 θ 和 ϕ 是两个相位转角. 两个相位的匹配条件依赖于数据库的具体形式和搜索算法中酉矩阵的形式. 对于均匀线性叠加态类型数据库和 Hadmard 酉变换, 相位匹配条件为 $\theta = \phi$.

而对于一般类型的数据库:

$$|\psi_0\rangle = \sin\theta_0|\tau\rangle + \cos\theta_0\mathrm{e}^{\mathrm{i}\delta}|c\rangle, \tag{15}$$

其相位匹配条件在 2002 年由龙桂鲁等 [42] 给出:

$$\begin{aligned}&\tan\frac{\theta}{2}\left[\cos 2\beta + \tan\theta_0\cos\delta\sin 2\beta\right]\\ =\ &\tan\frac{\phi}{2}\left[1 - \tan\theta_0\sin\delta\sin 2\beta\tan\frac{\theta}{2}\right],\end{aligned} \tag{16}$$

其中 $\sin\beta = \langle\tau|U|0\rangle$ 是酉算符的矩阵元. 相位匹配条件是量子搜索算法成功的必要条件. 相位匹配后来成为应用量子搜索算法的主要途径, 我们在第 7 节中给出一些例子.

随后 Hoyer [45] 和著名的密码分析专家、差分分析方法发明人 Biham 从不同角度, 用不同的方法进一步肯定了龙桂鲁的相位匹配条件 [46].

6 优化量子精确搜索算法 —— 龙算法

Grover 算法只有在四中找一, 或者是大数据库中 1/4 的数据是满足搜索条件时, 其成功率才是 1, 其他情况下它总有一定的失败概率, 这已经得到严格的数学证明 [47]. 利用相位匹配条件, 找到适当的相位, 能够改进的 Grover 搜索算法的成功率, 以百分百的得到目标态. 2001 年, 龙桂鲁给出了一个量子精确算法 [43]. Toyama 等称这一算法为龙算法 (Long's Algorithm), 证明这一算法是最简单的、优化的量子精确搜索算法 [48]. Castagnoli 强调 1997 年 Bennett 等只在数量级上证明了 Grover 算法是优化的, 而 Toyama 等则在 16 年之后证明了 Grover/Long 算法是精确优化的, 他将龙算法称为 Grover/Long 算法 [49].

龙算法的要点如下. 对于一个有 M 个标记态的规模为 N 的数据库搜索, 将原来 Grover 搜索算法两个 180° 相位反转改为一下角度:

$$\theta = \phi = 2\arcsin\left(\sin\beta\sin\left(\frac{\pi}{4J_S + 6}\right)\right), \tag{17}$$

其中 J_S, β 满足

$$\begin{aligned}J_S \geqslant J_{op} &= \left|\frac{(\frac{\pi}{2}) - \beta}{2\beta}\right|,\\ \beta &= \arcsin(\sqrt{\frac{M}{N}}),\end{aligned} \tag{18}$$

$|.|$ 表示最近的整数, J_S 可以是比最小搜索次数 J_{op} 大的任意整数. 经过 J_S 次搜索迭代后, 数据库的量子态变为

$$|\psi_0\rangle \to \mathrm{e}^{\mathrm{i}[\frac{\pi-\phi}{2}] + J_S(\pi+\phi)}|\tau\rangle. \tag{19}$$

此时测量, 我们以 100% 的成功率搜索得到目标态.

7 相位匹配和量子精确搜索算法的应用

量子计算创始人 Benioff 很早就关注了相位匹配，在美国数学学会大会报告中引用，称其为量子搜索算法的深入发展 [50]. Hoyer [45] 和密码分析专家 Biham 等 [46] 研究进一步肯定了相位匹配. 荷兰实验组利用光学系统验证了相位匹配 [51]. 相位匹配成为量子计算实验的重点环节, 如液晶全光系统中通过调制器来实现 [52], 离子阱系统采用公式 (17) 实现相位匹配 [53].

在量子搜索算法中, 由于任何一个态都可能是标记态, 如果采用其他不同于 Hadamard 的酉矩阵, 则就会造成不同的标记态的搜索步数不同, 难于操作. 因此, 在后来许多的量子应用中, 都采用了利用相位匹配, 通过改变相位来实现应用.

英国皇家工程院院士 Hanzo 称相位匹配为量子搜索的 “重要贡献”, 并利用相位匹配构造了无线用户的量子探测算法 [54]. 麻省理工 Chuang 应用了相位匹配构造定点量子搜索算法 [55].

Grover 指出他的算法有一定失败概率的缺陷, 并指出龙算法等 4 个算法解决了这一缺陷 [56]. Imre 教授将龙算法收入到其专著中 [57]. 澳大利亚 Ian Peterson 院士将龙算法用于构造量子滑模控制 [58]. 龙算法被用于量子模式识别以提高识别效率 [59]. 在结构搜索问题中, 加州大学圣迭戈分校的 Meyer 教授指出必须用精确搜索算法才能消除搜索字长的限制 [38]. 在量子图像压缩中, 龙算法更适用于这类小样本数据库情况 [60].

8 Shor 之问 —— 量子算法的困境与新量子算法

在大数分解算法和量子搜索算法提出之后, 量子算法的研究非常缓慢. 2003 年大数分解量子算法的提出者, Shor 发出著名的 Shor 之问, 为什么没有更多的量子算法被找到 [8]. 对此他解释为量子计算机的运行与经典计算的运行如此不同, 以至于经典算法中的构造设计技巧和直觉在量子计算过程中不再成立.

回看量子算法, 包括大数分解算法和 Grover 搜索算法在内的量子算法都是通过系统的酉演化对信息进行处理, 酉算符的逆也是酉算符, 因此在量子算法中只有酉算子的乘和除运算. 经典算法里, 加减乘除等所有的基本运算都可以使用. 相比较而言, 量子算法中只使用乘除运算而不能使用加减运算. 因为酉算子在加和减运算下不再封闭, 即酉算符的加和减一般情况下不再是酉算符了. 这种差别使得经典算法中的许多技巧不能在量子算法中使用, 影响了量子算法的发展.

而利用酉算符的线性组合来进行量子计算的对偶量子计算在 2002 年提出 [9], 并且得到了系统深入的发展 [10~27,61]. 这种新的量子计算模式采用了辅助比特, 在量子计算体系和辅助比特的整体系统, 演化是酉的, 但是在量子计算的子空间中, 演化不再是酉的, 这样就能实现所需要的非酉操作. 对偶量子计算的数学理论在 Gudder、杜鸿科、曹怀信以及龙桂鲁等的努力下, 已经建立并日渐成熟. 但对偶量子算法模式的应用却没有重大进展.

2009 年开始, 量子算法取得了重要的进展. 求解线性方程组的量子算法可以指数加快方程组的解法 [28,29], 封闭量子体系的新量子模拟算法 [30~32] 改善了量子模拟的精度, 开放量子系统的对偶量子模拟算法 [33] 不仅加快了计算速度, 而且提高了计算精度, 量子算法又开始了新的发展阶段. 而这些新量子算法就是利用了非酉演化, 即采用了酉算子的线性组合的对偶量子算法 [29,32,33].

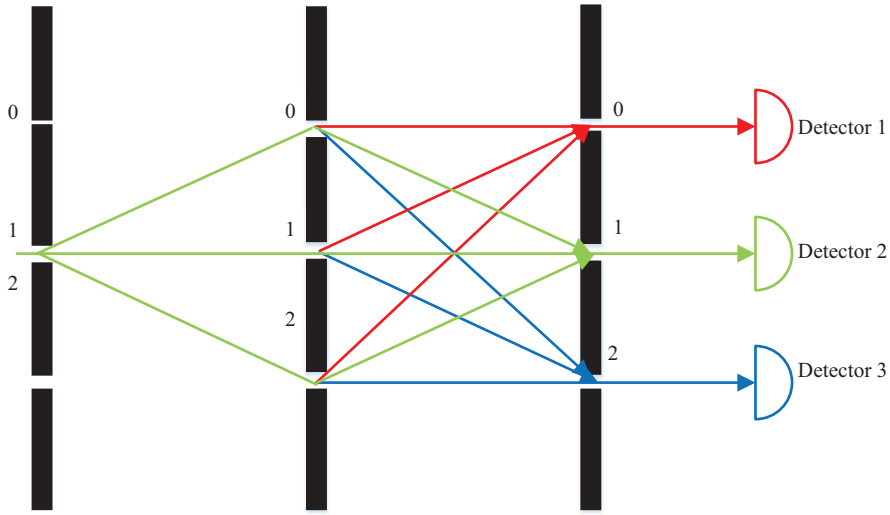

图 2 (网络版彩图) 三狭缝的对偶量子计算机演示图. 从标记为 1 的第 2 个狭缝输入, 和由中间屏幕的 3 个狭缝分为 3 个子波. 中间屏幕后, 在不同的狭缝对子波进行不同的操作. 对偶量子计算的输出从右边屏幕上的 3 个狭缝处获得, 不同的狭缝处的输出对应不同的量子计算结果

Figure 2 (Color online) An illustration for a three-slits duality quantum computer. The input is entered from the second slits marked as 1, and the input is divided into three sub waves by three slits of the middle screen. After the middle screen, the sub waves are performed individual operations in different slits. The output of the duality quantum computation is obtained from three slits on the right screen, and the outputs at different slits correspond to different quantum calculating results

9 对偶量子计算原理

龙桂鲁于 2002 年提出的对偶量子算法 [9, 14] 不同于传统的幺正演化的计算模式, 可以使用酉算符线性叠加的形式进行信息的处理, 从而一定的概率实现非酉演化, 扩展了构造量子算法的方式方法. 对偶量子计算是利用量子力学的波粒二象性, 通过对不同狭缝的波函数进行平行操作实现非幺正演化处理. 在对偶计算机中, 计算机的波函数被分成若干个子波并使其通过不同的路径, 在不同路径上进行不同的量子计算门操作, 而后这些子波重新合并产生干涉, 给出计算结果. 对偶量子计算可以通过广义量子门实现任意酉算符的线性组合. 事实上 Gudder 定理证明, 所有的线性有界算符都可以由广义量子门实现, 酉算符只是广义量子门集的极值点 [12]. 形象地说, 对偶计算机是一台通过 d 个狭缝的运动着量子计算机, 在不同的狭缝进行不同的量子操作, 最后通过在不同狭缝上的探测测量得到运算结果. 整个运算过程如图 2 所示. 目前的对偶量子计算已建立起严格数学理论, 引起了很多人的研究兴趣 [10∼13, 15∼26].

对偶量子计算机有两种新的操作, 即量子分波 (QWD) 操作和量子合波 (QWC) 操作. 分波操作将波函数分为许多振幅减小的相同的部分波函数, 数学上就是进行 Hilbert 空间的扩展. 这个操作的物理图是简单而自然的: 量子系统通过 d 个狭缝其波函数被分为 d 个子波, 各子波具有相同的波函数, 不同之处在于质心运动的位置. 相反, 合波操作把所有的子波叠加成一个波函数. 应该注意的是将同一量子系统的波函数分为多个子波并不违反量子不可克隆定理. 然而在现实之中移动的量子计算机设备难以实现. 幸运的是, 已经证明由 n 比特的普通量子计算机与 d 能级的辅助系统可以完美地模拟通过 d 狭缝的 n 比特的移动量子计算机 [10, 14]. 这也意味着我们可以在普通的量子计算机中进行对偶量子计算. 以下的讨论都是在以普通量子计算机和辅助系统组成的对偶量子计算模式下进行的.

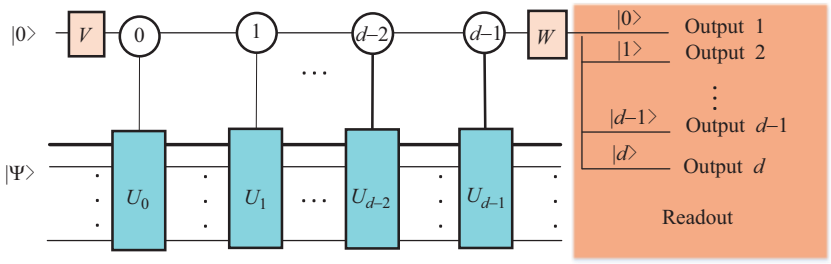

图 3 (网络版彩图) 多输出的对偶量子计算线路图. $|\Psi\rangle$ 是工作比特初态, $|0\rangle$ 是辅助比特初态

Figure 3 (Color online) The multi-output duality quantum computing circuit. $|\Psi\rangle$ denotes the initial state of work qubit, and $|0\rangle$ is the initial state of the controlling auxiliary qudit

n 比特的普通量子计算机可以由 n 个工作比特表示, 辅助系统可以由 d 能级的辅助比特表示. 分波操作对应幺正算符 V, 合波操作对应幺正算符 W. 以上两种操作作用在辅助系统上, 而辅助系统控制的受控操作作用在 n 个工作比特上. 整个对偶计算的线路图如图 3 所示.

为了更加清晰的阐述对偶量子计算, 以下将整个过程分为 4 个步骤. 考虑一个由工作系统 $|\Psi\rangle$ 和辅助系统 $|0\rangle$ 构成的对偶量子计算系统.

步骤 1: 首先, 将量子系统初始化为 $|\Psi\rangle|0\rangle$. 作用分波算符 V 在辅助系统 $|0\rangle$ 上, 此时系统由初态变为

$$\begin{aligned}|\Psi\rangle|0\rangle \rightarrow\ & |\Psi\rangle V|0\rangle \\ =\ & |\Psi\rangle \mathrm{I} V|0\rangle = |\Psi\rangle \left(\sum_{i=0}^{d-1}|i\rangle\langle i|\right) V|0\rangle \\ =\ & |\Psi\rangle \sum_{i=0}^{d-1}|i\rangle\langle i|V|0\rangle \\ =\ & \sum_{i=0}^{d-1} V_{i0}|\Psi\rangle|i\rangle, \end{aligned} \tag{20}$$

其中 $V_{i0}=p_i$ 是复数, 满足归一化条件 $\sum_{i=0}^{d-1}|V_{i0}|^2=1$, $|V_{i0}|\leqslant 1$. V_{i0} 是幺正矩阵 V 的第 1 列元素, 代表分波结构. 以上推导中用到了完备条件 $\sum|i\rangle\langle i|=\mathrm{I}$. $|\Psi\rangle|i\rangle$ 代表第 i 个狭缝处的末态.

步骤 2: 在初态为 $|\Psi\rangle$ 的工作比特上进行辅助系统控制的 $U_0, U_1, \ldots, U_{d-1}$ 幺正操作. 这个步骤将系统的量子态演化为

$$\sum_{i=0}^{d-1} V_{i0}U_i|\Psi\rangle|i\rangle. \tag{21}$$

对应的物理图像是同时在不同的狭缝上进行不同的幺正操作.

步骤 3: 作用合波算符 W 在辅助系统 $|i\rangle$ 上, 得到如下的量子态:

$$\begin{aligned}\sum_i V_{i0}U_i|\Psi\rangle W|i\rangle\ =\ & \sum_i V_{i0}U_i|\Psi\rangle \mathrm{I} W|i\rangle \\ =\ & \sum_i V_{i0}U_i|\Psi\rangle \sum_{k=0}^{d-1}|k\rangle\langle k|W|i\rangle\end{aligned}$$

$$= \sum_i \sum_k W_{ki} V_{i0} U_i |\Psi\rangle |k\rangle$$
$$= \sum_k L_k |\Psi\rangle |k\rangle, \tag{22}$$

其中 $L_k = \sum_i W_{ki} V_{i0} U_i$ 就是对偶量子门. 通常情况下对于闭合系统的动力学演化 [9, 14], 只需要用到 L_0 这一个量子门. 当讨论开放量子体系时, 需要考虑 k 个对偶量子门.

步骤 4: 在步骤 3 后, 辅助比特处于叠加态. 在经过测量后, 不同的辅助比特的状态对应不同的系统输出态. 对于辅助比特处于不同的 $|j\rangle$ 态, 工作比特对应 j 个末态.

对偶量子计算门定义如下:

$$L_c = \sum_{i=0}^{d-1} c_i U_i, \tag{23}$$

其中 U_i 是幺正的, c_i 是复数系数并满足

$$\sum_{i=0}^{d-1} |c_i| \leqslant 1. \tag{24}$$

当 c_i 被限定为实数时, c_i 记做 r_i, 满足限制条件 $\sum_i r_i \leqslant 1$. 在这种情况下, 对偶量子门被称为实数对偶门, 记做 L_r. L_r 可被表述为

$$L_r = \sum_{i=0}^{d-1} r_i U_i. \tag{25}$$

对应的物理图像是对偶量子系统有 d 个不同的狭缝, r_i 是量子计算机穿过第 i 个狭缝的概率.

因为幺正算符在加减运算下不闭合, 对偶量子门通常是非幺正的. 在有限的 Hilbert 空间下任意线性有界算符都可以表示为对偶量子门 [12]. 更多关于对偶量子计算的数学理论可见 [10,11,13,15∼23,26], 本文不再赘述.

需要指出, 当用到 L_0 这一个量子门进行闭合系统的动力学演化的时候, 算法是一个概率性算法. 算法成功的概率 P_s 对应于辅助系统处于 $|0\rangle$ 态的概率. 计算易得

$$P_s = \langle\Psi| \left(\sum_{i_1} W_{0 i_1} V_{i_1 0} U_{i_1} \right)^\dagger \left(\sum_{i_2} W_{0 i_2} V_{i_2 0} U_{i_2} \right) |\Psi\rangle, \tag{26}$$

其失败的概率

$$P_f = \sum_{j=1}^{d-1} \langle\Psi| \left(\sum_{i_1} W_{j i_1} V_{i_1 j} U_{i_1} \right)^\dagger \left(\sum_{i_2} W_{j i_2} V_{i_2 j} U_{i_2} \right) |\Psi\rangle. \tag{27}$$

在这种具有一定成功率的情况下, 我们可以直接进行测量. 如果测得辅助系统为 $|0\rangle$ 算法成功, 否则失败, 从步骤 1 开始进行下一次运算直到得到 $|0\rangle$ 为止. n 次重复后成功的概率为 $1 - (P_f)^n$, 这个概率在 n 比较大时逐渐趋近于 1.

在测量之前, 我们也可以通过 Grover/Long 搜索算法进行振幅放大, 从而提高算法成功率.

10 稀疏 Hamiltonian 体系的对偶量子模拟

理查德 · 费曼提出量子计算机概念的初衷就是进行量子模拟 [3]. 事实上量子系统模拟的复杂度是随比特数指数增加的, 利用经典计算机进行量子模拟显然不现实, 而量子计算机天然的适合这种计算. 模拟量子系统的动力学演化是量子计算机最主要的应用之一.

相比于经典计算机, 量子计算机可以指数级的加快量子模拟的效率 [3]. Lloyd [37] 在 1996 年给出了通用的基于乘积形式的 Hamiltonian 量模拟算法. 但这种模拟形式在高阶近似时会导致算法复杂度急剧升高. 比如, 采用 Lie-Trotter-Suzuki 公式来近似表示时间演化因子, 其公式内乘积形式的酉算符的数量是随着近似阶数指数级升高 [62]. 相反经典算法利用线性组合可以多项式复杂度就得到相同的精度 [63]. 然而, 由于酉算符在加减运算下不闭合, 这些经典算法不能直接用于量子计算. 这是我们熟知的一个困难, 即在经典计算过程中的直觉和技巧不再适用于量子算法的设计 [8].

对偶量子计算则可以作为将经典算法转化为量子算法的桥梁, 可以实现酉算符的加减乘除四则运算, 从而解决经典算法转化为量子算法的困难. 2012 年, Childs 和 Wiebe [30] 提出了基于酉算符线性组合的 Hamiltonian 量模拟算法. 该算法的结果优于以前所有量子模拟算法. 而这就是一个对偶量子算法, 在文献 [32] 已经详细给出. 我们这里给出其要点.

Childs-Wiebe 算法的主要结果如下:

定理1 系统 Hamiltonian 量 $H=\sum_{j=1}^{m}H_j$, 其中每个 $H_j\in C^{2^n\times 2^n}$ 是厄米的且满足 $\parallel H_j \parallel$ 不大于一个常数 h. 系统 Hamiltonian 量的演化 e^{-iHt} 可以通过幺正算符线性叠加的乘积形式以误差 ϵ 在量子计算机上模拟. 在 $m, ht, 1/\epsilon$ 都比较大的情况下, 这种模拟需要

$$\tilde{O}\left(m^2 ht \mathrm{e}^{1.6\sqrt{\log(mht/\epsilon)}}\right) \tag{28}$$

基本算符和 e^{-iH_jt} 算符. 时间演化因子 $U(t)$ 满足薛定谔方程

$$\mathrm{i}\frac{\mathrm{d}}{\mathrm{d}t}U(t)=HU(t), \tag{29}$$

可以表示为 $U(t)=\mathrm{e}^{-\mathrm{i}Ht}$.

给定 Hamiltonian 量分解为 $H=\sum_{j=1}^{m}H_j$, 将 $U(t)$ 用 Lie–Trotter–Suzuki 公式做近似,

$$\mathrm{e}^{-\mathrm{i}Ht}\approx(\prod_{j=1}^{m}\mathrm{e}^{-\mathrm{i}H_j\frac{t}{r}})^r.$$

时间演化因子可以表示为 S_χ 的 Taylor 展开:

$$\begin{aligned} S_1(t)&=\textstyle\prod_{j=1}^{m}\mathrm{e}^{-\mathrm{i}H_jt/2}\prod_{j=m}^{1}\mathrm{e}^{-\mathrm{i}H_jt/2},\\ S_\chi(t)&=\left(S_{\chi-1}(s_{\chi-1}t)\right)^2 S_{\chi-1}([1-4s_{\chi-1}]t)\left(S_{\chi-1}(s_{\chi-1}t)\right)^2, \end{aligned} \tag{30}$$

其中 $s_{\chi-1}=(4-4^{1/(2\chi-1)})^{-1}, \chi>1$ [30,62]. S_χ 的大小对应的是将 $\mathrm{e}^{-\mathrm{i}Ht}$ 精确到 $O(t^{2\chi+1})$ 量级. 当 χ 足够大且 t 足够小, $U(t)$ 可以近似到任意精度.

该算法最终将 $U(t)$ 表示为 $M_{k,k}(t)$ 形式:

$$M_{k,k}(t)=\sum_{q=1}^{k+1}C_qS_k(t/\ell_q)^{\ell_q}, \tag{31}$$

其中 ℓ_q 代表自然数, $q\in\{1,2,\ldots,k+1\}$, $C_1,\ldots,C_{k+1}\in R$ 满足 $\sum_{q=1}^{k+1}C_q=1$. 在 [30] 中, ℓ_q 和 C_i 定义如下:

$$\ell_q=\begin{cases} llq, & \text{if } q\leqslant k,\\ \mathrm{e}^{\gamma(k+1)}, & \text{if } q=k+1,\end{cases}\tag{32}$$

$$C_q=\begin{cases} \frac{q^2}{q^2-\mathrm{e}^{2\gamma(k+1)}}\prod_{j\neq q}^{k}\frac{q^2}{q^2-j^2}, & \text{if } q\leqslant k,\\ \prod_{j=1}^{k}\frac{\mathrm{e}^{2\gamma(k+1)}}{\mathrm{e}^{2\gamma(k+1)}-j^2}, & \text{if } q=k+1,\end{cases}\tag{33}$$

其中 γ 是用来调节 C_q 的参数. 公式精确到 $O(t^{4k+1})$ 量级, 即

$$M_{k,k}(\lambda)-U(\lambda)\in O(t^{4k+1}).\tag{34}$$

和通常的模拟算法一样将演化时间 t 分割为 r 段. 不同于传统乘积算法的是, 在这个算法里每段的演化因子 $U(t/r)=\mathrm{e}^{iHt/r}$ 近似为如下的求和叠加形式:

$$U(t/r)\approx M_{k,k}(t/r)=\sum_{q=1}^{k+1}C_qS_k(t/\ell_qr)^{\ell_q}.\tag{35}$$

这种基于酉算符线性叠加的模式正好就是对偶量子计算模式的算法. 在文献 [32] 中, 我们给出了 Childs-Wiebe 算法的对偶量子模式的描述, 其要点如下.

由方程 (30) 可知, $S_k(t/\ell_qr)^{\ell_q}$ 是幺正算符. 由方程 (23) 可知时间演化因子就是对偶量子门,

$$M_{k,k}(t/r)=N\sum_{i=1}^{k+1}c_iU_i(t/r)=NL_c(t/r),\tag{36}$$

其中 $N=\sum_{i=1}^{k+1}|C_i|$ 是归一化系数, $U_i(t/r)=S_k(t/\ell_ir)^{\ell_i}$, $c_i=C_i/N$, 广义对偶量子门

$$L_c(t/r)=\sum_i c_iU_i(t/r).\tag{37}$$

接下来给出 $L_c(t/r)$ 的具体形式. 分波算符和合波算符分别由幺正矩阵 V 和 W 表示. 矩阵元素 V_{i0} 和 W_{i0} 通过 c_i' 获得.

重新定义 U_i: 当 c_i' 为负的情况时, 将其负号放入 U_i' 中. 所以 c_i' 都为正实数. 在这种情况下, 可以选择采用 $V=W^\dagger$. 此时, $c_i=W_{0i}V_{i0}=|W_{0i}|^2=|V_{i0}|^2$ 是正实数. 即

$$V_{i,0}=W_{0,i}=\sqrt{c_i}.\tag{38}$$

在进行 QWD 操作后, 相继进行辅助系统控制算符和 QWC 算符操作. 测量辅助系统的状态, 如果结果是 $|0\rangle$, 那么初态的 $|\Psi\rangle|0\rangle$ 被演化为

$$\begin{aligned}\sum_i W_{0i}V_{i0}U_i|\Psi\rangle|0\rangle &= \sum_i(W_{0i}V_{i0})U_i|\Psi\rangle|0\rangle\\ &=\sum_{i=0}^{k}c_iU_i|\Psi\rangle|0\rangle\\ &=\frac{1}{N}(M_{k,k}(t/r))|\Psi\rangle|0\rangle,\end{aligned}\tag{39}$$

正是 Hamiltonian 量模拟的结果.

执行 r 个 $M_{k,k}(t/r)$ 片段演化后, 我们得到了时间演化因子 $U(t)$ 的近似 $M_{k,k}(t/r)^r$. 这是一个不确定的但有高概率成功的算法. 至此, 该 Hamiltonian 量模拟算法就通过对偶量子算法实现了.

11 高精度的对偶量子模拟算法

Berry 等 [31] 提出的基于 Taylor 展开截断项的 Hamiltonian 量模拟算法可以高效模拟一系列的物理系统的动力学演化. 算法的效率相较于过去的利用酉算符乘积的量子模拟算法有指数量级的提高. 该算法利用酉算符的线性组合, 自然也是一个对偶量子算法. 该算法原始表达非常抽象, 这里我们采用文献 [32] 的表述, 利用对偶量子计算的语言描述.

将 Hamiltonian 量分解为酉算符的线性叠加:

$$H=\sum_{\ell=1}^{L}\alpha_\ell H_\ell. \tag{40}$$

然后将有限时间 t 平均分为 r 段, 每段的时间演化因子可以近似为

$$U_r:=\exp(-iHt/r)\approx\sum_{k=0}^{K}\frac{(-iHt/r)^k}{k!}, \tag{41}$$

其中 K 是 Taylor 展开的阶数. 将方程 (40) 代入 (41), Taylor 截断项可被表述为

$$U_r\approx\widetilde{U}=\sum_{k=0}^{K}\sum_{\ell_1,\ldots,\ell_k=1}^{L}\frac{(-it/r)^k}{k!}\alpha_{\ell_1}\cdots\alpha_{\ell_k}H_{\ell_1}\cdots H_{\ell_k}. \tag{42}$$

设定 $\alpha_\ell>0$. 因为 H_ℓ 是幺正的, $\widetilde{U}$ 就是幺正算符的线性叠加, 正好就是对偶量子门的形式. Taylor 截断项的角标定义如下 [31]

$$J:=(k,\ell_1,\ldots,\ell_k):k\leqslant K\ ,\ell_1,\ldots,\ell_k\in\{1,...,L\}. \tag{43}$$

然后 $\widetilde{U}$ 可以简化为

$$\widetilde{U}=\sum_{j\in J}\beta_j V_j, \tag{44}$$

其中 $\beta_{(k,\ell_1,\ldots,\ell_k)}:=[(t/r)^k/k!]\alpha_{\ell_1}\cdots\alpha_{\ell_k}$, $V_{(k,\ell_1,\ldots,\ell_k)}:=(-i)^kH_{\ell_1}\cdots H_{\ell_k}$. 需要注意的是 $\widetilde{U}$ 没有归一化, 不能用对偶量子门直接实现.

标记归一化系数为 $s=\sum_{j\in J}\beta_j$. 由方程 (44) 可知, $L_r=\widetilde{U}/s$ 就是对偶量子门.

图 4 是实现该量子模拟算法的对偶量子线路图. 在图 4 中标记为 B 的受控酉操作 U_0, 对应于 Hamiltonian 量的线性叠加, $H=\sum_{\ell=1}^{L}\alpha_\ell H_\ell$, 图 4 的上半部分是实现 $U_r=\exp(-iHt/r)\approx\sum_{k=0}^{K}(-iHt/r)^k/k!$ 的线路图.

$$|\Psi\rangle|0\rangle\to|\Psi\rangle U_r|0\rangle. \tag{45}$$

$\widetilde{U}$ 操作需要通过作用在 K 个 L 能级的辅助系统 $|0\rangle_L$ 和 K 个辅助比特 $|0\rangle^K$ 的两个 QWD 操作和两个 QWC 操作实现. 方程 (42) 意味着需要做两次求和. 将初态表示为 $|\Psi\rangle|0\rangle^K|0\rangle_L^K$, 其中 $|0\rangle_L^K$ 表示 K 个 L 能级的系统并且都处于 $|0\rangle_L$ 态.

首先, 将 $|0\rangle^K$ 通过 QWD 操作转化为

$$|0\rangle^K\to\sum_{k=0}^{K}\sqrt{\frac{(Nt/r)^k}{k!}}|1^k0^{K-k}\rangle, \tag{46}$$

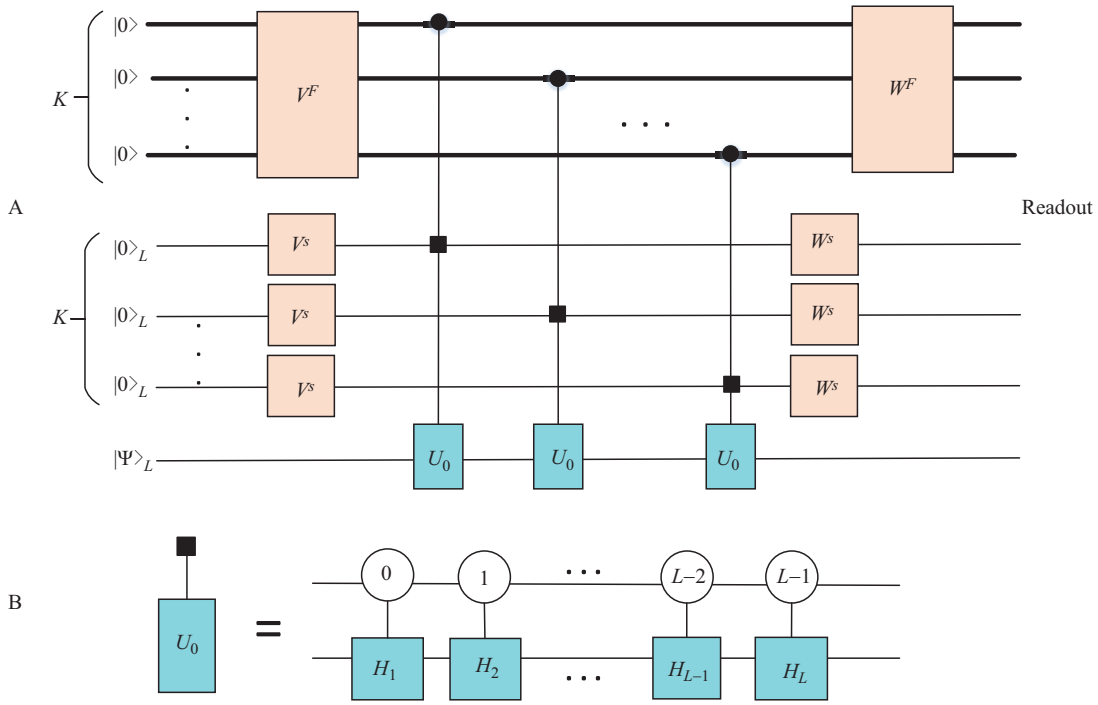

图 4 (网络版彩图)BCCKS 算法的对偶模式量子线路图. A 展示的是整个线路图. 其中 $|\Psi\rangle$ 是工作系统初态. 线路图共包含 K 个 $|0\rangle$ 态的辅助控制比特和 K 个 L 能级的 $|0\rangle_L$ 辅助控制系统. B 展示的是 U_0 由 $H_1, H_2, \ldots, H_{L-1}, H_L$ 组成. 只有当处在圆圈内相应的态的时候辅助系统控制的幺正算符 U_0 才会被激发

Figure 4 (Color online) Quantum circuit for the BCCKS algorithm in duality quantum computing. Part A is the quantum circuit of duality computing. $|\Psi\rangle$ is the initial state of duality quantum computer and there are K auxiliary controlling qubits $|0\rangle$ and K auxiliary controlling qudits $|0\rangle_L$with L energy level system . Part B is to illustrate that each unitary operation U_0 is composed of $H_1, H_2, \ldots, H_{L-1}, H_L$. The unitary operations U_0 are activated only when the L level $|0\rangle_L$ auxiliary controlling qudits hold the values indicated in respective circles

其中 $N = \sum_{l=1}^{L} \alpha_l$. QWD 标记为一个 $2^K \times 2^K$ 的矩阵 V^F. 矩阵元素满足

$$V_{i,0}^F = \frac{v_{i,0}^F}{\sqrt{\sum_i |v_{i,0}^F|^2}}, \tag{47}$$

其中

$$v_{i,0}^F = \begin{cases} \sqrt{\frac{(Nt/r)^k}{k!}}, & i = 2^K - 2^{K-k}, k \in \{0, 1, \ldots, K\}, \\ 0, & \text{others.} \end{cases} \tag{48}$$

再将 V^F 作用在 $|0\rangle^K$ 部分, 得到 $\sum_{k=0}^{K} \sqrt{(Nt/r)^k/(k!)}|1^k 0^{K-k}\rangle$.

其次, 再次使用 QWD 操作将 $|0\rangle_L$ 转化为 $\sum_{\ell=1}^{L} \sqrt{\alpha_\ell}|\ell\rangle$. 将第 2 个 QWD 算符标记为 $L \times L$ 的矩阵 V^S. 矩阵元素满足

$$V_{\ell,0}^S = \frac{v_{\ell,0}^S}{\sqrt{\sum_\ell |v_{\ell,0}^S|^2}}, \tag{49}$$

其中

$$v_{\ell,0}^S = \sqrt{\alpha_\ell}. \tag{50}$$

对应于 K 个辅助比特 $|0\rangle^K$, K 个 L 能级辅助系统 $|0\rangle_L$ 需要通过 V^S 转化为 K 个 $\sum_{\ell=1}^{L}\sqrt{\alpha_\ell}|\ell\rangle$ 态. 可以被标记为:

$$\left(\sum_{\ell=1}^{L}\sqrt{\alpha_\ell}|\ell\rangle\right)^K. \tag{51}$$

在 $|0\rangle_L$ 部分执行第 2 个幺正算符 V^S 后, 我们得到 $\sum_{\ell=1}^{L}\sqrt{\alpha_\ell}|\ell\rangle$. 使用归一化常数 $s=\sum_{j\in J}\beta_j$ 后, 辅助系统的归一化态为

$$|0\rangle^K|0\rangle_L^K \to \frac{1}{\sqrt{s}}\sum_{k=0}^{K}\sqrt{\frac{(Nt/r)^k}{k!}}\left(\sum_{\ell=1}^{L}\sqrt{\alpha_\ell}|\ell\rangle\right)^K|1^k0^{K-k}\rangle. \tag{52}$$

假设 $|0\rangle_L$ 辅助比特处于可激活操作算符 U_j 数目为 k. 那么, 有如下过程:

$$|\Psi\rangle \to \frac{1}{\sqrt{s}}\sum_{k=0}^{K}\sqrt{\frac{(Nt/r)^k}{k!}}\left(\sum_{\ell=1}^{L}\sqrt{\alpha_\ell}\right)^k U_j|\Psi\rangle. \tag{53}$$

然后, 对应于两次 QWD 操作, 需要两次 QWC 操作来完成合波. 我们分别记做 W^F 和 W^S. 对于实系数量子计算, 取 $W^F=(V^F)^\dagger$, $W^S=(V^S)^\dagger$. QWC 算符 W^F 和 W^S 分别作用在 $|1^k0^{K-k}\rangle$ 和 $|\ell\rangle$. 算法的物理图像就是每一次 QWD 和 QWC 操作实现一次幺正算符叠加过程. 对偶量子计算所需要的结果在 L 能级辅助系统处于 $|0\rangle_L$ 态且 K 个辅助比特处于 $|0\rangle^K$ 态的项, 如下所示:

$$\begin{aligned}\sum_{k=0}^{K}\sqrt{(Nt/r)^k/k!}|1^k0^{K-k}\rangle &\longrightarrow \sum_{k=0}^{K}(Nt/r)^k/k!|0\rangle^K,\\ \sum_{\ell=1}^{L}\sqrt{\alpha_\ell}|\ell\rangle &\longrightarrow \sum_{\ell=1}^{L}\alpha_\ell|0\rangle_L.\end{aligned} \tag{54}$$

至此, 系统初态转化为

$$|\Psi\rangle|0\rangle^K|0\rangle_L^K \to \frac{1}{s}\sum_{k=0}^{K}\frac{(t/r)^k}{k!}\left(\sum_{\ell=1}^{L}\alpha_\ell\right)^k U_j|\Psi\rangle|0\rangle^K|0\rangle_L^K, \tag{55}$$

其中 U_j 对应于 $(-i)^kH_{\ell_1}\cdots H_{\ell_k}$ 某些项.

由对应关系

$$\sum_{j\in J}\beta_jV_j=\sum_{k=0}^{K}(t/r)^k/k!(\sum_{\ell=1}^{L}\alpha_\ell)^kU_j,$$

我们成功地实现了如下过程:

$$|\Psi\rangle|0\rangle^K|0\rangle_L^K \to \frac{1}{s}\widetilde{U}|\Psi\rangle|0\rangle^K|0\rangle_L^K. \tag{56}$$

测量之前, 使用具有鲁棒性的振幅放大操作来放大所需项的振幅, 可以接近确定性的实现 $\widetilde{U}$. 近似表示 $\widetilde{U}$ 的精度可以由近似误差 ϵ 表示. 由 Chernoff 界限 [31], 询问复杂度为

$$K=O\left(\frac{\log(r/\epsilon)}{\log\log(r/\epsilon)}\right), \tag{57}$$

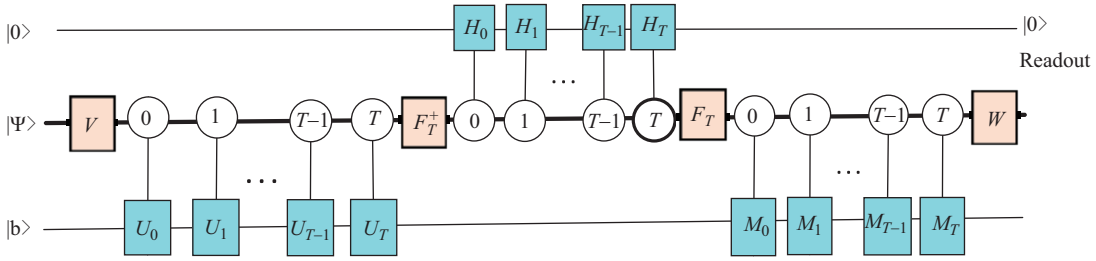

图 5 (网络版彩图)HHL 算法的对偶量子线路图. 我们只需要辅助比特处在 $|0\rangle$ 时系统输出结果

Figure 5 (Color online) The duality quantum computing circuit of HHL algorithm. We only need the output when the ancillary qubit is in state $|0\rangle$

每个片段的近似精度满足

$$\| \widetilde{U} - U_r \| \leqslant \frac{\epsilon}{r}. \tag{58}$$

整个模拟过程的询问复杂度为 r 乘以 K. 一个片段里门的整体复杂度为

$$O\left(\frac{L(n+\log L)\log(T/\epsilon)}{\log\log(T/\epsilon)}\right), \tag{59}$$

其中 $T = (\alpha_1 + \cdots + \alpha_L)t$.

至此, 我们利用对偶量子计算模式给出了实现基于幺正算符线性组合的 Hamiltonian 量模拟算法的标准过程.

12 求解线性方程组对偶量子算法

解线性方程组在经济学、计算机、机器学习和物理领域都扮演着举足轻重的角色. 在 2009 年, Harrow 等人提出了解线性方程组的量子算法 (HHL 算法) [28], 在一定的限制条件下比经典的解方程组算法有指数级加速. 最近的研究表明, 这个量子算法就是对偶量子算法, 它使用了酉算子的线性组合 [29].

考虑一个线性方程组 $A|x\rangle = |b\rangle$, 其中 A 是一个 $N \times N$ 的系数矩阵. HHL 算法在量子计算机上经过 $O(\log N)$ 数量的算符操作就能求解出 $|x\rangle$, 而对应的经典算法需要 $O(N)$ 步操作. 当我们只关心代表观测者的厄米算符 M 的平均值 $\langle x|M|x\rangle$ 时, 该算法能比最好的经典算法指数级加速.

HHL 算法的主要运算过程如下. 算法在一个由工作系统和辅助系统组成的量子系统执行. 首先高效制备工作系统初态 $|b\rangle$ 和辅助系统初态 $|\Psi_0\rangle$. 然后利用 $|\Psi_0\rangle$ 控制的酉算符 U 在 $|b\rangle$ 上执行人们熟知的相位估计操作, 并进行傅立叶逆变换. 整个系统近似的演化到 $\sum_j \beta_j|\lambda_j\rangle|u_j\rangle$ 态 (忽略归一化系数). $|b\rangle$ 被分解为 A 的本征基矢的线性组合, 表示为 $|b\rangle = \sum_j \beta_j|u_j\rangle$. 在整个量子系统再加一个辅助比特并在辅助比特上进行 $|\lambda_j\rangle$ 控制的旋转操作. 我们通过相位估计的逆变换将 $|\lambda_j\rangle$ 态变为 $|\Psi_0\rangle|b\rangle$. 当我们观测到辅助比特处于 $|0\rangle$ 时算法成功, 此时系统对应的输出态是 $|x\rangle = \sum_j \beta_j\lambda_j^{-1}|u_j\rangle$. 态矢量 $|x\rangle$ 就是线性方程组 $A\vec{x} = \vec{b}$ 的解 $\vec{x}$.

HHL 算法的基本思路可概括为输出一个 $|x\rangle = \sum_j \beta_j\lambda_j^{-1}|u_j\rangle$ 态, 这个输出态是输入态 $|b\rangle$ 经历非幺正演化后的结果. 该算法也是具有对偶量子模式的基于酉算符组合的非幺正演化算法. 我们给出其在对偶量子模式下的量子线路图, 如图 5 所示.

13 开放量子体系的对偶量子模拟算法

由于和环境不可避免的耦合作用, 几乎所有现实的量子系统都是开放量子体系. 开放量子体系的演化通常是非幺正的, 因此也适合使用对偶量子计算模式进行模拟 [33]. 开放量子体系的时间演化可以通过 Kraus 算子来实现, 而 Kraus 算子可以表示为幺正算符线性叠加的形式.

与环境耦合的开放量子体系演化可以表示为一个完全正定的线性映射 $\varepsilon(\rho)$. 设定初态的工作系统和环境都是纯态, 表示为 $\rho_{\text{env}} = |e_0\rangle\langle e_0|$. 系统的演化过程如下 [36]:

$$\varepsilon(\rho) = \sum_k \langle e_k|U\{\rho \otimes |e_0\rangle\langle e_0|\}U^\dagger|e_k\rangle \tag{60}$$

$$= \sum_k E_k \rho E_k^\dagger, \tag{61}$$

其中

$$E_k = \langle e_k|U|e_0\rangle$$

是 Kraus 算子, 满足完备性条件

$$\sum_k E_k^\dagger E_k = I.$$

需要注意的是通常情况下, E_k 是非幺正的, 只作用在工作系统上. 我们使用对偶量子算法模拟开放体系的复杂度为 $O(d^3\|H\|_{\max} t\log(r/\epsilon)/\log\log(r/\epsilon))$, 相比以前的幺正演化算法在精度上有指数级提升 [33].

我们的方法包含两个步骤: 第 1 阶段是利用对偶量子门实现 Kraus 算子; 第 2 阶段是使用 Taylor 截断项来近似时间演化算符.

定理2 对偶量子门 $L_k = \sum_i W_{ki} V_{i0} U_i$ 是保迹的 Kraus 算子, 即 $\sum_k L_k^\dagger L_k = I$.

证明 首先定义 $L_k = \sum_i W_{ki} V_{i0} U_i$, 然后有 $L_k^\dagger = \sum_i W_{ki}^\dagger V_{i0}^\dagger U_i^\dagger$. 推导过程如下:

$$\begin{aligned}
\sum_k L_k^\dagger L_k &= \sum_k \left(\sum_i W_{ki}^\dagger V_{i0}^\dagger U_i^\dagger \sum_{i'} W_{ki'} V_{i'0} U_{i'} \right) \\
&= \sum_k W_{ki}^\dagger W_{ki'} \left(\sum_i V_{i0}^\dagger U_i^\dagger \sum_{i'} V_{i'0} U_{i'} \right) \\
&= \left(\delta_{ii'} \sum_{ii'} V_{i0}^\dagger U_i^\dagger V_{i'0} U_{i'} \right) \\
&= \left(\sum_i V_{i0} U_i^\dagger V_{i0} U_i \right) \\
&= \sum_i |V_{i0}|^2 U_i^\dagger U_i \\
&= I.
\end{aligned} \tag{62}$$

证明过程中用到了 W, V 和 U_i 都是幺正矩阵的性质. 因此, 对偶量子门 L_k 可以用来实现 Kraus 算子 E_k. 事实上, E_k 是有限 Hilbert 空间的线性有界算符, 总可以表示成幺正算符线性叠加的形式. 环境对系统的作用可以等效为不同算符同时作用在系统上的叠加效果. 在这种 Kraus 算子表示形式下, 我们可以直接得到不包含环境的系统的末态信息.

在前面的部分已经利用 $L_k=\sum_i W_{ki}V_{i0}U_i$ 实现了 Kraus 算子 E_k. 为了实现整个算法, 接下来只需要实现 Kraus 算子里的幺正算符 U_i. U_i 可以视为时间演化算符通过 Taylor 截断项来近似实现. 具体的实现过程与 BCCKS 算法一样, 这里就不在赘述. 我们的算法中, 以精度 ϵ 实现 U_i 的操作的复杂度为

$$K=O\left(\frac{r\log(r/\epsilon)}{\log\log(r/\epsilon)}\right). \tag{63}$$

考虑到 L_k 的系数满足 $\sum_i|W_{ki}V_{i0}|\leqslant 1$, 实现 E_k 的复杂度与实现 U_i 是相同的. 实现 d 个 E_k 的整个算法的复杂度为

$$\mathrm{dKr}=O\left(d^3\|H\|_{\max}t\frac{\log(r/\epsilon)}{\log\log(r/\epsilon)}\right). \tag{64}$$

而采用幺正演化的 Stinespring 标准表示的 Llyod 的算法的复杂度为 $O(ld^4ht^2/\epsilon)$. 对偶算法与该算法对比, 对维度的依赖由 $O(d^4)$ 降到 $O(d^3)$ 且精度 ϵ 的表现有指数级提升.

14 总结与展望

量子计算具有量子平行性, 有强大的平行计算能力. 已经被 Shor 算法、Grover 算法 (或其优化形式) 和量子模拟算法所证明. 传统算法对幺正演化的要求, 限制了新算法的提出. 对偶量子算法作为新型的计算模式, 能够通过酉算符的线性叠加实现非幺正演化. 因此, 对偶量子计算可以实现非幺正的量子算法.

最近发展的 HHL 对偶量子算法、稀疏 Hamiltonian 系统的对偶量子模拟算法、高精度对偶量子模拟算法、开放体系对偶量子模拟算法等 4 个量子算法都采用了酉算法的线性组合进行计算, 不再是酉过程, 显示出它们在相较于传统量子算法的优势.

利用酉算符构造量子算法, 使得构造过程和对计算过程的理解完全不同于经典算法, 经典计算中构造算法的技巧不能再用来构造量子算法. 对偶量子计算在设计算法时的灵活性, 可以架起经典算法和量子算法的桥梁. 乐观的估计量子计算机可能在 10∼20 年之间研制成功. 当量子计算机研制成功之后, 如何利用量子计算机开展研究, 将是人们考虑更多的问题. 随着量子计算机硬件的发展, 量子算法的研究将会越来越迫切, 自然也就成为更加受人关注的课题. 而如何利用对偶量子计算模式, 借鉴经典算法的技巧, 发展对偶量子算法, 是一个重要的研究方向.

参考文献

1 Benioff P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. J Stat Phys, 1980, 22: 563–591

2 Manin Y I. Vychislimoe i nevychislimoe (Computable and noncomputable) (in Russian). Sov Radio, 1980, 13–15

3 Feynman R P. Simulating physics with computers. Int J Theor Phys, 1982, 21: 467–488

4 Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer. Proc Royal Soc A: Math, Phys Eng Sci, 1985, 400: 97–117

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

6 Grover L K. A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing, Philadelphia, 1996. 212–219

7 Wang S H, Long G L. Big data and quantum computation. Chinese Sci Bull, 2015, 60: 499–508

8 Shor P W. Why haven't more quantum algorithms been found? J ACM, 2003, 50: 87–90

9 Long G L. General quantum interference principle and duality computer. Commun Theor Phys, 2006, 45: 825–844

10 Long G L, Liu Y. Duality computing in quantum computers. Commun Theor Phys, 2008, 50: 1303–1306
11 Long G L, Liu Y, Wang C. Allowable generalized quantum gates. Commun Theor Phys, 2009, 51: 65–67
12 Gudder S. Mathematical theory of duality quantum computers. Quantum Inf Process, 2007, 6: 37–48
13 Long G L. Mathematical theory of the duality computer in the density matrix formalism. Quantum Inf Process, 2007, 6: 49–54
14 Long G L. Duality quantum computing and duality quantum information processing. Int J Theor Phys, 2011, 50: 1305–1318
15 Gudder S. Duality quantum computers and quantum operations. Int J Theor Phys, 2008, 47: 268–279
16 Wang Y Q, Du H K, Dou Y N. Note on generalized quantum gates and quantum operations. Int J Theor Phys, 2008, 47: 2268–2278
17 Du H K, Wang Y Q, Xu J L. Applications of the generalized Lüders theorem. J Math Phys, 2008, 49: 013507
18 Cao H X, Li L, Chen Z L, et al. Restricted allowable generalized quantum gates. Chinese Sci Bull, 2010, 55: 2122–2125
19 Zhang Y, Cao H X, Li L. Realization of allowable qeneralized quantum gates. Sci China Phys Mech Astron 2010, 53: 1878–1883
20 Chen L, Cao H X, Meng H X. Generalized duality quantum computers acting on mixed states. Quantum Inf Process, 2015, 14: 4351–4360
21 Cao H X, Chen Z L, Guo Z H, et al. Complex duality quantum computers acting on pure and mixed states. Sci China Phys Mech Astron, 2012, 55: 2452–2462
22 Cao H X, Long G L, Guo Z H, et al. Mathematical theory of generalized duality quantum computers acting on vector-states. Int J Theor Phys, 2013, 52: 1–17
23 Cui J X, Zhou T, Long G L. Density matrix formalism of duality quantum computer and the solution of zero-wave-function paradox. Quantum Inf Process, 2012, 11: 317–323
24 Long G L, Liu Y. Duality quantum computing. Front Comput Sci, 2008, 2: 167–178
25 Long G L, Liu Y. General principle of quantum interference and the duality quantum computer. Rep Prog Phys, 2008, 28: 410–431
26 Zou X F, Qiu D W, Wu L H, et al. On mathematical theory of the duality computers. Quantum Inf Process, 2009, 8: 37–50
27 Qiang X, Zhou X, Aungskunsiri K, et al. Quantum processing by remote quantum control. Quantum Sci Technol, 2017, 045002
28 Harrow A W, Hassidim A, Lloyd S. Quantum algorithm for linear systems of equations. Phys Rev Lett, 2009, 103: 150502
29 Wei S J, Zou Z R, Ruan D, et al. Realization of the algorithm for system of linear equations in duality quantum computing. In: Proceeding IEEE 85th Vehicular Technology Conference, Sydney, 2017
30 Childs A M, Wiebe N. Hamiltonian simulation using linear combinations of unitary operations. Quantum Inform Comput, 2012, 12: 901-924
31 Berry D W, Childs A M, Cleve R, et al. Simulating Hamiltonian dynamics with a truncated Taylor series. Phys Rev Lett, 2015, 114: 090502
32 Wei S J, Long G L. Duality quantum computer and the efficient quantum simulations. Quantum Inf Process, 2016, 15: 1189–1212
33 Wei S J, Ruan D, Long G L. Duality quantum algorithm efficiently simulates open quantum systems. Sci Rep, 2016, 6: 30727
34 Barenco A, Bennett C H, Cleve R, et al. Elementary gates for quantum computation. Physical Review A, 1995, 52: 3457
35 Liu Y, Long G L, Sun Y. Analytic one-bit and CNOT gate constructions of general n-qubit controlled gates. Int J Quant Inform, 2008, 6: 447-462
36 Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2010
37 Lloyd S. Universal quantum simulators. Science, 1996: 1073–1077
38 Hunziker M, Meyer D A. Quantum algorithms for highly structured search problems. Quantum Inf Process, 2002, 1: 145–154
39 Grover L K. Quantum computers can search rapidly by using almost any transformation. Physical Rev Lett, 1998, 80:

4329
40 Long G L, Zhang W L, Li Y S, et al, Arbitrary phase rotation of the marked state cannot be used for Grover's quantum search algorithm. Commun Theor Phys, 1999, 32: 335
41 Long G L, Li Y S, Zhang W L, et al. Phase matching in quantum searching. Physics Lett A, 1999, 262: 27–34
42 Long G L, Li X, Sun Y. Phase matching condition for quantum search with a generalized initial state. Physics Lett A, 2002, 294: 143–152
43 Long G L. Grover algorithm with zero theoretical failure rate. Physical Rev A, 2001, 64: 022307
44 Long G L, Liu Y. Search an unsorted database with quantum mechanics. Front Comput Sci, 2007, 1: 247–271
45 Hoyer P. Arbitrary phases in quantum amplitude amplification. Physical Rev A, 2000, 62: 052304
46 Biham E, Biham O, Biron D, et al. Analysis of generalized Grover quantum search algorithms using recursion equations. Physical Rev A, 2000, 63: 012310
47 Diao Z. Exactness of the original Grover search algorithm. Physical Rev A, 2010, 82: 044301
48 Toyama F M, van Dijk W, Nogami Y. Quantum search with certainty based on modified Grover algorithms: optimum choice of parameters. Quantum Inf Process, 2013: 1–18
49 Castagnoli G. Highlighting the mechanism of the quantum speedup by time-symmetric and relational quantum mechanics. Found Physics, 2016, 46: 360–381
50 Benioff P. Space searches with a quantum robot. AMS Contemporary Math Series, 2002, 305: 1–13
51 Bhattacharya N, van den Heuvell H B L, Spreeuw R J C. Implementation of quantum search algorithm using classical Fourier optics. Physical Rev Lett, 2002, 88: 137901
52 Puentes G, La Mela C, Ledesma S, et al. Optical simulation of quantum algorithms using programmable liquid-crystal displays. Physical Rev A, 2004, 69: 042319
53 Ivanov S S, Ivanov P A, Vitanov N V. Simple implementation of a quantum search with trapped ions. Physical Rev A, 2008, 78: 030301
54 Botsinis P, Ng S X, Hanzo L. Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design. IEEE Access, 2013, 1: 94–122
55 Yoder T J, Low G H, Chuang I L. Fixed-point quantum search with an optimal number of queries. Physical Rev Lett, 2014, 113: 210501
56 Grover L K, Radhakrishnan J. Is partial quantum search of a database any easier? In: Proceedings of the 17th Annual ACM Symposium on Parallelism in Algorithms and Architectures. New York: ACM, 2005. 186–194
57 Imre S, Balazs F. Quantum Computing and Communications: an engineering approach. Hoboken: John Wiley & Sons, 2013
58 Dong D, Petersen I R. Sliding mode control of quantum systems. New J Physics, 2009, 11: 105033
59 Trugenberger C A. Quantum pattern recognition. Quantum Inf Process, 2002, 1: 471–493
60 Pang C Y, Zhou Z W, Guo G C. A hybrid quantum encoding algorithm of vector quantization for image compression. Chinese Physics, 2006, 15: 3039
61 Marshman R J, Lund A P, Rohde P P, et al. Passive quantum error correction of linear optics networks through error averaging. arXiv: 1709.02157
62 Suzuki M. General theory of fractal path integrals with applications to many body theories and statistical physics. J Math Phys, 1991, 32: 400–407
63 Blanes S, Casas F, Ros J. Extrapolation of symplectic integrators. Celest Mechan Dynam Astron, 1999, 75: 149–161

Quantum Computing

Shi-Jie WEI[1,2], Tao WANG[1], Dong RUAN[1,2] & Gui-Lu LONG[1,2,3*]

1. *State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing* 100084*, China*;
2. *Collaborative Innovation Center of Quantum Matter, Beijing* 100084*, China*;
3. *Tsinghua National Laboratory for Information Science and Technology, Beijing* 100084*, China*
* Corresponding author. E-mail: gllong@tsinghua.edu.cn

Abstract Quantum computing exploits quantum mechanical properties to perform computations. It enables quantum parallelism and provides much more powerful data processing capabilities than classical computers. With a quantum computer, one can exponentially accelerate quantum system simulation and accelerate some important classical algorithms. Traditional quantum algorithms use unitary evolution to process information. A quantum computing process is the product of a series of unitary operators. In 1994, Shor invented a quantum prime factorization algorithm that exponentially accelerates the factorization of an integer. In 1996, Grover proposed a quantum search algorithm that accelerates the search of an unsorted database using square-root steps. Afterwards, the development of quantum algorithms slowed down, leading to a subsequent query by Shor in 2003 regarding why no more significant quantum algorithms have been found. Since 2009, many important new quantum algorithms have been proposed, such as a quantum algorithm for solving linear equations with the capability of exponential acceleration, a quantum algorithm for sparse Hamiltonian simulation using linear combinations of unitary operators, and a novel algorithm for Hamiltonian simulation, which provides exponential improvements in precision. In this paper, we first describe the basic principles of quantum computation. We then describe the Shor algorithm and Grover/Long search algorithm. These quantum algorithms are the general quantum algorithms that use unitary operations in their computational processes. Next, we introduce the basic principles of duality quantum computing, which was proposed in 2002. In contrast to traditional quantum computing, duality quantum computing allows the use of linear combinations of unitary operators in the computation process, meaning the multiplication, division, addition, and subtraction of unitary operators are all possible in duality quantum computing. Thus, duality quantum computing provides more flexibility for constructing quantum algorithms and the techniques used in classical algorithm design can be directly used to construct quantum algorithms. We then review recent work regarding newer quantum algorithms that enable the linear combination of unitary operators, which are actually duality quantum algorithms. Additionally, a duality quantum simulation algorithm for open quantum systems is introduced. This algorithm not only reduces computational complexity, but also improves accuracy exponentially. Finally, a summary and the future prospects of quantum algorithms are provided.

Keywords quantum computing, quantum algorithm, Long's algorithm, duality quantum computing

Shi-Jie WEI was born in 1989. He received his Bachelor's degree in China from QingDao University, ShanDong, in 2008. He received a Master's degree in China from ZheJiang University, ZheJiang, in 2012. Currently, he is a Ph.D. student at Tsinghua University, Beijing, China. His research interests include quantum information and quantum algorithms.

Tao WANG was born in 1991. He received his Bachelor's degree in China from Xi'an Jiaotong University, Xi'an, in 2009. He is currently a Ph.D. student at Tsinghua University, Beijing, China. His research interests include quantum information, quantum optics, and optical microcavity.

Dong RUAN was born in 1970. He received his Ph.D. degree in 1997 from Tsinghua University, Beijing. He is currently a professor at Tsinghua University. His research interests include quantum computing, quantum physics, and mathematical physics. He is vice-chair of the National College Steering Committee on Physics Major Teaching, MOE.

Gui-Lu LONG was born in 1962. He received his Ph.D. degree in 1987 from Tsinghua University, Beijing. He is currently a professor at Tsinghua University. His research interests include duality quantum computing, quantum secure direct communication, and quantum information processing. He is a fellow of the APS and IoP, as well as vice-chair of the Commission on Physics and Development, IUPAP, and president of the Association of Asia Pacific Physical Societies.