精确 Grover 量子搜索算法概述

李冠中，李绿周*

(中山大学计算机学院 广州 510006)

【摘要】Grover 算法自提出以来就备受关注，因其对无序数据库搜索问题有相对于经典算法平方级别的加速。但是原始 Grover 算法通常无法百分之百得到目标元素，即使目标元素占比已知。为此，精确 Grover 量子搜索算法被提出，它们作为原始 Grover 算法的扩展，在保持平方加速的同时，能以 100% 的概率输出目标元素。该文较系统地梳理已有的 3 种精确 Grover 量子搜索算法，详细介绍算法的流程、参数设置、背后的几何直观，并针对目标元素占比已知及未知的情况，说明精确量子搜索的查询复杂性下界。

关 键 词 精确 Grover 量子搜索算法； Grover 算法； 量子计算； 无序数据库搜索
中图分类号 TP301 文献标志码 A doi:10.12178/1001-0548.2022100

Overview of Exact Grover's Quantum Search Algorithms

LI Guanzhong and LI Lyuzhou*

(School of Computer Science and Engineering, Sun Yat-sen University Guangzhou 510006)

Abstract Grover's algorithm has attracted much attention ever since it was proposed, because it has a quadratic speedup over classical algorithm for searching unstructured database. However, the original Grover's algorithm usually cannot obtain the target elements with certainty, even if the proportion of target elements is known. To this end, exact Grover's quantum search algorithms were proposed as extensions of the original Grover's algorithm, which can output the target element with certainty, while maintaining the quadratic speedup. This paper systematically sorts out the three existing exact Grover's quantum search algorithms, introducing in detail the algorithm process, parameter settings, and the geometric intuition behind them. Moreover, the lower bound on the query complexity of these algorithms is shown, under both situations when the proportion of target elements is known or unknown.

Key words exact Grover's quantum search algorithm; Grover's algorithm; quantum computing; unstructured database search

求解无序数据库搜索问题的 Grover 量子搜索算法[1] 于 1996 年被提出，相对于经典算法有平方级别的加速。自问世以来，得到广泛应用，如被用于求解最小值查找问题[2]、串匹配问题[3]、量子动态规划[4] 及计算几何问题[5]。不仅如此，针对 Grover 算法本身的扩展也不少，如量子振幅放大[6]、图上量子游走搜索[7]、不动点量子搜索[8-9] 及本文要介绍的精确 Grover 量子搜索算法[6, 10-11]。

1 原始 Grover 算法及其缺陷

无序数据库搜索问题可以抽象地描述如下，在大小为$N=2^n$的无序数据库中，有M个元素是符合要求的，这些目标元素通过一个函数$f:\{0,1,\cdots,N-1\}\to\{0,1\}$来标识：若编号为$x$的元素为目标元素，那么$f(x)=1$；否则，$f(x)=0$。假设有一个可以识别搜索问题目标元素的黑盒：要判断编号为x的元素是否为目标元素，只需要将编号x输入黑盒，它就会输出$f(x)$的值。现在希望以尽可能少的黑盒调用次数 (称之为查询复杂性)，找出一个目标元素。

在量子计算中，实现函数$f(x)$的黑盒的作用效果是一个酉操作O_f，其在计算基态上的作用效果为：

收稿日期：2022－04－02；修回日期：2022－04－13
基金项目：国家自然科学基金 (61772565)；广东省基础与应用基础研究基金 (2020B1515020050)
作者简介：李冠中 (1999－)，男，博士生，主要从事量子计算方面的研究.
*通信作者：李绿周，E-mail：lilvzh@mail.sysu.edu.cn

$$O_f|x\rangle|q\rangle=|x\rangle|q\oplus f(x)\rangle \tag{1}$$

式中，$|x\rangle$是存储元素编号的量子寄存器 (即n个 qubit)；$|q\rangle$是单 qubit 辅助寄存器，用于储存黑盒返回的结果，运算$\oplus$为异或。如果将辅助寄存器$|q\rangle$的初始态设置为$|-\rangle:=(|0\rangle-|1\rangle)/\sqrt{2}$，那么黑盒将不改变辅助寄存器的状态$|-\rangle$，故可以忽略它，因此可以将黑盒的作用效果表示为：

$$O_f|x\rangle=(-1)^{f(x)}|x\rangle \tag{2}$$

原始 Grover 算法的具体流程为，首先利用n个 qubit 上的 Hadamard 变换制备初始均匀叠加态$|\psi\rangle=H^{\otimes n}|0\rangle$，然后迭代$O(\sqrt{N/M})$次 Grover 算子$G$：

$$\begin{aligned}G:=&H^{\otimes n}(2|0\rangle\langle 0|-I)H^{\otimes n}O_f=\\&(2|\psi\rangle\langle\psi|-I)O_f\end{aligned} \tag{3}$$

最后进行计算基态测量，将以很大概率得到某一目标元素的编号。即 Grover 算法的查询复杂度为$O(\sqrt{N/M})$。相比之下，在经典计算机上则期望需要$O(N/M)$次检索才能以高概率得到目标元素，即其查询复杂度为$O(N/M)$。因此 Grover 算法相对于经典算法有平方级别的加速。

Grover 算子G的作用效果有着很强的几何直观，令

$$|A\rangle=\frac{1}{\sqrt{N-M}}\sum_{x:f(x)=0}|x\rangle \tag{4}$$

$$|B\rangle=\frac{1}{\sqrt{M}}\sum_{x:f(x)=1}|x\rangle \tag{5}$$

分别为非目标元素和目标元素的均匀叠加态，那么在单位正交向量$|A\rangle$和$|B\rangle$张成的二维子空间中，G的作用相当于先以$|A\rangle$为法线进行反射，再以$|\psi\rangle$为法线进行反射，总的效果是由$|A\rangle$朝着$|B\rangle$旋转了2θ角度，这里$\sin(\theta)=\sqrt{M/N}$为初始态$|\psi\rangle$在$|B\rangle$上的投影。

这么看来，Grover 算法总的流程，在几何直观上可以理解为，从与$|A\rangle$偏离了θ角度的初始状态向量$|\psi\rangle$出发，通过作用k次 Grover 算子G，把它朝着$|B\rangle$旋转了$k\cdot 2\theta$角度，最终得到状态向量

$$G^k|\psi\rangle=\cos((2k+1)\theta)|A\rangle+\sin((2k+1)\theta)|B\rangle \tag{6}$$

如果迭代次数k选得恰当，使得最终态尽可能地接近$|B\rangle$，即使得$(2k+1)\theta$尽可能接近$\pi/2$，那么在计算基上测量将以高概率$(\sin^2((2k+1)\theta))$得到问题的一个目标元素。特别地，当$M/N=1/4$，即目标元素的占比为1/4时，θ为$\pi/6$，那么取k为1，$(2k+1)\theta$等于$\pi/2$，最终态就是$|B\rangle$，进行计算基态测量将以100%的概率得到一个目标元素。

但是通常情况下，目标元素的占比M/N不会使得

$$k_{\text{opt}}:=\frac{\pi/2-\theta}{2\theta}=\frac{\pi}{4\arcsin\left(\sqrt{M/N}\right)}-\frac{1}{2} \tag{7}$$

恰为整数，而迭代次数k必须是整数，因此原始 Grover 算法无法做到以100%的概率精确地得到一个目标元素。

2　精确 Grover 量子搜索算法

为了弥补上述缺陷，即在不牺牲平方加速的同时，使得到的最终状态向量就是$|B\rangle$(可以相差一个整体相位，因为这并不会影响测量结果)，有 3 种方法[6,10-11]在 2000 年左右被提出，它们的思路虽然不一样，但都基于对原始 Grover 算子进行扩展：

$$G(\phi,\varphi)=-\mathcal{A}S_0(\phi)\mathcal{A}^{\dagger}S_f(\varphi) \tag{8}$$

再通过设置适当的角度ϕ,φ和迭代次数k，使得多次迭代扩展 Grover 算子$G(\phi,\varphi)$后得到的最终态就是目标元素的均匀叠加态$|B\rangle$。本文把 3 种方法的思路总结为：大步小步、共轭旋转和三维旋转，由于推导过程较为繁琐，下面在分别阐述 3 种方法时某些步骤有所省略，感兴趣的读者可以参考原始文献。

在$G(\phi,\varphi)$的定义式中，算子$\mathcal{A}$满足$\mathcal{A}|0\rangle=1/\sqrt{N}\sum_{x=0}^{N-1}|x\rangle$，用于得到均匀叠加态，如在原始 Grover 算法中$\mathcal{A}$就是 Hadamard 变换$H^{\otimes n}$；$S_0(\phi)|x\rangle=\mathrm{e}^{\mathrm{i}\phi}|x\rangle$当且仅当$|x\rangle=|0\rangle$，用于旋转状态$|0\rangle$的相位；$S_f(\varphi)|x\rangle=\mathrm{e}^{\mathrm{i}\varphi}|x\rangle$当且仅当$f(x)=1$，用于旋转目标元素的相位。特别地，当$\varphi=\phi=\pi$时，$G(\phi,\varphi)$恢复到原始 Grover 算子$G=G(\pi,\pi)$。

2.1　大步小步

这一方法[6]的思路比较直接。由于原始 Grover 算法中的误差来自需要旋转的角度$(\pi/2-\theta)$不是单次旋转角度(2θ)的整数倍，那么不妨在前$\lfloor k_{\text{opt}}\rfloor$步仍作用原始 Grover 算子每次旋转$2\theta$角度，最后一步减缓速度作用$G(\phi,\varphi)$，旋转剩余的角度。因此总流程可以形象地描述为：从$|\psi\rangle$出发先走$\lfloor k_{\text{opt}}\rfloor$大步，再走一小步到达$|B\rangle$。

具体来说，首先作用$\lfloor k_{\text{opt}}\rfloor$次原始 Grover 算子于初始状态向量$|\psi\rangle=\mathcal{A}|0\rangle$，得到状态向量

$$\left|\tilde{\psi}\right\rangle := \cos\left(\left(2\left\lfloor k_{\text{opt}}\right\rfloor+1\right)\theta\right)|A\rangle+\sin\left(\left(2\left\lfloor k_{\text{opt}}\right\rfloor+1\right)\theta\right)|B\rangle \tag{9}$$

其次考虑$G(\phi,\varphi)$在正交基$|A\rangle$和$|B\rangle$下的矩阵，可以得到：

$$G(\phi,\varphi)=\begin{bmatrix} -(1-\mathrm{e}^{\mathrm{i}\phi})\sin^2(\theta)-\mathrm{e}^{\mathrm{i}\phi} & \mathrm{e}^{\mathrm{i}\varphi}(1-\mathrm{e}^{\mathrm{i}\phi})\sin(\theta)\cos(\theta) \\ (1-\mathrm{e}^{\mathrm{i}\phi})\sin(\theta)\cos(\theta) & \mathrm{e}^{\mathrm{i}\varphi}((1-\mathrm{e}^{\mathrm{i}\phi})\sin^2(\theta)-1) \end{bmatrix} \tag{10}$$

再令$G(\phi,\varphi)\left|\tilde{\psi}\right\rangle$的$|A\rangle$分量为0，便能解出参数$\phi$和$\varphi$，使得最终态为目标元素的均匀叠加态$|B\rangle$。

2.2 共轭旋转

这一方法[10]主要基于如下观察：通过选取适当的角度ϕ和φ，可以使得$G(\phi,\varphi)$在共轭一个条件相位旋转的意义下，实现任意角度β的二维旋转。具体来说，当参数ϕ和φ满足：

$$\sin(\phi/2)\sin(2\theta)=\sin(\beta) \tag{11}$$

$$\tan(\varphi/2)=\tan(\phi/2)\cos(2\theta) \tag{12}$$

时，$G(\phi,\varphi)$的对角元相等，且可以分解为：

$$G(\phi,\varphi)=\mathrm{e}^{\mathrm{i}v}\begin{bmatrix}1&0\\0&\mathrm{e}^{\mathrm{i}u}\end{bmatrix}\begin{bmatrix}\cos(\beta)&-\sin(\beta)\\\sin(\beta)&\cos(\beta)\end{bmatrix}\begin{bmatrix}1&0\\0&\mathrm{e}^{-\mathrm{i}u}\end{bmatrix} \tag{13}$$

式中，参数$u=(\pi-\varphi)/2$；v作为整体相位无需考虑。因此，如果在上式两边同时进行$k=\left\lceil k_{\text{opt}}\right\rceil$次幂，并令角度$\beta$满足$k\beta=\pi/2-\theta$，那么移项可以得到：

$$\begin{bmatrix}\cos(\pi/2-\theta)&-\sin(\pi/2-\theta)\\\sin(\pi/2-\theta)&\cos(\pi/2-\theta)\end{bmatrix}= \mathrm{e}^{-\mathrm{i}kv}\begin{bmatrix}1&0\\0&\mathrm{e}^{-\mathrm{i}u}\end{bmatrix}G^k(\phi,\varphi)\begin{bmatrix}1&0\\0&\mathrm{e}^{\mathrm{i}u}\end{bmatrix} \tag{14}$$

把它作用到初态$|\psi\rangle=\cos(\theta)|A\rangle+\sin(\theta)|B\rangle$上，就能得到目标元素的均匀叠加态$|B\rangle$。注意到$S_f(\varphi)$在正交基$|A\rangle$和$|B\rangle$下的矩阵表示就是$\mathrm{diag}(1,\mathrm{e}^{\mathrm{i}\varphi})$，因此总的算法流程可以表示为$G^k(\phi,\varphi)S_f(u)|\psi\rangle=|B\rangle$。也就是说，从初始状态$|\psi\rangle$出发，先作用条件相位旋转$S_f(u)$把目标元素的相位旋转角度$u$，再作用$k$次扩展 Grover 算子$G(\phi,\varphi)$，便得到$|B\rangle$。

2.3 三维旋转

这一方法[11]的思路为：把$G(\phi,\phi)$在正交基$|A\rangle$和$|B\rangle$下的二维酉矩阵对应到相应 Bloch 球中的三维旋转，再通过选取适当的角度ϕ和旋转次数k，使得$G^k(\phi,\phi)|\psi\rangle$在该 Bloch 球面上与$|B\rangle$重合。

具体来说，由于任意二维酉矩阵都可以写成下式右边的形式，因此令

$$-G(\phi,\phi)=\mathrm{e}^{\mathrm{i}\phi}\left[\cos\left(\frac{\alpha}{2}\right)\boldsymbol{I}+\mathrm{i}\sin\left(\frac{\alpha}{2}\right)\left(n_x\boldsymbol{X}+n_y\boldsymbol{Y}+n_z\boldsymbol{Z}\right)\right] \tag{15}$$

再通过把$-G(\phi,\phi)$展开成单位矩阵和泡利矩阵$\boldsymbol{I},\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}$的线性组合，对比$\boldsymbol{I}$前的系数，得到旋转角度$\alpha=4\beta$,其中$\beta$满足$\sin(\beta)=\sin(\phi/2)\sin(\theta)$。对比$\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}$前的系数，得到转轴

$$\boldsymbol{n}=\frac{\cos(\theta)}{\cos(\beta)}\left[\cos(\phi/2),\sin(\phi/2),\cos(\phi/2)\tan(\theta)\right] \tag{16}$$

即在$\{|A\rangle,|B\rangle\}$的 Bloch 球中，$G(\phi,\phi)$相当于以$\boldsymbol{n}$为转轴、角度为α的三维旋转[12]。

由于初态$|\psi\rangle$在 Bloch 球中对应的向量为$\boldsymbol{s}:=[\sin(2\theta),0,-\cos(2\theta)]$，而算法最终欲得的$|B\rangle$对应的向量为$\boldsymbol{t}:=[0,0,1]$，故$\langle\boldsymbol{n}|\boldsymbol{s}\rangle=\langle\boldsymbol{n}|\boldsymbol{t}\rangle$。这说明$\boldsymbol{s}$和$\boldsymbol{t}$在 Bloch 球面以$\boldsymbol{n}$为轴的同一个的圆上，所以确实可以通过绕固定轴$\boldsymbol{n}$进行多次旋转，把$\boldsymbol{s}$转到$\boldsymbol{t}$。为了确定参数$\phi$和旋转次数$k$，记$\boldsymbol{r}$为$\boldsymbol{s}$和$\boldsymbol{t}$在$\boldsymbol{n}$上的投影，如图 1 所示，解析几何计算表明$\boldsymbol{s}-\boldsymbol{r}$和$\boldsymbol{t}-\boldsymbol{r}$之间的角度为$\omega=\pi-2\beta$。根据之前的推导，每作用一次$G(\phi,\phi)$相当于绕转轴$\boldsymbol{n}$旋转$\alpha=4\beta$，而$\omega$是所希望的总旋转角度，因此令$\omega=k\alpha$可以求出$\phi$与$k$应该满足关系式：

$$\sin\left(\frac{\pi}{4k+2}\right)=\sin\left(\frac{\phi}{2}\right)\sin(\theta) \tag{17}$$

容易看出当$k>k_{\text{opt}}$时ϕ有实数解，从而最小可以取$k=\left\lceil k_{\text{opt}}\right\rceil$，并得到相应的$\phi$值。

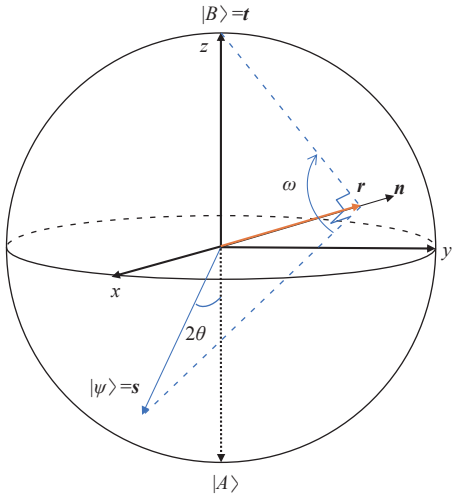

图 1 在$\{|A\rangle,|B\rangle\}$的 Bloch 球中，$G(\phi,\phi)$的多次作用相当于把初态$\boldsymbol{s}$绕转轴$\boldsymbol{n}$旋转到目标元素的均匀叠加态$\boldsymbol{t}$

最后，本文把上述 3 种精确 Grover 量子搜索算法总结如表 1 所示。值得注意的是，3 种算法中参数的设置都依赖于目标元素的占比M/N。另外，

(扩展)Grover 算子的迭代次数都是$\lfloor k_{\text{opt}} \rfloor = O(\sqrt{N/M})$，保持了原始 Grover 算法的平方加速。

实际操作中，还需考虑扩展 Grover 算子$G(\phi,\varphi)$的量子电路实现。由于

$$G(\phi,\varphi) = -(\mathcal{A}S_0(\phi)\mathcal{A})\cdot S_f(\varphi) := -S_\psi(\phi)\cdot S_f(\varphi) \quad (18)$$

容易验证，图 2 和图 3 分别展示了$S_f(\varphi)$和$S_\psi(\phi)$的电路实现，其中最后一行为辅助 qubit。注意到$S_f(\varphi)$需要调用两次黑盒O_f，因此表 1 中后两种方法的黑盒调用次数是原始 Grover 算法的两倍，不过这并不影响平方加速的数量级。

表 1　3 种精确 Grover 量子搜索算法

方法	大步小步	共轭旋转	三维旋转
流程	$G(\phi,\varphi)G(\pi,\pi)^k\mathcal{A}\|0\rangle$	$G^k(\phi,\varphi)S_f(u)\mathcal{A}\|0\rangle$	$G^k(\phi,\phi)\mathcal{A}\|0\rangle$
参数k	$\lfloor k_{\text{opt}} \rfloor$	$\lceil k_{\text{opt}} \rceil$	$\lceil k_{\text{opt}} \rceil$
参数ϕ	$2\operatorname{arccot}\left(\sqrt{\frac{\sin^2(2\theta)}{\cot^2((2k+1)\theta)}-\cos^2(2\theta)}\right)$	$2\arcsin\left(\frac{\sin\left(\frac{\pi/2-\theta}{k}\right)}{\sin(2\theta)}\right)$	$2\arcsin\left(\frac{\sin\left(\frac{\pi}{4k+2}\right)}{\sin(\theta)}\right)$
参数φ	$\arctan\left(\frac{\cot(\phi/2)}{-\cos(2\theta)}\right)$	$2\arctan\left(\tan\frac{\phi}{2}\cos(2\theta)\right)$	无
参数u	无	$(\pi-\varphi)/2$	无

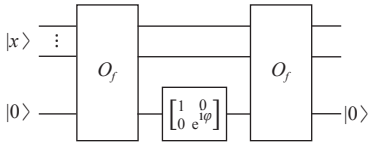

图 2　$S_f(\varphi)$的电路实现，其中$O_f|x\rangle|b\rangle = |x\rangle|b\oplus f(x)\rangle$

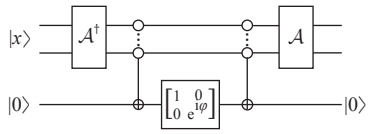

图 3　$S_\psi(\phi)$的电路实现

3　精确量子搜索的查询下界

3.1　目标元素占比未知时的查询下界

上面 3 种方法说明：在目标元素的占比已知的情况下，可以设计量子搜索算法在保持平方加速的同时，精确地找到目标元素。由此自然引出的一个问题是：如果目标元素的占比未知，还能设计出量子搜索算法既百分之百找到目标元素又保持平方加速吗？答案是否定的。事实上，假设存在这样的精确量子搜索算法，它在调用 T 次黑盒：$\mathrm{S}_x|i\rangle = (-1)^{x_i}|i\rangle$后 (这里把搜索问题函数$f:\{0,1,\cdots,N-1\}\to\{0,1\}$视为长为$N$的比特串$x_0x_1\cdots x_{N-1}$，以便于后面的讨论)，精确地输出目标元素$i$(如果无解，则输出不合法的指标，比如$|N\rangle$)，那么该算法稍加修改就能以相同的黑盒调用次数精确计算$\mathrm{OR}_N = x_0\vee x_1\vee\cdots\vee x_{N-1}$(如在算法的最后进行二分投影测量$\{P_0 = |N\rangle\langle N|, P_1 = I-P_0\}$)。但是，下面将用多项式方法[13] 证明：任意精确计算OR_N的量子算法都至少要调用$N/2$次黑盒，因此，在目标元素占比未知的情况下，任意精确量子搜索算法都必定丢失平方加速！

对于任意精确计算OR_N的量子算法，假设它进行了 T 次黑盒调用。首先把黑盒写成如下形式：

$$S_x|i\rangle = (1-2x_i)|i\rangle \quad (19)$$

可以看出，如果把基态前的振幅表示成关于变量$x_0,x_1,\cdots,x_{N-1}$的多元多项式，那么每次黑盒调用只会使得任意基态前的振幅多项式的次数增加至多 1。又注意到任意两次黑盒调用之间的酉变换作为线性变换，不会增加多项式的次数，因此最终测得P_1的概率 (振幅的模平方和) 可以表示成次数$\leqslant 2T$的多项式$p(x_0,x_1,\cdots,x_{N-1})$。由于算法以概率 1 计算$\mathrm{OR}_N$，因此$p(x) = \mathrm{OR}_N(x), \forall x = (x_0,x_1,\cdots,x_{N-1})\in\{0,1\}^N$。考虑对$p$的$N$个变量$x_0,x_1,\cdots,x_{N-1}$的所有排列进行平均所得的对称多项式

$$q(x) = \frac{1}{N!}\sum_{\pi\in S_N} p(\pi(x)) \quad (20)$$

那么可以证明，存在次数不超过$\deg(q)$的单变量多项式$r(z)$，使得$r(|x|) = q(x)$。而且不难看出$r(0)=0$，且对任意$t\in\{1,2,\cdots,N\}$都有$r(\mathrm{t})=1$，所以$\deg(r(z))\geqslant N$(因为$r(z)-1$是有N个零点的非零多项式)。从而$T\geqslant \mathrm{N}/2$。

3.2　目标元素占比已知时的查询下界

在目标元素的占比已知的情况下，利用文献 [14] 的 quantum angle 方法，并把它直接地扩展到多个

目标元素的情形 (即文献 [15] 文末提及的选取 $\lfloor N/M \rfloor$个“不相交”数据库的思路)，可以证得精确量子搜索的查询下界为

$$k_{\text{low}} := \left\lceil \frac{\pi}{4\arcsin\left(\sqrt{1/\lfloor N/M \rfloor}\right)} - \frac{1}{2} \right\rceil \tag{21}$$

这说明前面 3 种精确 Grover 量子搜索算法的查询复杂性都达到了最优。

事实上，对于任意精确量子搜索算法，设其进行 T 次黑盒调用后的状态为：

$$\left|\Psi_x^T\right\rangle = U_T S_x U_{T-1} S_x \cdots U_1 S_x U_0 |0\rangle \tag{22}$$

那么令$\prod_x = \sum_{j:x_j=1} |j\rangle\langle j|$，则该算法必须保证对于任意数据库$x = x_1 x_2 \cdots x_N$，都有

$$\left\| \prod_x \left|\Psi_x^T\right\rangle \right\|^2 = 1 \tag{23}$$

令 $\left|\Psi^T\right\rangle = U_T U_{T-1} \cdots U_1 U_0 |0\rangle$，并记$K := \lfloor N/M \rfloor$，那么得到查询下界$k_{\text{low}}$的思路在于给出如下表达式 (即 quantum angle 的均值)：

$$\frac{1}{K} \sum_{y \in S} \angle\left(\Psi^T, \Psi_y^T\right) \tag{24}$$

的上下界，其中

$$\angle\left(\Psi^T, \Psi_x^T\right) = \arccos\left|\left\langle \Psi^T | \Psi_x^T \right\rangle\right| \tag{25}$$

而S则表示$[N]:=\{1,2,\cdots,N\}$的K个不相交子集的集合 (把数据库y对应到$[N]$的子集$\{i : y_i = 1\}$)。具体的上下界如下式所示：

$$\frac{\pi}{2} - \arcsin\left(\sqrt{1/K}\right) \leqslant \frac{1}{K} \sum_{y \in S} \angle\left(\Psi^T, \Psi_y^T\right) \leqslant 2T \arcsin\left(\sqrt{1/K}\right) \tag{26}$$

由此便可以得出 T 的下界：

$$T \geqslant \frac{\pi}{4\arcsin\left(\sqrt{1/K}\right)} - \frac{1}{2} \tag{27}$$

式 (26) 的详细证明和文献 [14] 中的 Lemma 5(上界) 和 Lemma 7(下界) 几乎一模一样，只需要把求和下标由 y = 1至 N改为 $y \in S$，并把 N改为 $K = \lfloor N/M \rfloor$即可，这里不再赘述，只简要说明背后的直观想法：表达式 (24) 下界的直观是，经过 T 次查询，算法最终能以很大概率区分平凡黑盒 I和数据库x的黑盒的S_x，即Ψ^T和Ψ_x^T几乎垂直。而表达式 (24) 上界的直观是，每次查询最多只能使两者之间的角度增加很小的值。

4 结束语

本文梳理了 3 种精确 Grover 量子搜索算法，给出了算法流程、参数设置以及背后的几何直观，并指出它们都依赖于目标元素的占比，由此为出发点，说明了算法的最优性：对于目标元素占比已知的情况，3 种精确 Grover 量子搜索算法已经达到最优；而对于目标元素占比未知的情形，精确量子搜索算法相比经典算法没有加速。因此本文对精确量子搜索算法给出了较为完整的概述。

参 考 文 献

[1] GROVER L K. A fast quantum mechanical algorithm for database search[C]//Proceedings of the 28th Annual ACM Symposium on Theory of Computing. Pennsylvania: ACM, 1996: 212-219.

[2] CHRISTOPH D, PETER H. A quantum algorithm for finding the minimum[EB/OL]. (1996-07-18). https://arxiv.org/pdf/quant-ph/9607014.pdf.

[3] RAMESH H, VINAY V. String matching in $\tilde{O}$(sqrt(n)+sqrt(m)) quantum time[J]. Discrete Algorithms, 2003, 1(1): 103-110.

[4] AMBAINIS A, BALODIS K, IRAIDS J, et al. Quantum speedups for exponential-time dynamic programming algorithms[C]//Proceedings of the 13th Annual ACM-SIAM Symposium on Discrete Algorithms. San Diego: SIAM, 2019: 1783-1793.

[5] ANDRIS A, NIKITA L. Quantum algorithms for computational geometry problems[C]//The 15th Conference on the Theory of Quantum Computation, Communication and Cryptography. Riga: [s.n.], 2020, 9: 1-10.

[6] BRASSARD G, HOYER P, MOSCA M, et al. Quantum amplitude amplification and estimation[J]. Contemporary Mathematics, 2002, 305: 53-74.

[7] LI L, XU Y, ZHANG D. Robust quantum walk search [EB/OL]. (2021-11-17). https://arxiv.org/pdf/2111.09012.pdf.

[8] GROVER L K. Fixed-point quantum search[J]. Physical Review Letters, 2005, 95(15): 150501.

[9] YODER T J, LOW G H, CHUANG I L. Fixed-point quantum search with an optimal number of queries[J]. Physical Review Letters, 2014, 113: 210501.

[10] HØYER P. Arbitrary phases in quantum amplitude amplification[J]. Physical Review A, 2000, 62(5): 052304.

[11] LONG G L. Grover algorithm with zero theoretical failure rate[J]. Physical Review A, 2001, 64(2): 022307.

[12] NIELSEN M A, CHUANG I. Quantum computation and quantum information[M]. Cambridge: Cambridge University Press, 2002.

[13] BEALS R, BUHRMAN H, CLEVE R, et al. Quantum lower bounds by polynomials[C]//Proceedings of the 39th Annual Symposium on Foundations of Computer Science. Palo Alto: IEEE, 1998: 352-361.

[14] DOHOTARU C, HOYER P. Exact quantum lower bound for Grover's problem[J]. Quantum Information & Computation, 2009, 9(5): 533-540.

[15] BOYER M, BRASSARD G, HØYER P, et al. Tight bounds on quantum searching[J]. Fortschritte der Physik, 1998, 46(4-5): 493-505.

编 辑 蒋 晓