·特约论文·　　DOI：10. 13471/j. cnki. acta. snus. 2023A070

求图中点度数的量子算法*

郎健翔，李绿周

中山大学计算机学院，广东 广州 510006

摘　要：本文探讨了图属性测试问题的量子加速：对于给定的图和整数k，图中是否存在一个度数为k的顶点？该问题的量子复杂度在邻接矩阵oracle模型下被证明为$\mathcal{O}\left(N\sqrt{k}\right)$，而其经典复杂度为$\Omega\left(N^2\right)$，其中$N$是图中顶点的数量. 为了证明该结果，得出了一个技术性结论，即对于给定的函数$g:[N]\to\{0,1\}$和整数k，存在一个量子算法可以在$\mathcal{O}\left(\sqrt{Nk}\right)$次查询内判定$\left|\{x:g(x)=1\}\right|$是否等于$k$. 文中的结果基于量子奇异值变换（QSVT）和有误差输入的量子搜索技术.

关键词：量子奇异值变换；量子算法；图属性测试

中图分类号：TP301.6　　**文献标志码：**A　　**文章编号：**2097－0137（2024）01－0001－09

Quantum algorithm for finding degrees

LANG Jianxiang, LI Lüzhou

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

Abstract: Quantum speedups for the graph property testing problem is studied: For a given graph and an integer k, does the graph have a vertex of degree k? The quantum complexity of this problem is proven to be $\mathcal{O}\left(N\sqrt{k}\right)$ under the adjacency matrix oracle model, whereas its classical complexity is $\Omega\left(N^2\right)$, where N is the number of vertexes in the graph. In order to prove the result, a technical result that there exists a quantum algorithm for deciding whether $\left|\{x:g(x)=1\}\right|$ equals k or not in $\mathcal{O}\left(\sqrt{Nk}\right)$ queries, for a given function $g:[N]\to\{0,1\}$ and an integer k is obtained. These results are based on the techniques of quantum singular value transformation (QSVT) and quantum search on bounded-error inputs.

Key words: quantum singular value transformation; quantum algorithm; graph property testing

1　引言

属性测试是一个重要且广泛研究的领域，受到经典计算和量子计算社区的广泛关注（Goldreich，2017；Montanaro et al.，2016）. 其目的是确定给定对象是否具有预先确定的属性. 研究对象包括函数、概率分布、图等. 本文关注图的属性.

对于一个N个顶点的图，如果任何经典算法在最坏情况下都需要探查邻接矩阵中的所有条目，以确定某个属性，则该属性被称为难以捉摸的（Rosenberg，1973）. 也就是说，在邻接矩阵模型下的经典查询复

* **收稿日期：**2023－09－07　　**录用日期：**2023－11－02　　**网络首发日期：**2023－12－18
基金项目：国家自然科学基金（62272492）；广东省基础与应用基础研究基金（2020B1515020050）
作者简介：郎健翔（1999年生），男；**研究方向：**量子计算；E-mail：langjx3@mail2.sysu.edu.cn
通信作者：李绿周（1981年生），男；**研究方向：**量子计算；E-mail：lilvzh@mail.sysu.edu.cn

杂度为 $\Omega(N^2)$. 著名的 Aanderaa-Karp-Rosenberg 猜想（也称为难以捉摸猜想）认为，任何非平凡的单调图属性都是难以捉摸的. 然而，这个猜想目前还没有被证明. 令人惊讶的是，在一系列工作（Buhrman et al.，1999；Magniez et al.，2007；Kulkarni et al.，2015）之后，所有非平凡单调图属性的量子查询复杂度的下界被证明为 $\Omega(N)$（Aaronson et al.，2021）. 这个下界是最优的，因为非平凡单调图属性“至少包含一条边”可以使用 Grover 算法在 $\mathcal{O}(N)$ 次查询内确定. 虽然量子计算领域的大部分关注点都集中在单调图属性上，但非单调图属性在量子模型中的理解还不够充分（一些非单调图属性在（Sun et al.，2004）中被研究）.

在本文中，我们考虑的问题是确定一个图是否具有特定度数的顶点，这是一个难以捉摸且非单调的图属性. 更具体的问题描述如下.

问题 给定一个 N 个顶点的无向图 $G=(V,E)$ 和一个非负整数 k，目标是确定图 G 是否具有度数为 k 的顶点. 如果存在这样的顶点，则找出它.

假设一个图 $G=(V,E)$ 可以通过邻接矩阵查询模型进行访问. 它的量子版本用 O_G 表示：

$$O_G|v_i\rangle|v_j\rangle|b\rangle=\begin{cases}|v_i\rangle|v_j\rangle|b\rangle, & \text{if } (v_i,v_j)\notin E,\\ |v_i\rangle|v_j\rangle|b\oplus 1\rangle, & \text{if } (v_i,v_j)\in E,\end{cases}$$

其中 $(v_i,v_j)\in E$ 表示顶点 $|v_i\rangle$ 和 $|v_j\rangle$ 之间存在一条边.

1.1 结果和技术

本文旨在探讨使用最少的查询次数来解决上述问题的量子算法. 我们的主要结果如下.

定理 1 对于一个由 N 个顶点组成的无向图 $G=(V,E)$，可以通过邻接矩阵 Oracle O_G 访问该图，同时给定一个正整数 $k>0$. 存在一个量子算法，使用 $\mathcal{O}\left(N\sqrt{k}\right)$ 次对 O_G 的查询，如果图中存在度数为 k 的顶点，则该算法能够找到这样的顶点；否则，算法输出“不存在这样的顶点”.

一种直接解决上述问题的方法是首先使用精确量子计数算法（Brassard et al.，2002）以 $\mathcal{O}(N)$ 的查询次数获取每个顶点的度数，并且借助 Grover 搜索在 $\mathcal{O}\left(\sqrt{N}\right)$ 次查询中找到度数为 k 的顶点. 这种方法的开销为 $\mathcal{O}\left(N\sqrt{N}\right)$. 需要注意的是，我们仅需要知道目标顶点是否具有度数 k，而不需要知道该顶点的确切度数. 因此，我们将提出一种量子算法来确定一个顶点是否具有度数 k，然后将上述问题规约为此问题. 更一般地，我们可以得到一个有效的量子算法来解决精确计数的判定问题，具体方法如下.

定理 2 给定一个函数 $g:[N]\to\{0,1\}$，以及满足 $1\leqslant k\leqslant N$ 的整数 k，令 $M=\left|\{x:g(x)=1\}\right|$. 则存在一个量子算法，使用 $\mathcal{O}\left(\sqrt{Nk}\log\left(\frac{12}{\delta}\right)\right)$ 次对 g 的查询，并以至少为 $1-\delta$ 的概率判断 $M=k$ 或 $M\neq k$.

为了证明定理 2，我们将使用量子奇异值转换（QSVT）技术（Gilyén et al.，2019）. 此外，基于定理 2 和有限误差输入的量子搜索（Høyer et al.，2003），我们将证明定理 1.

1.2 相关工作

寻找顶点度数的经典算法. Goyal et al.（2020）证明了判断一个 n 个顶点的无向图是否有度为 0 或 1 或 2 的顶点是难以捉摸的性质，对于 $k>2$ 的情况下的下界是 $0.42n^2$，这改进了之前的下界 $0.25n^2$（Balasubramanian et al.，1997）. 此外，他们还证明了判断一个有向图是否有出度为 k（对于非负整数 $k\leqslant(n+1)/2$）的顶点是难以捉摸的问题. 这改进了之前 $k>1$ 时 $n(n-1-k)/2$ 的下界（Balasubramanian et al.，1997）. 一个非常相关的问题是在查询模型中寻找图中最大度数的顶点. 在无向图（Balasubramanian et al.，1997；Goyal et al.，2020）、有向图（Balasubramanian et al.，1997；Goyal et al.，2020）和竞赛图（Balasubramanian et al.，1997；Gutin et al.，2018；Goyal et al.，2020；Beretta et al.，2019）方面取得了一些进展. 竞赛图就是将完全无向图的边给定了方向，是社会学、投票等领域中使用的一个非常有用的模型. 此外，Dey（2017）给出了在竞赛图中寻找一些明确定义的顶点集的难以捉摸的下界.

图问题上的量子算法. 目前大多数解决图问题的量子算法都基于两种查询模型：邻接矩阵和邻接表.

其中，邻接矩阵查询模型被用于许多图问题，如最短路径、连通性、最小生成树等等，而邻接表查询模型则被用于某些需要实现全局变换的问题，如判定二分图、判定可遍历性等等.最近，一些新的查询模型也被研究了，如割问题和独立集问题.另外，在量子模型中，也有一些出色的工作涉及到图的性质检测，包括二分图性检测、扩展性检测等等.目前还没有关于量子算法来判断一个图是否有一个特定度数顶点的工作.

2　预备知识

在本文中，定义$[N]\coloneqq 0,1,\cdots,N-1$.我们将使用两个函数：一个是误差函数

$$\operatorname{erf}(x)=\frac{2}{\sqrt{\pi}}\int_0^x \mathrm{e}^{-\eta^2}\,\mathrm{d}\eta,$$

另一个是符号函数

$$\operatorname{sgn}(x)=\begin{cases}-1, & x<0,\\ 0, & x=0,\\ 1, & x>0.\end{cases}$$

接下来，简要介绍两个稍后将会用到的工具.

2.1　量子奇异值变换

量子奇异值变换(QSVT,quantum singular value transformation)技术最初在 Gilyén et al.(2019)中被提出，为我们设计量子算法提供了一种新方法.然后，参考 Martyn et al.(2021)利用 QSVT 技术提出了一个统一的框架，解释了大部分已有算法.本文中的算法也将基于 QSVT，特别是以下结果.

定理 3　给定一个酉矩阵U、它的逆$U^\dagger$以及算符$A_\phi=\mathrm{e}^{\mathrm{i}\phi|A_0\rangle\langle A_0|}$和$B_\phi=\mathrm{e}^{\mathrm{i}\phi|B_0\rangle\langle B_0|}$，定义$a=\langle A_0|U|B_0\rangle$.如果一个多项式$\operatorname{Poly}(a)$满足以下条件：i) $\deg\big(\operatorname{Poly}(a)\big)\leqslant d$；ii) 当$x\in[-1,1]$时，$\big|\operatorname{Poly}(a)\big|\leqslant 1$；iii) $\operatorname{Poly}(a)$是奇函数，那么我们可以利用 QSVT 技术构建一个电路，使得

$$\left\langle A_0\middle|\left[\prod_{t=1}^{d/2}U B_{\phi_{2t-1}}U^\dagger A_{\phi_{2t}}\right]U\middle|B_0\right\rangle=\operatorname{Poly}(a).$$

这个定理类似于Martyn et al.(2021)的定理2，但方向相反.其正确性在Gilyén et al.(2019)中已经暗示.

2.2　有界误差输入上的量子搜索

普通的 Grover 搜索只能在正确定义的oracle上生效，当对带有误差的oracle进行查询时，将会失败.于是Høyer et al.(2003)提出了以下有界误差输入的量子搜索技术.

定理 4(Høyer et al., 2003；Ambainis et al., 2020)　给定n个算法(无论是量子还是经典的),每个算法都以有界的出错概率给出一个布尔值，并且给定一个整数$T\geqslant 1$.那么存在一个量子算法，它使用$\mathcal{O}\left(\sqrt{n/T}\right)$次查询，并且以常数的概率：如果$n$个值中至少有$T$个值为 1，则返回一个对应值为1的索引；如果没有值为 1，则返回NULL.(当解的数量[T]未知时，期望查询次数也为$\mathcal{O}\left(\sqrt{n/T}\right)$).

3　量子算法

我们将本文考虑的问题规约为确定给定顶点的度数是否为k的问题，这进一步推广为在第 3.1 节中的精确计数判定问题.

3.1　精确计数问题的判定问题

定理2是本文中至关重要的技术结果.

定理 2 的证明　该证明包括两个步骤：(i)首先构造一个多项式$\operatorname{Ploy}(x)$来近似刻画问题的函数$f(x)$,(ii)然后针对多项式$\operatorname{Ploy}(x)$，根据定理3构造一个量子电路来实现它.

首先我们定义以下函数：

$$f(x)=\frac{1}{2}\operatorname{sgn}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)+\frac{1}{2}\operatorname{sgn}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)$$
$$-\frac{1}{2}\operatorname{sgn}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)-\frac{1}{2}\operatorname{sgn}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)$$
$$=\begin{cases}-1, & -\frac{1}{2}\left(\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}\right)<x<-\frac{1}{2}\left(\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}\right),\\ 1, & \frac{1}{2}\left(\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}\right)>x>\frac{1}{2}\left(\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}\right),\\ 0, & \text{其他}.\end{cases}\tag{1}$$

注意到该函数满足以下条件：

$$f\left(\sqrt{\frac{M}{N}}\right)=\begin{cases}1, & M=k,\\ 0, & M\neq k\end{cases}\tag{2}$$

是一个区别$M=k$还是$M\neq k$的指示器. 然后，我们可以构造一个多项式$\mathrm{Poly}(x)$，满足以下条件：

（i）$\mathrm{Poly}(x)$是奇函数；

（ii）$\mathrm{Poly}(x)$的次数为$\mathcal{O}\left(\sqrt{Nk}\log\left(\frac{12}{\delta}\right)\right)$；

（iii）当$x\in[-1,1]$时，$\left|\mathrm{Poly}(x)\right|\leqslant 1$；

（iv）当$x=\sqrt{\frac{M}{N}}$时，$\left|f(x)-\mathrm{Poly}(x)\right|\leqslant\frac{\delta}{2}$.

上述条件的证明将在后面的引理3中给出.

现在我们将构造一个量子电路来实现$\mathrm{Poly}(x)$. 设$\left|A_0\right\rangle=\sum_{i=1}^{M}\frac{1}{\sqrt{M}}\left|m_i\right\rangle$，其中$\left|m_i\right\rangle$是满足$g(m_i)=1$的状态. 定义$A_\phi$如下：

$$A_\phi\left|j\right\rangle=\begin{cases}\left|j\right\rangle, & f(j)=1,\\ \mathrm{e}^{\mathrm{i}\phi}\left|j\right\rangle, & f(j)\neq 1,\end{cases}$$

如Yoder et al.(2014)所示，可以通过使用一个或两个Oracle查询来实现A_ϕ. 此外，设$\left|B_0\right\rangle=\left|0\right\rangle$，即全零状态，$U=H^{\otimes n}$. 不需要查询Oracle即可实现$B_\phi$. 根据定理3中的变量$a$，我们有$\left\langle A_0\right|U\left|B_0\right\rangle=\sqrt{\frac{M}{N}}$. 根据定理3，可以构造一个量子电路$\left[\prod_{t=1}^{d/2}UB_{\phi_{2t-1}}U^{\dagger}A_{\phi_{2t}}\right]U$，记作$U_{\mathrm{QSVT}}$，其中$d=\mathcal{O}\left(\sqrt{kN}\log\left(\frac{12}{\delta}\right)\right)$，满足以下条件：

$$\left\langle A_0\right|U_{\mathrm{QSVT}}\left|B_0\right\rangle=\mathrm{Poly}\left(\sqrt{\frac{M}{N}}\right).$$

注意到$\left|f\left(\sqrt{\frac{M}{N}}\right)-\mathrm{Poly}\left(\sqrt{\frac{M}{N}}\right)\right|\leqslant\frac{\delta}{2}$和$f\left(\sqrt{\frac{M}{N}}\right)=\begin{cases}1, & M=k,\\ 0, & M\neq k.\end{cases}$因此，当$M=k$时，有以下结果：

$$\left\langle A_0\right|U_{\mathrm{QSVT}}\left|B_0\right\rangle=\mathrm{Poly}\left(\sqrt{\frac{M}{N}}\right)\geqslant 1-\frac{\delta}{2}.$$

用当前态作为输入查询g的结果为0以$1-\delta$的概率成立，当$M\neq k$时：

$$\left\langle A_0 \left| U_{\mathrm{QSVT}} \right| B_0 \right\rangle = \mathrm{Poly}\left(\sqrt{\frac{M}{N}}\right) \leqslant \frac{\delta}{2}.$$

用当前态作为输入查询g的结果为1以$1-\delta$的概率成立.因此，构造的量子电路可以以至少$1-\delta$的概率判断$M=k$是否成立.

3.2　关键引理的证明

本文的目的是证明引理3，该引理说明存在一个期望的多项式$\mathrm{Ploy}(x)$来逼近式(1)中的函数$f(x)$.在此之前，需要使用Low et al.(2017)中的两个引理.

引理1（关于符号函数$\mathrm{sgn}(x)$的整体逼近(Low et al., 2017)[Lemma 10]）　对任意$\Delta>0$，$x\in\mathbb{R}$，$\epsilon\in\left(0,\sqrt{2/(\mathrm{e}\pi)}\right]$，令$l=\frac{\sqrt{2}}{\Delta}\log^{1/2}\left(\frac{2}{\pi\epsilon^2}\right)$.则函数$f_{\Delta,\epsilon}(x)\coloneqq\mathrm{erf}(lx)$满足

$$\left|f_{\Delta,\epsilon}(x)\right|\leqslant 1,\quad \max_{|x|\geqslant\Delta/2}\left|f_{\Delta,\epsilon}(x)-\mathrm{sgn}(x)\right|\leqslant\epsilon.$$

引理2(误差函数$\mathrm{erf}(lx)$的多项式逼近(Low et al.,2017)[Corollary 4])　对任意$l>0$，$\epsilon\in(0,\mathcal{O}(1)]$,可定义奇次幂的多项式$p_{\mathrm{erf},l,n}$:

$$p_{\mathrm{erf},l,n}(x)=\frac{2l\mathrm{e}^{-l^2/2}}{\sqrt{\pi}}\left(I_0\left(l^2/2\right)x+\sum_{j=1}^{(n-1)/2}I_j\left(l^2/2\right)(-1)^j\left(\frac{T_{2j+1}(x)}{2j+1}-\frac{T_{2j-1}(x)}{2j-1}\right)\right),$$

使得

$$\max_{x\in[-2,2]}\left|p_{\mathrm{erf},l,n}(x)-\mathrm{erf}(lx)\right|\leqslant\epsilon,$$①

其中$I_j(x)$表示第一类修正贝塞尔函数，$T_j(x)$表示第一类切比雪夫多项式，

$$n=\mathcal{O}\left(\sqrt{\left(l^2+\log\left(1/\epsilon\right)\right)\log\left(1/\epsilon\right)}\right).$$

现在我们将证明一个引用在定理2证明中的引理.

引理3　我们可以高效地构造一个多项式$\mathrm{Poly}(x)$来逼近以下函数

$$\begin{aligned}f(x)=&\frac{1}{2}\mathrm{sgn}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)+\frac{1}{2}\mathrm{sgn}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)\\&-\frac{1}{2}\mathrm{sgn}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)-\frac{1}{2}\mathrm{sgn}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right),\end{aligned}\tag{3}$$

使得

(i) $\mathrm{Poly}(x)$是奇函数；

(ii) $\mathrm{Poly}(x)$的次数为$\mathcal{O}\left(\sqrt{Nk}\log\left(\frac{12}{\delta}\right)\right)$；

(iii) 当$x\in[-1,1]$时，$\left|\mathrm{Poly}(x)\right|\leqslant 1$；

(iv) 当$x=\sqrt{\frac{M}{N}}$时，$\left|f(x)-\mathrm{Poly}(x)\right|\leqslant\frac{\delta}{2}$.

证明　令$\Delta=\sqrt{\frac{k+1}{N}}-\sqrt{\frac{k}{N}}$，对于每个$\mathrm{sgn}(x\pm c)$(其中$c$指代公式(3)中的常数)，根据引理1和引理2，

① 在Low et al.(2017)中，$x\in[-1,1]$，但是当$x\in[-2,2]$时引理也成立.

存在$f_{\Delta,\epsilon}(x)$和$p_{\mathrm{erf},l,n}$.现在，我们定义以下多项式

$$\begin{aligned}\mathrm{Poly}(x)=&\frac{1}{2(1+2\epsilon)}p_{\mathrm{erf},l,n}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)+\frac{1}{2(1+2\epsilon)}p_{\mathrm{erf},l,n}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)\\&-\frac{1}{2(1+2\epsilon)}p_{\mathrm{erf},l,n}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)-\frac{1}{2(1+2\epsilon)}p_{\mathrm{erf},l,n}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right).\end{aligned}$$

当$x\in[0,1]$时，注意到$x\pm c\in[-2,2]$,因此有

$$\begin{aligned}\mathrm{Poly}(x)\leqslant&\frac{1}{2(1+2\epsilon)}\left(f_{\Delta,\epsilon}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)+\epsilon\right)+\frac{1}{2(1+2\epsilon)}\left(f_{\Delta,\epsilon}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)+\epsilon\right)\\&-\frac{1}{2(1+2\epsilon)}\left(f_{\Delta,\epsilon}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)-\epsilon\right)-\frac{1}{2(1+2\epsilon)}\left(f_{\Delta,\epsilon}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)-\epsilon\right)\\\leqslant&\frac{1}{2(1+2\epsilon)}\left(f_{\Delta,\epsilon}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)+2\epsilon\right)+\frac{1}{2(1+2\epsilon)}\left(f_{\Delta,\epsilon}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)+2\epsilon\right)\\\leqslant&\frac{1+2\epsilon}{2(1+2\epsilon)}+\frac{1+2\epsilon}{2(1+2\epsilon)}=1.\end{aligned}$$

上述第一个小于号是由引理2得出的；第二个小于号是由

$$-f_{\Delta,\epsilon}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)-f_{\Delta,\epsilon}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)\leqslant 0$$

推导出来的，这可以通过引理1中给出的$f_{\Delta,\epsilon}$的表达式进行解析验证；第三个小于号成立是因为根据引理1，$\left|f_{\Delta,\epsilon}(x\pm c)\right|\leqslant 1$.类似地，有

$$\begin{aligned}\mathrm{Poly}(x)\geqslant&\frac{1}{2(1+2\epsilon)}\left(f_{\Delta,\epsilon}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)-\epsilon\right)+\frac{1}{2(1+2\epsilon)}\left(f_{\Delta,\epsilon}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)-\epsilon\right)\\&-\frac{1}{2(1+2\epsilon)}\left(f_{\Delta,\epsilon}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)+\epsilon\right)-\frac{1}{2(1+2\epsilon)}\left(f_{\Delta,\epsilon}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)+\epsilon\right)\\\geqslant&-\frac{1}{2(1+2\epsilon)}\left(f_{\Delta,\epsilon}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)+2\epsilon\right)-\frac{1}{2(1+2\epsilon)}\left(f_{\Delta,\epsilon}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)+2\epsilon\right)\\\geqslant&-\frac{1+2\epsilon}{2(1+2\epsilon)}-\frac{1+2\epsilon}{2(1+2\epsilon)}=-1.\end{aligned}$$

由于 $f_{\Delta,\epsilon}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)+f_{\Delta,\epsilon}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)\geqslant 0$ 可以通过解析验证. 当 $x\in[-1,0]$ 时，可以对称地证明 $\left|\mathrm{Poly}(x)\right|\leqslant 1$. 因此，性质(iii)得到验证.

当 $x=\sqrt{\frac{M}{N}}$ 时，以下条件同时成立：

$$\left|x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right|\geqslant\frac{\Delta}{2},\qquad \left|x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right|\geqslant\frac{\Delta}{2},$$

$$\left|x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right|\geqslant\frac{\Delta}{2},\qquad \left|x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right|\geqslant\frac{\Delta}{2}.$$

因此，有

$$\begin{aligned}\left|f(x)-\mathrm{Poly}(x)\right|&\leqslant\left|(1+2\epsilon)\mathrm{Poly}(x)-\mathrm{Poly}(x)\right|+\left|(1+2\epsilon)\mathrm{Poly}(x)-f(x)\right|\\&\leqslant 2\epsilon+\frac{1}{2}\left|p_{\mathrm{erf},l,n}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)-\mathrm{sgn}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)\right|\\&\quad+\frac{1}{2}\left|p_{\mathrm{erf},l,n}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)-\mathrm{sgn}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k-1}{N}}}{2}\right)\right|\\&\quad+\frac{1}{2}\left|p_{\mathrm{erf},l,n}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)-\mathrm{sgn}\left(x-\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)\right|\\&\quad+\frac{1}{2}\left|p_{\mathrm{erf},l,n}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)-\mathrm{sgn}\left(x+\frac{\sqrt{\frac{k}{N}}+\sqrt{\frac{k+1}{N}}}{2}\right)\right|\\&\leqslant 6\epsilon.\end{aligned}$$

第二个小于号成立是因为：i) $\left|\mathrm{Poly}(x)\right|\leqslant 1$，ii) $\left|p_{\mathrm{erf},l,n}(x)-\mathrm{sgn}(x)\right|\leqslant\left|p_{\mathrm{erf},l,n}(x)-f_{\Delta,\epsilon}(x)\right|+\left|f_{\Delta,\epsilon}(x)-\mathrm{sgn}(x)\right|\leqslant 2\epsilon$. 令 $\delta/2=6\epsilon$，因此，性质(iv)得到证明.

将引理 1 中 l 的表达式代入引理 2，我们可以看出 $\mathrm{Poly}(x)$ 的次数是 $\mathcal{O}\left(\sqrt{\frac{1}{\Delta}}\log\left(\frac{1}{\epsilon}\right)\right)$. 由于 $\Delta=\sqrt{\frac{k+1}{N}}-\sqrt{\frac{k}{N}}\geqslant\sqrt{\frac{1}{(k+1)N}}$，且 $\delta=12\epsilon$，$\mathrm{Poly}(x)$ 的次数是 $\mathcal{O}\left(\sqrt{Nk}\log\left(\frac{12}{\delta}\right)\right)$. 因此，得到了性质(ii).

最后，容易发现 $\mathrm{Poly}(x)$ 是奇函数，这可以通过 $p_{\mathrm{erf},l,n}$ 是奇多项式这一事实直接验证. 因此，证明了性质(i).

3.3 判断一个图中是否存在度数为 k 的顶点

现在我们可以展示用于确定给定图是否存在度数为k的顶点的量子算法.

推论 1 给定一个由N个顶点组成的无向图$G=(V,E)$，可以通过邻接矩阵 Oracle O_G 访问该图，同时给定一个正整数$k>0$.则对于每个顶点$v_i\in V$，存在一个量子算法$\mathcal{A}_i$，使用$\mathcal{O}\left(\sqrt{Nk}\log\left(\frac{12}{\delta}\right)\right)$次对$O_G$的查询，以至少$1-\delta$的概率决定$v_i$的度数是否为$k$.其中$\delta$是给定的概率误差限.

证明 设$g(x)=O_G(v_i,x)$，其中$x\in V$.根据定理2，存在一个量子算法，可以决定v_i的度数是否为k.这时，定理1可以由定理4和推论1推导得出.

注 1 在上述定理中，要求$k>0$.当$k=0$时，我们也可以构造一个消耗$\mathcal{O}(N)$次查询的量子算法.实际上，如果将式(1)替换为$f(x)=\mathrm{sgn}(x)$，则可以通过类似的思路得到$k=0$的算法.

4 结 论

我们提出了一个量子算法，可以在$\mathcal{O}\left(N\sqrt{k}\right)$次查询内解决判断一个$N$个顶点的图中是否存在度数为$k$的顶点的问题，而其经典复杂度为$\Omega(N^2)$.为了完成该算法，我们使用了QSVT技术构建了一个算法，可以在$\mathcal{O}\left(\sqrt{Nk}\right)$次查询内判断$N$个元素的无序数据库中的目标状态数量是否为$k$.需要注意的是，本文研究的图的性质是一种非单调图的性质，而这类性质在量子计算领域中的关注较少.另一个值得进一步研究的相关问题是考虑如何设计量子算法来找到图中具有最大度数的顶点.

参考文献：

AARONSON S，BEN-DAVID S，KOTHARI R，et al，2021. Degree *vs*. approximate degree and quantum implications of Huang's sensitivity theorem[C]//Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing，6 C：1330-1342.

AMBAINIS A，BALODIS K，IRAIDS J，et al，2020. Quantum lower and upper bounds for 2d-grid and Dyck language[C]//45th International Symposium on Mathematical Foundations of Computer Science，8.

BALASUBRAMANIAN R，RAMAN V，SRINIVASARAGAVAN G，1997. Finding scores in tournaments[J]. J Algorithms，24(2)：380-394.

BERETTA L，NARDINI F M，TRANI R，et al，2019. An optimal algorithm to find champions of tournament graphs[C]//International Symposium on String Processing and Information Retrieval：267-273.

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

BUHRMAN H，CLEVE R，de WOLF R，et al，1999. Bounds for small-error and zero-error quantum algorithms[C]//Proceedings of the 40th Annual Symposium on Foundations of Computer Science：358-368.

DEY P，2017. Query complexity of tournament solutions[C]//Proceedings of the Thirty-First AAAI Conference on Artificial Intelligence，31(1)：2992-2998.

GILYÉN A，SU Y，LOW G H，et al，2019. Quantum singular value transformation and beyond：Exponential improvements for quantum matrix arithmetics[C]//Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing：193-204.

GOLDREICH O，2017. Introduction to property testing[M]. Cambridge：Cambridge University Press.

GOYAL D，JAYAPAUL V，RAMAN V，2020. Elusiveness of finding degrees[J]. Discrete Appl Math，286：128-139.

GUTIN G，MERTZIOS G B，REIDL F，2018. Searching for maximum out-degree vertices in tournaments[EB/OL]. arXiv：1801.04702.

HØYER P，MOSCA M，de WOLF R，2003. Quantum search on bounded-error inputs[M]//Baeten J C M，et al，Eds. Automata，Languages and Programming. Heidelberg：Springer，291−299.

KULKARNI R，PODDER S，2015. Quantum query complexity of subgraph isomorphism and homomorphism[EB/OL]. arXiv：1509.06361.

LOW G H，CHUANG I L，2017. Hamiltonian simulation by uniform spectral amplification[EB/OL]. arXiv：1707.05391.

MAGNIEZ F，SANTHA M，SZEGEDY M，2007. Quantum algorithms for the triangle problem[J]. SIAM J Comput，37(2)：413−424.

MARTYN J M，ROSSI Z M，TAN A K，et al，2021. Grand unification of quantum algorithms[J]. PRX Quantum，2(4)：040203.

MONTANARO A，de WOLF R，2016. A survey of quantum property testing[J]. Theory Comput，7：1−81.

ROSENBERG A L，1973. On the time required to recognize properties of graphs：A problem[J]. ACM SIGACT News，5(4)：15−16.

SUN X，YAO A C，ZHANG S，2004. Graph properties and circular functions：How low can quantum query complexity go?[C]// Proceedings of 19th IEEE Annual Conference on Computational Complexity：286−293.

YODER T J，LOW G H，CHUANG I L，2014. Fixed-point quantum search with an optimal number of queries[J]. Phys Rev Lett，113(21)：210501.

（责任编辑　冯兆永）