路径边采样量子算法

Stacey Jeffery[1], Shelby Kimmel[2],和 Alvaro Piedrafita[1]

[1]CWI 和 QuSoft[2]Middlebury College,

skimmel@middlebury.edu

arXiv:2303.03319v1 [quant-ph] 6 Mar 2023

摘要

我们提出了一种量子算法，用于在一个以邻接矩阵表示的无向图中，对两个节点 s和 t之间路径上的边进行采样，并证明其查询复杂度渐近上与检测 s 和 t之间是否存在路径的查询复杂度相同，至多相差对数因子。我们在一些特定情况下，将这种路径采样算法用作st-路径查找和 st-割集查找算法的子程序。我们的主要技术贡献是一种算法，用于生成与跨度程序的正见证向量成比例的量子态。

1 引言

在图中查找和检测两个顶点之间的路径是重要的相关问题，无论就其本身而言，还是作为其他应用中的子程序，都是如此；但这一领域仍有许多尚待理解之处。尽管从经典角度看，这些问题似乎是等价的，一个耐人寻味的问题是，对于量子算法而言是否也同样如此：在某些情况下，量子算法能够在比任何已知量子算法查找一条连接 s 和 t的路径所需时间显著更短的时间内检测到这样一条路径。特别地，粘合树图上的路径查找是 Aaronson 在查询复杂度领域提出的十大开放问题之一 [CCD+03，Aar21], ，因为在这类图中查找一条 st-路径的最佳已知量子算法，其运行时间比检测该路径的最佳量子算法差得多，达到指数级；而理解这些问题之间的关系，或可增进我们对量子计算机为何能在某些问题上实现显著加速的理解。作为一个更具直接实际意义的例子：在超奇异同源图中进行路径查找，是攻击基于超奇异同源的密码系统的一种方法 [CLG07，DJP14], ，但目前已知的此类最佳攻击仍需指数时间 [Tan09] （另见 [GV18]）。

本文研究一个介于两者之间的问题的量子查询复杂度：在无向图中寻找一条 st-路径上的边。[1] 在经典情形下，很难想象如何在不先找到一条 st-路径的情况下，找到一条 st-路径上的边；但我们证明，在量子情形下，只需与检测是否存在一条 st-路径所需资源相近的资源，就可以对一条 st-路径上的边进行采样。在某些情况下，这所需的查询次数显著少于此前已知最佳路径查找算法所需的次数。我们证明，对路径上的边进行采样的能力有一些实用的应用，包括破坏网络（寻找st-割集），以及比现有路径查找算法更快地在某些图中寻找路径。

此前，D¨urr、Heiligman、Høyer 和 Mhalla [DHHM06] 描述了一种在邻接矩阵模型中判定连通性的算法，该算法针对一个有 $O(n^{3/2})$ 个顶点的 n图使用 $O(n^{3/2})$

[1]In 本文中，我们用 $path$ 表示一条自避路径，即一条没有重复顶点的路径 .

次查询。该算法会跟踪已知的连通分量，然后使用量子搜索查找连接此前已知不连通的任意两个分量的边。作者利用此算法判定连通性；我们注意到，经过 s 至 t，该算法将以高概率生成图的连通分量列表，并为每个分量生成一组边，作为该分量连通性的证明（生成树）。如果 s 和t 属于同一分量，就可以利用这些数据找到一条从 s 到 t的路径。此算法使用 $O(\log\ n)$ 个量子比特和 $O(n\log\ n)$ 个经典比特，并适用于有向图和无向图。

然而，D 的算法¨并未利用图中的任何结构。这与 Belovs 和 Reichardt 提出的无向路径检测量子算法形成对比；该算法 [BR12], 在 [JJKP18、ACK+23]中得到了进一步分析和改进。例如，当存在一条长度为 s 、连接顶点 t 和 $\widetilde{O}$的$\sqrt{L}n$-路径时，它可以通过 st次邻接矩阵查询来检测这两个顶点之间是否存在路径；在存在多条较短路径，或在不存在路径时满足某些承诺条件的情况下，效果甚至更好。事实上，对于输入满足足够特定结构的承诺条件，该算法的性能甚至比最佳可能的经典算法 [JK17]高出超多项式倍。尽管在许多情况下，这一路径检测算法比 O $n^{3/2}$运行得更快，但它不会输出有关 st-路径的任何信息——它只判断路径是否存在。

我们的贡献是一种算法，即使对于具有特定结构的输入，也能复现 Belovs-Reichardt 无向路径检测算法的查询复杂度——例如，当存在一条长度为 L 的路径时，我们的算法使用 $\widetilde{O}($ $\sqrt{L}n)$ 次查询——但现在还会返回有关 st-路径上的边的一些信息：即一条路径边。[2] 具体而言，我们的算法会输出一条 st-路径边，其采样概率取决于 s 与 t 之间的最优 st-流。如果将图中的边替换为带电阻器的导线，并在 s 与 t 之间接入电池，这就相当于电子在电网络中的流动情况。直观来说，某条边属于越多条路径，或属于越短的路径，就越可能被采样。因此，当 s 与 t 之间只有一条路径时，我们的算法会以相同的概率采样该路径上的每条边（在全变差距离意义下存在一定误差）。当存在长度不同的不相交路径时，与长路径上的边相比，我们的算法更可能采样短路径上的边——采样一条特定路径的概率与 $1/\ell$ 成正比，其中该路径的长度为 ℓ。（遗憾的是，这意味着如果长路径很多，我们仍可能更有可能采样到某条长路径上的边，而非短路径上的边。）我们证明，即使承诺存在一条长度为 L 的路径，只要 $L \geq 3$，经典地寻找一条 st-路径边在最坏情况下仍需要 $\Omega(n^2)$ 次查询。

凭借快速找到短路径上的边的能力，我们可以设计一种改进算法，用于在具有唯一短 st-路径的无向图中查找 st-路径。给定一个 n顶点图的邻接矩阵，如果存在一条唯一的 st-路径，其长度（可能未知）为 L，我们便能通过 $\widetilde{O}(L^{1+o(1)}n)$ 次期望查询找到该路径上的所有边。当 $L = o(\sqrt{n})$ 时，这优于 D¨urr 等人的算法。在存在多条 st-路径的一般情况下，我们证明，当 L 是最长路径的长度（可能未知）时，可以通过 $\widetilde{O}(L^{3/2}n)$ 次查询找到单条路径上的所有边（不过在这种情况下，我们的方法并未将边采样算法用作子程序）。当 $L = o(n^{1/3})$ 时，这优于 D¨urr 等人的算法。

此外，在 s 和 t 分别属于一个高度连通分量，且连接这些分量的边很少的情况下，我们还利用采样算法查找 st-割集。由于这些为数不多的连接边是流的瓶颈，因此会有大量流经这些边，从而有很高的概率采样到它们，进而找到一个 st-割集。我们描述了一类特定的 n顶点图，在这类图中，我们可以通过 $\widetilde{O}(n)$ 次查询找到这样的割集，而任何经典算法都需要 $\Omega(n^2)$ 次查询。

我们的边采样算法是一个新型基于跨度程序的算法（第3节）的特例，该算法用于生成一种称为跨度程序见证态（或简称见证

[2]正如我们在介绍 Belovs-Reichardt算法在路径较短和/或存在多条路径的情况下的优势时所暗示的，针对 st-路径检测的 Belovs-Reichardt算法，其复杂度实际上以一种更微妙的方式取决于图的结构：它将 L 替换为 s 和 t 之间的上界，而该上界是 s 和 t 之间 *effective resistance* *at most* 最短路径的长度。这种更微妙的分析也适用于我们的边查找算法。

态）。用于判定布尔函数的跨度程序算法分析中的一个关键要素 [Rei11] 是正见证（见定义 2），它是一个向量，用来证明函数在特定输入上的取值为 1。通常的跨度程序算法会在输入 x 上 $f(x)$输出，而在我们的情形中，我们输出一个与输入 x的正见证成比例的量子态。对于用于 st-连通性 [BR12],的 Belovs-Reichardt 跨度程序，正见证是路径 s 和 t之间路径上边的线性组合，其振幅取决于最优 st-流（见定义 4）。生成并测量这样的量子态，即可对 st-路径边进行采样。

我们的结果更一般地适用于输入 x 定义了某个任意图的一个子图 $G(x)$ G的情形，该图不一定是完全图。虽然本文并未尝试分析时间复杂度，但我们推测，如果能够高效地在底层图 G 上进行量子游走（如 [JK17]中所述），那么我们的图查询算法也能达到较高的时间效率。例如，当 G 是一个 n顶点完全图时（也就是说，预言机允许你查询一个 n顶点图的完整邻接矩阵元素，正如我们在本引言中一直假设的那样），就可以高效地进行这种游走。因此，在这种情况下，我们算法的时间复杂度很可能与查询复杂度相同，至多相差对数因子。

1.1 未来方向

一个自然的未来方向是尝试将我们的边查找技术用于比本文所考虑的情形更一般的路径查找问题。我们的算法有一个出人意料之处：它不一定按照边在路径中出现的顺序查找边，而是往往能以较高概率找到路径中间的边。因此，我们算法的形式似乎避开了近期针对粘合树图中路径查找问题提出的一个下界；该下界适用于始终在量子态 [CCG22]中维护一条从起始节点到任意顶点的路径的算法。不过，对于这一特定应用，有一点让我们不太乐观：在粘合树图中，连接起始顶点的所有边都属于某条 st路径。尽管如此，我们仍希望，对于某些图，在某条 st路径中找到中间的一条边，能够为路径查找带来新的分治方法。

我们只能在非常特定的图上利用按照最优st-流进行边采样这一事实，例如只有单条路径的图，或具有瓶颈流的图；不过，我们希望这种边采样分布能在更多应用中发挥作用。在最近独立开展的研究中，Apers 和 Piddock [AP22] 在邻接表模型中开发了一种类似的边采样算法，并用它分析电流与量子游走之间的联系。他们证明，在树上，通过该边采样算法进行的游走只需经过对数级轮次，就能以很高的概率到达目标顶点。我们认为，这类边采样方法很可能会有更多应用。

我们目前只将张成程序见证态生成算法应用于路径检测的张成程序。对于各种图问题，都存在张成程序算法；这些问题包括二分性 [CMB18]和环检测 [CMB18、DKW19], 三角形 [CLM20] 以及其他子图检测 [LMS11], , 还有其他组合搜索问题 [Bel12、BT20]。或许，这些问题的张成程序见证态对某些应用会有帮助。除了张成程序算法之外，对偶对抗算法（对于判定问题，它与跨度程序等价，但可推广到状态转换问题 [LMR+11]）以及多维量子游走 [JZ22、Jef22a] 在其设计和分析中都具有类似的见证概念。类似的技术或许能为这些更一般的算法设计范式带来见证生成算法。

我们怀疑我们的路径查找算法并非最优，因为对于最长路径长度为 $\Omega(n^{1/3})$ 的图，我们的算法并未优于 Dürr 等人的算法。我们想知道，当最长路径长度为 $o(n)$ 时，是否能够使用 $o(n^{3/2})$ 次查询找到路径，或者证明这是不可能的；或许可以通过拓展用于证明下界的技术

焊接树上的路径查找 [CCG22]。

最后，我们的所有算法仅适用于无向图，而 [DHHM06]的算法同样适用于有向图和无向图。虽然已有用于有向图问题的张成程序算法（例如参见 [BT20]），但当路径较短或路径较多时，它们并不能像无向图的张成程序算法那样实现相同的加速。能否通过某些方法在有向图中获得查询复杂度方面类似的改进，将是一个有趣的研究问题。

组织结构。在第3节中，我们介绍主要的技术成果：一种生成与 x 的张成程序见证成比例的量子态的算法。在第4节中，我们展示如何将其应用于查找路径边（第 4.1 节），并给出一个特定图族的例子：在该图族中，查找路径边的经典复杂度比我们的量子算法差一个平方级别（定理 20）。在第4.2节中，我们展示如何将边查找算法应用于在特定图族中高效查找 st-割集；在第4.3节中，我们展示当存在长度为 L 的唯一 st-路径时，如何在 $\widetilde{O}(nL^{1+o(1)})$ 次查询内查找 st-路径（定理 25）；此外，当 L 为最长 st-路径的长度时，还给出一种在一般图中通过 $\widetilde{O}(nL^{3/2})$ 次查询查找 st- 路径的算法（定理 26 ）。

2 预备知识

我们首先介绍一些基本记号。令 $\|\cdot\|$ 表示 l_2 范数，$[m] \coloneqq \{1,2,3,\ldots,m\}$，并令 $\mathcal{L}(H,V)$ 表示从向量空间 H 到向量空间V.的线性算子集合

2.1 跨度程序

跨度程序是一种线性代数计算模型，由 [KW93], 提出，在分析查询 [Rei11、Rei14], 空间 [Jef22b], 以及量子算法中的时间复杂度方面[BR12、CJOP20、BTT22] 已被证明极为有用。我们的定义紧密遵循参考文献 [IJ19] 。

定义1（跨度程序）。对于有限集 R，定义在 R^m 上的跨度程序是一个元组 $\mathcal{P} = (H, \mathcal{V}, |\tau\rangle, A)$，其中

1. H是有限维内积空间的直和：$H = H_1 \oplus H_2 \cdots H_m \oplus H_{true} \oplus H_{false}$，并且对于 $j \in [m]$ 和 $a \in R$，有 $H_{j,\,a} \subseteq H_j$，使得 $\sum_{a \in R} H_{j,\,a} = H_j$ ；
2. $\mathcal{V}$ 是一个向量空间；3.
   $|\tau\rangle \in \mathcal{V}$ 是一个目标向量；以及
4. $A \in \mathcal{L}(H, \mathcal{V})$。

给定一个字符串 $x \in R^m$，我们用 $H(x)$ 表示子空间 $H_{1,\,x_1} \oplus \cdots \oplus H_{m,\,x_m} \oplus H_{true}$，并用 $\Pi_{H(x)}$ 表示投影到空间 $H(x)$上的正交投影算子。

跨度程序分析和量子查询复杂度中的一个重要概念是见证：

定义 2（正见证）。给定一个定义在 R^m 上且具有 $x \in R^m$ 的跨度程序 $\mathcal{P} = (H, \mathcal{V}, |\tau\rangle, A)$，$|w\rangle \in H(x)$ 是 $\mathcal{P}$ 中 x 的一个正见证，如果 $A|w\rangle = |\tau\rangle$。若 x 存在正见证，我们将 $\mathcal{P}$ 中 x 的见证大小定义为

$$w_+(x) = w_+(\mathcal{P}, x) \coloneqq \min\left\{ \||w\rangle\|^2 : |w\rangle \in H(x) \text{ and } A|w\rangle = |\tau\rangle \right\}. \tag{1}$$

我们称 $|w\rangle \in H(x)$ 为 x 的最优正见证，当且仅当 $\||w\rangle\|^2 = w_+(\mathcal{P}, x)$ 且 $A|w\rangle = |\tau\rangle$。

我们的主要算法会生成这个唯一最优正见证 $|w\rangle/\||w\rangle\|$ 的归一化版本。（要证明最优正见证是唯一的，不妨反证，假设最优正见证不唯一——那么两个最优正见证的线性组合会产生一个见证，其见证大小小于其中任意一个。）

跨度程序 $\mathcal{P}$ 以如下方式编码函数 $f\colon\ X \to \{0,1\}$。如果 x 具有正见证，则称 $f(x) = 1$；如果 x 不具有正见证，则称 $f(x) = 0$。我们称这样的 $\mathcal{P}$ 决定了函数 f。

我们还需要近似负见证这一概念。

定义 3（负误差、近似负见证）。给定在 R^m 和 $x \in R^m$ 上的跨度程序 $\mathcal{P} = (H, \mathcal{V}, |\tau\rangle, A)$，我们将 x 在 $\mathcal{P}$ 中的负误差定义为

$$e_-(x,\mathcal{P}) := \min\left\{\|\langle\widetilde{\omega}|A\Pi_{H(x)}\|^2 : \langle\widetilde{\omega}| \in \mathcal{L}(\mathcal{V},\mathbb{R}), \langle\widetilde{\omega}|\tau\rangle = 1\right\}. \tag{2}$$

注意，当且仅当 $\mathcal{P}$ 决定一个函数 f，且具有 $f(x) = 0$ 时，$e_-(x,\mathcal{P}) = 0$。任何满足 $\|\langle\widetilde{\omega}|A\Pi_{H(x)}\|^2 = e_-(x,\mathcal{P})$ 的 $\langle\widetilde{\omega}|$ 都称为 x 在 P 中的近似负见证。我们将 x 的近似负见证大小定义为:

$$\widetilde{w}_-(x,\mathcal{P}) := \min\left\{\|\langle\widetilde{\omega}|A\|^2 : \langle\widetilde{\omega}| \in \mathcal{L}(\mathcal{V},\mathbb{R}), \langle\widetilde{\omega}|\tau\rangle = 1, \|\langle\widetilde{\omega}|A\Pi_{H(x)}\|^2 = e_-(x,\mathcal{P})\right\}. \tag{3}$$

我们称同时使 $\|\langle\widetilde{\omega}|A\|^2$ 最小化的近似负见证 $\langle\widetilde{\omega}|$ 为最优近似负见证。

我们使用以下记号表示最大正见证大小和近似负见证大小s:

$$W_+(\mathcal{P},f) = W_+ := \max_{x\in f^{-1}(1)} w_+(\mathcal{P},x), \qquad \widetilde{W}_-(\mathcal{P},f) = \widetilde{W}_- := \max_{x\in f^{-1}(1)} \widetilde{w}_-(x,\mathcal{P}). \tag{4}$$

请注意，我们将范围限制在 f 的 1 输入上。这是因为我们的见证生成算法会假定 x 是一个 1 输入，而以往用于判定 f 的基于跨度程序的算法则不作此假定。

2.2 Quantum 查询算法

我们所构造的算法都是查询算法，其中可以访问酉预言机 O_x for some $x \in X \subseteq R^m$ such that O_x 作用于空间 $\mathbb{C}^m \otimes \mathbb{C}^q$ 上，形式为 $O_x|i\rangle|a\rangle = |i\rangle|x_i + a \bmod q\rangle$。其中 $q = |R|$，x_i 是 x 的 i^{th} 元素的值，而 $|i\rangle \in \mathbb{C}^m$ 和 $|a\rangle \in \mathbb{C}^q$ 是标准基态。

算法的查询复杂度是指在 $x \in X$的所有可能情况下，最坏情况下必须使用 O_x 的次数。在我们的情形中，我们还将考虑输入 x上的期望查询复杂度，即给定特定输入 x时必须使用 O_x 的平均次数，其中随机性来自算法执行过程中发生的随机事件。

2.3 图论及其与跨度程序的联系

设 $G = (V,E)$ 为一个无向图。[3] 我们将特别考虑顶点带有特殊标记的图 s、$t \in V$，使得在 G. 中存在一条从 s 到 t 的路径。令 $\vec{E} = \{(u,v) : \{u,v\} \in E\}$；也就是说，$\vec{E}$ 是与 G. 的边相对应的有向边集合。给定图 $G = (V,E)$，对于 $u \in V$，我们用 G_u^- 表示 G 在顶点 $V \setminus \{u\}$上的子图；对于 $S \subseteq E$，通过沿用记号，我们用 G_S^- 表示删除了边 S 的 G 的子图。（根据上下文可以明确，我们是在从图中删除边还是顶点。）

在一个具有 G、s 且 t 连通的图上，我们将考虑单位 st-流。它是环和 st-路径的线性组合，形式上定义为 $\vec{E}$ 上满足以下性质的函数。

[3] 我们的结果可轻松推广到多重图，参见 [JJKP18], 但为简洁起见，我们不考虑多重图hs这里。

定义 4（单位 st-流）。设 $G=(V,E)$ 是一个无向图，具有 s、$t\in V(G)$，且 s 和 t 连通。那么，G 上的单位 st-流是一个函数 $\theta\colon \overrightarrow{E}\to\mathbb{R}$，满足：

1. *For all* $(u,v)\in\overrightarrow{E}$, $\theta(u,v)=-\theta(v,u)$;
2. $\sum_{v:(s,v)\in\overrightarrow{E}}\theta(s,v)=\sum_{v:(v,t)\in\overrightarrow{E}}\theta(v,t)=1$; *and*
3. *for all* $u\in V\setminus\{s,t\}$, $\sum_{v:(u,v)\in\overrightarrow{E}}\theta(u,v)=0$.

定义 5（单位流能量）。给定一个图 $G=(V,E)$，以及其上的单位 st-流 θ（位于 G 上），θ 的单位流能量为 $J(\theta)=\frac{1}{2}\sum_{e\in\overrightarrow{E}}\theta(e)^2$.

定义 6（有效电阻）。设 $G=(V,E)$ 是一个包含 $s,t\in V$ 的图。如果 s 和 t 在 G 中连通，则 G 中 s 与 t 之间的有效电阻为 $R_{s,t}(G)=\min_\theta J(\theta)$，其中 θ 遍历 G 的所有单位 st-单位流。如果 s 和 t 在 G 中不连通，则 $R_{s,t}(G)=\infty$.

最优流的解释 能量最小的 st-流是唯一的；如果图表示由单位电阻构成的网络，并且我们在 s 和 t之间施加电势差，那么它描述了流经该边的电流。最小能量流还可以从其他角度解释，并与其他图性质存在联系。为供参考，也为了帮助希望建立对这一概念直觉的读者，我们在 附录 A中汇总了其中一些关系。

图访问 我们通过让字符串 $x\in\{0,1\}^m$指定 G 的一个子图 $G(x)$，将图问题转化为预言机问题。具体而言，我们将每条边 $e\in E$ 与 $[m]$ 中的一个数字关联起来。然后，给定字符串 $x\in\{0,1\}^m$，令 $G(x)=(V,E(x))$ 为 G 的子图：当且仅当 e 与整数 $i\in[m]$ 相关联，且 $x_i=1$ 时，它才包含边 $e\in E$，其中 x_i 是 x 的第 i 个比特。在这个预言机问题中，我们可以访问预言机 O_x，以查询 x（或者在经典情形下，可以逐个查询 x 的比特值）；同时给定母图 G 的描述，以及 x 的比特与 G 的边之间的对应关系。目标是尽可能少地进行查询，以确定有关图 $G(x)$ 的某些信息。令 $E_i\subset E$ 为与 $x.$ 的第 i 个比特相关联的边集。除非另有说明，否则应假设 $m=|E|$，并将 G 的每条边与输入字符串中的一个比特一一对应。在这种情况下，当 G 为完全图时，O_x 等价于对某个图的邻接矩阵进行查询访问。考虑原图的子图（例如 G_u^-）时，除非另有说明，我们假设这些子图中的边沿用原图中的索引。

本文中的大多数应用都与检测s 和 t 之间是否存在路径的问题有关——这通常称为 st连通性。我们定义 st-$\mathrm{CONN}_G(x)$：如果 s 和 t 在 $G(x)$ 中连通，则$=1$，否则为 0。下面的跨度程序记为 $\mathcal{P}_{G_{st}}$，最早由文献 [KW93] 提出，并在量子情形下由文献 [BR12], 使用，用于判定 st-$\mathrm{CONN}_G(x)$：对于图 $G=(V,E)$，其中 $m=|E|$，定义跨度程序 $\mathcal{P}_{G_{st}}$ 如下：

$$\begin{aligned}&\forall i\in[m], H_{i,1}=\mathrm{span}\{|(u,v)\rangle:\{u,v\}\in E_i\}, H_{i,0}=\emptyset\\&\mathcal{V}=\mathrm{span}\{|v\rangle:v\in V(G)\}\\&|\tau\rangle=|s\rangle-|t\rangle\\&\forall(u,v)\in\overrightarrow{E}:\ A|u,v\rangle=|u\rangle-|v\rangle.\end{aligned}\tag{5}$$

对于$\mathcal{P}_{G_{st}}$，负近似见证大小有界于 $\widetilde{W}_-=O(n^2)$ [IJ19]。如果 s 和t 在 $G(x)$中连通，则 x 在$\mathcal{P}_{G_{st}}$中的最优正见证为 [BR12，JJKP18]

$$|\theta^*\rangle=\frac{1}{2}\sum_{e\in\overrightarrow{E}}\theta^*(e)|e\rangle,\tag{6}$$

其中 θ^* 是具有最小能量的 st单位流，因此根据定义 2 和 6， $w_+(\mathcal{P}_{G_{st}}, x) = \frac{1}{2}R_{s,t}(G(x))$。

我们的一个主要应用是将见证态生成算法应用于跨度程序 $\mathcal{P}_{G_{st}}$，在这种情况下，我们生成一个接近 $|\theta^*\rangle/\||\theta^*\rangle\|$ 的量子态，其中 θ^* 是 G 上的最优单位 st-流（x）。如果我们能精确地创建 $|\theta^*\rangle/\||\theta^*\rangle\|$，然后在标准基下测量，那么得到边 e 的概率为 $\theta^*(e)^2/(2R_{s,t}(G(x)))$。令 $q_{G(x),s,t}$ 表示如下分布：对于 $\forall e \in \vec{E}$，

$$q_{G(x),s,t}(e) = \theta^*(e)^2/(2R_{s,t}(G(x))). \tag{7}$$

此外，这个最优流 θ^* 是（自避） st-路径的凸组合，正如我们在 附录A 中所证明的：

引理7. $G(x)$ 中的一条 st-路径是由不同顶点组成的序列 $\vec{u} = (u_0, \ldots, u_\ell)$，满足 $s = u_0$, $t = u_\ell$，且对于所有 $i \in [\ell]$，$(u_{i-1}, u_i) \in \vec{E}(G(x))$。根据 $\vec{u}$，我们定义

$$|\rho_{\vec{u}}\rangle = \frac{1}{\sqrt{2}} \sum_{i=0}^{\ell-1} (|u_i, u_{i+1}\rangle - |u_{i+1}, u_i\rangle) \tag{8}$$

并将所有此类量子态称为 st-路径态，属于 $G(x)$。那么，如果 $|\theta^*\rangle$ 是 $\mathcal{P}_{G_{s,t}}$中用于 x 的最优正见证，它就是 $G(x)$ 中 st-路径态的线性组合。

我们使用的最后一对工具是：一种量子算法，在有效电阻较小时，无需预先知道有效电阻即可用更少的查询来判定 st-$\text{CONN}_G(x)$；以及一种用于估计有效电阻的量子算法：

引理 8 ([ACK+23])。 固定 $\delta > 0$ 以及一族 n 顶点图 G，其顶点为 s 和 t。那么存在一个量子算法 路径检测(O_x, G, s, t, δ) 满足：

1. 该算法以 $1 - O(\delta)$ 的概率返回 st-$\text{CONN}_G(x)$。
2. *On input x, the algorithm uses $O\left(n\sqrt{R_{s,t}(G(x))}\log\left(\frac{n}{R_{s,t}(G(x))\delta}\right)\right)$ expected queries if st-$\text{CONN}_G(x) = 1$, and $O\left(n^{3/2}\log 1/\delta\right)$ expected queries if st-$\text{CONN}_G(x) = 0$.*

引理 9 ([IJ19]) 。固定 $\delta > 0$ 以及一族 n 顶点图 G，其顶点为 s 和 t。那么存在一个量子算法 WitnessSizeEst$(O_x, G, s, t, \epsilon, \delta)$，对于满足 st- $\hat{}\text{CONN}_G(x) = 1$ 的输入 x，以 $1 - \delta$ 的概率输出 $R_{s,t}(G(x))$ 的估计值 R，使得

$$\left|\hat{R} - R_{s,t}(G(x))\right| \leq \epsilon R_{s,t}(G(x)), \tag{9}$$

使用 $\widetilde{O}\left(\sqrt{\frac{R_{s,t}(G(x))n^2}{\epsilon^3}}\log(1/\delta)\right)$ 期望查询次数；对于满足 st-$\text{CONN}_G(x) = 0$ 的输入 x，至多使用 $\widetilde{O}\left((n/\epsilon)^{3/2}\log(1/\delta)\right)$。

引理 9 是 [IJ19 定理 3 的一个特例。8], 该定理给出了一种算法，可利用任意跨度程序估计量 $w_+(x)$。如果我们将这一构造应用于跨度程序$\mathcal{P}_{G_{s,t}}$，就可以估计其正见证大小，这些大小恰好是 $\frac{1}{2}R_{s,t}(G(x))$。[IJ19 定理 3 中描述的算法8] 假设输入是 st-$\text{CONN}_G(x)$ 的一个 1 输入，但很容易对其进行修改，使其无论输入为何，都至多在 $\widetilde{O}\left((n/\epsilon)^{3/2}\log(1/\delta)\right)$ 步后停止，因为 $R_{s,t}(G(x)) \leq n$。按原样表述的算法也只能达到有界误差，但通过重复运行 $\log(1/\delta)$ 次并取中位数估计，可以将成功概率提高到 $1 - \delta$。

3 见证生成

O我们关于生成跨度程序见证态的主要技术结果如下 :

定理 10. 给定一个决定函数的跨度程序 $\mathcal{P}$ f，以及常数 ϵ，δ，存在一个算法（算法 1），其输入为一个预言机 O_x，满足 $f(x) = 1$，且具有最优正见证 $|w\rangle$；该算法输出量子态 $|\hat{}w\rangle/\||\hat{}w\rangle\|$，满足 $\left\||w\rangle/\sqrt{w_+(x)} - |\hat{}w\rangle/\||\hat{}w\rangle\|\right\|^2 \leq O(\epsilon)$，其概率为 $1 - O(\delta)$，并使用 $\widetilde{O}\left(\sqrt{w_+(x)}\,\widetilde{W}_-\log\left(\frac{1}{\delta}\right)\right)$ 次期望查询来调用 ~~O_x~~。

作为比较，跨度程序算法能够以有界误差决定 f，其期望查询复杂度为 $\widetilde{O}\left(\sqrt{w_+(x)}\widetilde{W}_-\right)$，因此定理 10 给出了生成见证量子态的匹配复杂度。正如我们将在第 4.1 节中看到的，对于用于子图 G 上 st- 连通性的跨度程序 $\mathcal{P}_{G_{s,\,t}}$，这意味着我们可以用跨度程序算法判定是否存在 st- 路径所需的相同复杂度，采样一条 st-路径边。

我们的见证态生成算法的一个关键子程序将是量子相位估计。在量子相位估计中，会对作用于希尔伯特空间 $\mathcal{H}_A$ 上的输入态 $|\psi\rangle \in \mathcal{H}_A$ 的酉算子 U 实现受控版本。相对于 U，量子态 $|\psi\rangle$ 可以分解到其特征基中，表示为 $|\psi\rangle = \sum_i \alpha_i|\lambda_i\rangle$，其中 $U|\lambda_i\rangle = e^{i\phi_i\pi}$，我们称 ϕ_i 为量子态 $|\lambda_i\rangle$ 的相位。随后，当以精度 Θ 执行相位估计时，测量得到相位 0 的概率近似为 $\sum_i{}_{:\ |\phi_i|\leq\Theta}\,|\alpha_i|^2$；而测量相位 0 后得到的未归一化态近似为 $\sum_i{}_{:\ |\phi_i|\leq\Theta}\,\alpha_i|\lambda_i\rangle$。换言之，相位估计可用于以一定概率投影到低相位空间（相位小于 Θ），该概率取决于原始量子态在低相位特征态上的振幅大小。对于精度参数 ϵ，在相位估计中使用 U 的次数按 $O\left(\frac{1}{\Theta}\log\frac{1}{\epsilon}\right)$ 级增长。相位估计保证的更严格描述见下文的引理 11。

我们用来证明定理 10 的算法，其基本思路是在量子态 $|\hat{}0\rangle$ 上，使用酉算子 $U(\mathcal{P}, x, \alpha)$ 进行相位估计（该酉算子可通过访问预言机 O_x 实现，并且依赖于跨度程序 $\mathcal{P}$ 和一个正实参数 α）。我们证明，相对于 $U(\mathcal{P}, x, \alpha)$，$|\hat{}0\rangle$ 的特征谱可分解为两个量子态：$|\hat{}0\rangle \oplus \frac{1}{\alpha}|w\rangle$，它是 $U(\mathcal{P}, x, \alpha)$ 的一个 0 相位特征态；以及 $|\psi_{x,\ +}\rangle$，它与 $U(\mathcal{P}, x, \alpha)$ 的低相位空间只有很小的重叠。

如果我们以足够小的精度，对 $|\hat{}0\rangle$ 使用 $U(\mathcal{P}, x, \alpha)$ 进行相位估计，随后如上文所述，测得相位为 0，那么我们就会近似投影到量子态 $|\hat{}0\rangle \oplus \frac{1}{\alpha}|w\rangle$。此后，如果我们进行测量 $\{|\hat{}0\rangle\langle\hat{}0|, I - |\hat{}0\rangle\langle\hat{}0|\}$，并得到测量结果 $I - |\hat{}0\rangle\langle\hat{}0|$，该量子态就会投影到 $|w\rangle$，从而达到预期效果。

接下来，我们需要在选择 α 时进行权衡。当 α 太小时，$|\hat{}0\rangle$ 与 $|\hat{}0\rangle \oplus \frac{1}{\alpha}|w\rangle$ 的张成空间重叠很小，因此在对 $|\hat{}0\rangle$ 使用 $U(\mathcal{P}, x, \alpha)$ 进行相位估计时，我们测得相位为 0 的可能性不高。然而，当 α 过大时，虽然测得相位为 0 并因此获得量子态 $|\hat{}0\rangle \oplus \frac{1}{\alpha}|w\rangle$ 的可能性会很高，但随后测得结果 $I - |\hat{}0\rangle\langle\hat{}0|$ 的可能性会很低。

最佳点是 $\alpha \approx \sqrt{w_+(x)}$，此时我们所需的两个测量结果都有合理的出现概率。由于我们事先不知道 $w_+(x)$，因此必须先估计一个合适的 α 值来使用；我们通过迭代测试越来越大的 α 值来实现这一点。[4] 我们的测试包括：对 $|\hat{}0\rangle$ 执行采用 $U(\mathcal{P}, x, \alpha)$ 的相位估计，并估计测量到相位 0 的概率；我们将证明，这可以估计 $\alpha/\sqrt{w_+(x)}$。

[4] 在 [IJ19] 中有一种类似的算法，可以估计 $w_+(x)$，但它的精度超出了我们的需要。

3.1 定理 10 的证明定理 10

在介绍用于证明定理 10的算法之前，我们先介绍分析中将用到的一些关键概念、引理和定理。

设 $\tilde{H} = H \oplus$ 张成$\{|\hat{0}\rangle\}$，且 $\tilde{H}(x) = H(x) \oplus$张成$\{|\hat{0}\rangle\}$，其中 $|\hat{0}\rangle$ 与 H正交。然后~ ~我们将 $A^\alpha \in \mathcal{L}(H, \mathcal{V})$ 定义为

$$\tilde{A}^\alpha = \frac{1}{\alpha}|\tau\rangle\langle\hat{0}| - A. \tag{10}$$

~ ~ ~ ~设 $\Lambda^\alpha \in \mathcal{L}(H, H)$ 为投影到 A^α 的核上的正交投影，并设 $\Pi_x \in \mathcal{L}(H, H)$~为 $H(x)$ 上的正交投影算子。最后，设 $U(\mathcal{P}, x, \alpha) = (2\Pi_x - I)(2\Lambda^\alpha - I)$。注意，$2\Pi_x - I$ 可以通过两次应用 O_x [IJ19 引理 3.1], 来实现，而 $2\Lambda^\alpha - I$ 无需应用任何 O_x即可实现。

我们将使用参考文献 [MNRS11], 中所述的并行化相位估计；与标准相位估计相比，该方法具有更优的误差界。具体而言，给定一个作用于希尔伯特空间 $\mathcal{H}$ 上的酉算子 U、精度 $\Theta > 0$ 和准确度 $\epsilon > 0$，我们可以构造一个电路 $D(U)$，在 U 上实现 $O(\log \frac{1}{\epsilon})$ 个并行的相位估计电路副本，每个副本的精度为$O(\Theta)$，并分别估计量子态 $|\psi\rangle$ 的单个副本的相位。也就是说， $D(U)$ 作用于空间 $\mathcal{H}_A \otimes ((\mathbb{C}^2)^{\otimes b})_B$，其中 $b = O\left(\log \frac{1}{\Theta} \log \frac{1}{\epsilon}\right)$， A 标记输入态寄存器， B标记存储并行相位估计结果的寄存器。

我们使用电路 $D(U)$ 来检查输入态是否与 U [Kit95、CEMM98、MNRS11] 的低相位本征空间有较大的重叠。为了刻画酉算子 U 的低相位空间，令 $P_\Theta(U$（或在 P_Θ 的含义可由上下文明确时直接写作 U ）表示投影到以下张成空间$\{|u\rangle$ ： $U|u\rangle = e^{i\theta}|u\rangle$ 其中 $|\theta| \leq \Theta\}$ （是 U 的本征相位小于 Θ 的本征空间）。接下来的引理给出了并行相位估计电路 $D(U)$ 的关键性质：

引理 11 ([Kit95、CEMM98、MNRS11])。设 U 是希尔伯特空间 $\mathcal{H}_A$ 上的酉算子，且 Θ、 $\epsilon > 0$。我们称 Θ 为精度，称 ϵ 为准确度。那么存在一个电路 $D(U)$，它作用于空间 $\mathcal{H}_A \otimes ((\mathbb{C}^2)^{\otimes b})_B$，其中 $b = O\left(\log \frac{1}{\Theta} \log \frac{1}{\epsilon}\right)$；并且该电路使用 $O\left(\frac{1}{\Theta} \log \frac{1}{\epsilon}\right)$ 次对U的受控调用。于是，对于任意量子态 $|\psi\rangle \in \mathcal{H}_A$,

1. $D(U)(P_0|\psi\rangle)_A|0\rangle_B = (P_0|\psi\rangle)_A|0\rangle_B$
2. $\|P_0|\psi\rangle\|^2 \leq \|(I_A \otimes |0\rangle\langle 0|_B)D(U)(|\psi\rangle_A|0\rangle_B)\|^2 \leq \|P_\Theta|\psi\rangle\|^2 + \epsilon.$

迭代量子振幅估计是振幅估计的一种稳健版本，通过重复应用振幅估计来获得更优的误差界：

引理12 （迭代量子振幅估计 [GGZW21]）。设 $\delta > 0$ 和 $\mathcal{A}$ 是酉量子电路，使得对于量子态 $|0\rangle$， $\mathcal{A}|\psi\rangle = \alpha_0|0\rangle|\psi_0\rangle + \alpha_1|1\rangle|\psi_1\rangle$。那么存在一种算法，以加性误差 $|\alpha_0|^2$ 估计 δ，且成功概率至少为 $1 - p$，使用$O\left(\frac{1}{\delta}\log\left(\frac{1}{p}\log\frac{1}{\delta}\right)\right)$次对 $\mathcal{A}$和 $\mathcal{A}^\dagger$的调用。

分析跨度程序算法时，一个关键的数学工具是有效谱隙引理：

引理 13 (有效谱隙引理， [LMR+11])。设 Π 和 Λ 为投影，并令$U = (2\Pi - I)(2\Lambda - I)$ 为由它们各自对应的反射相乘得到的酉算子。若 $\Lambda|w\rangle = 0$，则 $\|P_\Theta(U)\Pi|w\rangle\| \leq \frac{\Theta}{2}\||w\rangle\|$.

我们需要以下关于最优正见证与最优负近似见证之间的关系：

定理 14。 [IJ19，定理 2。11] 给定一个跨度程序 $\mathcal{P}=(H,\ \mathcal{V},\ |\tau\rangle,\ A)$，定义在 R^m 和 $x\in R^m$上。若 $|w\rangle$ 是 x 的最优正见证，且 $\langle\widetilde{\omega}|$ 是 x的最优负近似见证，则

$$|w\rangle = w_+(x)\Pi_{H(x)}(\langle\widetilde{\omega}|A)^\dagger. \tag{11}$$

如定理 10后文所述，我们将量子态 $|\hat{0}\rangle$ 分解为两个正交态的线性组合。它们是

$$\begin{aligned}|\psi_{x,0}\rangle =&|\hat{0}\rangle + \frac{1}{\alpha}|w\rangle,\\ |\psi_{x,+}\rangle =&|\hat{0}\rangle - \frac{\alpha}{w_+(x)}|w\rangle,\end{aligned} \tag{12}$$

所以我们可以将 $|\hat{0}\rangle$ 写成

$$|\hat{0}\rangle = a_0|\psi_{x,0}\rangle + a_+|\psi_{x,+}\rangle,\quad \text{where}\quad a_0=\frac{1}{1+\frac{w_+(x)}{\alpha^2}},\qquad a_+=\frac{1}{1+\frac{\alpha^2}{w_+(x)}}. \tag{13}$$

我们首先证明$|\psi_{x,0}\rangle$ 是 $U(\mathcal{P},x,\alpha)$ 的 0 相位特征向量。注意到 $A^\alpha|\psi_{x,0}\rangle = \frac{1}{\alpha}(|\tau\rangle - |\tau\rangle) = 0$（见式 (10)），因此回想起 Λ^α 是到 A^α 的核上的正交投影算子，可得 $\Lambda^\alpha|\psi_{x,0}\rangle = |\psi_{x,0}\rangle$。此外，由于 Π_x 是到 $\tilde{H}(x) = H(x)\oplus$ 张成空间$\{|\hat{0}\rangle\}$上的正交投影算子，因此可知 $\Pi_x|\psi_{x,0}\rangle = |\psi_{x,0}\rangle$；这里我们利用了 $|w\rangle$ 是一个正见证这一点，所以 $|w\rangle\in H(x)$。因此 $U(\mathcal{P},x,\alpha)|\psi_{x,0}\rangle = |\psi_{x,0}\rangle$.

另一方面，当 Θ 和 α 足够小时，$|\psi_{x,\ +}\rangle$ 与 $P_\Theta(U(\mathcal{P},x,\alpha))$ 的重叠很小，如下列引理所示。

引理 15. 若 $\alpha^2\geq 1/\widetilde{W}_-$，则 $\|P_\Theta(U(\mathcal{P},x,\alpha))|\psi_{x,\ +}\rangle\|\leq\Theta\alpha\sqrt{\widetilde{W}_-}$。

证明。 设 $\langle\widetilde{\omega}|$ 是 x 的最优负近似见证（参见 定义 3），并令

$$|v\rangle = |\hat{0}\rangle - \alpha(\langle\widetilde{\omega}|A)^\dagger. \tag{14}$$

利用 定理 14 以及 $\Pi_x|\hat{0}\rangle = |\hat{0}\rangle$这一事实，可得

$$\Pi_x|v\rangle = |\hat{0}\rangle - \alpha\Pi_{H(x)}(\langle\widetilde{\omega}|A)^\dagger = |\hat{0}\rangle - \alpha\frac{|w\rangle}{w_+(x)} = |\psi_{x,+}\rangle. \tag{15}$$

现在我们将证明 $\Lambda^\alpha|v\rangle = 0$。设 $|k\rangle$ 属于 A^α的核，因此 $A^\alpha|k\rangle = 0$。利用 等式 (10) 并重新整理，

$$A|k\rangle = \frac{1}{\alpha}|\tau\rangle\langle\hat{0}|k\rangle. \tag{16}$$

Then

$$\begin{aligned}\langle v|k\rangle &= \langle\hat{0}|k\rangle - \alpha\langle\widetilde{\omega}|A|k\rangle\\ &= \langle\hat{0}|k\rangle - \langle\hat{0}|k\rangle\langle\widetilde{\omega}|\tau\rangle\\ &= 0\end{aligned} \tag{17}$$

其中我们用到了 等式 (14) 和 (16) 以及最优负近似见证的性质。因此 $|v\rangle$ 与 A^α的核中任意元素正交，所以 $\Lambda^\alpha|v\rangle = 0$。

现在我们可以应用引理 13 于 $|v\rangle$，得到:

$$\begin{aligned}\|P_\Theta(U(\mathcal{P},x,\alpha))|\psi_{x,+}\rangle\| &= \|P_\Theta(U(\mathcal{P},x,\alpha))\Pi_x|v\rangle\|\\ &\leq \frac{\Theta}{2}\||v\rangle\|\\ &= \frac{\Theta}{2}\sqrt{1+\alpha^2\widetilde{w}_-(x,\mathcal{P})}\\ &\leq \Theta\alpha\sqrt{\widetilde{W}_-},\end{aligned} \tag{18}$$

其中 t　　在第一行中，我们使用了公式（15），而在最后一行中，使用了我们的假设，即 $\alpha^2\widetilde{W}_- \geq 1$。 □

推论 16. $\|P_0(U(\mathcal{P},x,\alpha))|\psi_{x,+}\rangle\| = 0$。

证明。 应用引理 15 并将 Θ 设为 0。 □

为证明 定理 10，我们分析以下算法：

算法 1： WitnessGeneration$(\mathcal{P}, O_x, \delta, \epsilon)$

输入　　：误差容限 δ，准确度 ϵ，用于判定函数 f 的跨度程序 $\mathcal{P}$，
预言机 O_x

输出：量子态 $|\hat{w}\rangle/\||\hat{w}\rangle\|$，使得对于最优正见证 $|w\rangle$，
x，$\||w\rangle/\sqrt{w_+(x)} - |\hat{w}\rangle/\||\hat{w}\rangle\|\|^2 \leq O(\epsilon)$ 的概率为 $1-O(\delta)$

$\epsilon' \leftarrow$ 最小值$\{\epsilon, 1/96\}$;
$T \leftarrow \left|\text{对数}\sqrt{W_+W_-}\right|$; $p \leftarrow$ 最小值 $\left\{\delta/\text{对数}(W_+W_-)\ 1/\sqrt{W_+\widetilde{W}_-}\right\}$

// 探测阶段
对于 $i=0$ 到 T，执行
　$\alpha \leftarrow 2^i/\sqrt{\widetilde{W}_-}$
　$\hat{a} \leftarrow$ 迭代振幅估计（引理12）估计（概率为
　失败 p 且加性误差为 $1/48$）的寄存器 B 中测量结果 $|0\rangle_B$ 的概率
　当 D（U（$\mathcal{P}$，x，α））（参见引理 11）作用于 $\hat{0}\rangle_A|0\rangle_B$ 误差为 ϵ'，精度
　$\sqrt{\frac{\epsilon'}{\alpha^2\widetilde{W}_-}}$
　如果 $\frac{15}{48} \leq \hat{a}_{48} \leq \frac{35}{48}$，则中断
// 状态生成阶段
对 $j=1$ 到 $\log(1/\delta)$ 执行
　将 $D(U(\mathcal{P},x,\alpha))$ 应用于 $\hat{0}\rangle_A|0\rangle_B$，误差为 ϵ'，精度为 $\sqrt{\frac{\epsilon'}{\alpha^2\widetilde{W}_-}}$
　进行测量，测量结果为 $M = \{(I - |\hat{0}\rangle\langle\hat{0}|)_A \otimes |0\rangle\langle 0|_B\}$，作用于所得结果
　量子态
　如果测量结果为 M，则
　　返回所得量子态
返回“失败”

为了分析 算法 1，我们需要以下引理和推论。在 算法 1中，我们估计执行相位估计后，在 $|0\rangle$　B 寄存器中测得结果 a_0 的概率。在以下引理中，我们证明该概率与式（13）中的相近。

引理 17. 将 $D(U(\mathcal{P},x,\alpha)))$ 应用于输入量子态 ϵ，误差为 $\sqrt{\frac{\epsilon}{\alpha^2\widetilde{W}_-}}$，精度为 引理 11（见此处），对输入量子态 $|\hat{0}\rangle_A|0\rangle_B$ 执行 $\alpha \geq 1/\sqrt{\widetilde{W}_-}$ 后，测量结果 $|0\rangle$ 在 B 寄存器中的概率范围为 $[a_0, a_0+2\epsilon]$.

证明。在整个证明过程中，令 $U = U(\mathcal{P},x,\alpha)$。在我们对 $|\hat{0}\rangle_A|0\rangle_B$ 应用 $D(U)$，其误差为 ϵ、精度为 Θ 后，在寄存器B 中测得 $|0\rangle$ 的概率，根据引理 11 第 2 条，至多为

$$\|P_\Theta(U)|\hat{0}\rangle\|^2 + \epsilon = \|a_0 P_\Theta(U)|\psi_{x,0}\rangle + a_+ P_\Theta(U)|\psi_{x,+}\rangle\|^2 + \epsilon, \tag{19}$$

根据式（13）。现在，$P_\Theta(U)|\psi_{x,0}\rangle$ 和 $P_\Theta(U)|\psi_{x,+}\rangle$ 正交，因为

$$\langle\psi_{x,0}|P_\Theta(U)P_\Theta(U)|\psi_{x,+}\rangle = \langle\psi_{x,0}|\psi_{x,+}\rangle = 0, \tag{20}$$

这里我们用到了 $P_\Theta(U)|\psi_{x,0}\rangle = |\psi_{x,0}\rangle$ 以及 $|\psi_{x,0}\rangle$ 和 $|\psi_{x,+}\rangle$ 彼此正交。接下来从 式（19） 出发，并利用正交条件，使用 $\Theta = \sqrt{\frac{\epsilon}{\alpha^2\widetilde{W}_-}}$，

$$\begin{aligned}
\|P_\Theta(U)|\hat{0}\rangle\|^2 + \epsilon &= a_0^2\|P_\Theta(U)|\psi_{x,0}\rangle\|^2 + a_+^2\|P_\Theta(U)|\psi_{x,+}\rangle\|^2 + \epsilon \\
&\le a_0^2\||\psi_{x,0}\rangle\|^2 + a_+^2\Theta^2\alpha^2\widetilde{W}_- + \epsilon \qquad \text{by Lemma 15, since } \alpha^2\widetilde{W}_- \ge 1 \\
&\le a_0 + a_+^2\epsilon + \epsilon \\
&\le a_0 + 2\epsilon, \qquad (21)
\end{aligned}$$

其中我们用到了 $\||\psi_{x,0}\rangle\|^2 = 1/a_0$ 以及 $a_+ \le 1$ （参见 式（13）） 。

根据 引理 11 第 2 项，应用 $D(U(\mathcal{P}, x, \alpha))$ 于 $|\hat{0}\rangle_A|0\rangle_B$ 后，在寄存器 B 中测得 $|0\rangle$，且误差为 ϵ、精度任意的概率至少为

$$\|P_0(U)|\hat{0}\rangle\|^2 = \|a_0P_0(U)|\psi_{x,0}\rangle + a_+P_0(U)|\psi_{x,+}\rangle\|^2 = a_0^2\||\psi_{x,0}\rangle\|^2 = a_0, \qquad (22)$$

其中我们用到了推论 16。 □

推论 18。 在 算法 1中，如果探测阶段的某次迭代里，迭代振幅估计在 第 4 行 没有失败，并随后在 第 5 行导致中断，那么

$$a_0 \in \left[\frac{1}{4}, \frac{3}{4}\right], \qquad \frac{a_0^2 w_+(x)}{\alpha^2} \in \left[\frac{3}{16}, \frac{1}{4}\right]. \qquad (23)$$

证明。 如果迭代振幅估计在 第 4 行 没有失败，并在第 5 行导致中断，那么我们得到一个估计值 $\hat{a}$，其范围为 $[\frac{15}{48}, \frac{35}{48}]$。因此，由于迭代振幅估计的加性误差为 $1/48$，测得测量结果 $|0\rangle_B$ 的概率范围为 $[\frac{14}{48}, \frac{36}{48}]$。根据 引理 17，同一概率的范围为 $[a_0, a_0 + 2\epsilon']$，所以这两个范围特别地存在重叠。因此，由于我们选择 $2\epsilon'$ 不超过 $1/48$，可得

$$a_0 \in \left[\frac{13}{48}, \frac{36}{48}\right] \subset \left[\frac{1}{4}, \frac{3}{4}\right]. \qquad (24)$$

根据 $a_0 = (1 + \frac{w_+(x)}{\alpha^2})^{-1}$ （参见式（13）），可得出 $\frac{a_0^2 w_+(x)}{\alpha^2} = a_0(1 - a_0)$ 的上述取值范围。 □

现在，我们证明算法 1的主要性能保证，对成功概率和期望查询复杂度进行界定，从而证明定理 10。

定理 10 的证明。令 $U = U(\mathcal{P}, x, \alpha)$，我们分析算法 1。我们首先证明，若探测阶段和状态生成阶段均成功，则该算法会生成所需的量子态。随后，我们将分析这一情况发生的概率，以界定该算法的成功概率。

如果在某次迭代中，迭代振幅估计此前一直未失败，随后本次也未失败，并在第 6 行触发中断，则称探测阶段是成功的；在这种情况下，我们可以应用推论 18。在这些假设下，当我们得到测量结果 $M = (I - |\hat{0}\rangle\langle\hat{0}|)_A \otimes |0\rangle\langle 0|_B$ 时，我们考察一次成功的状态生成阶段的结果。通过测量结果 M 产生的未归一化态 $|\hat{w}\rangle$ 为

$$\begin{aligned}
|\hat{w}\rangle &= (I - |\hat{0}\rangle\langle\hat{0}|)_A \otimes |0\rangle\langle 0|_B D(U)|\hat{0}\rangle_A|0\rangle_B \\
&= a_0(I - |\hat{0}\rangle\langle\hat{0}|)_A D(U)|\psi_{x,0}\rangle_A|0\rangle_B + a_+(I - |\hat{0}\rangle\langle\hat{0}|)_A \otimes |0\rangle\langle 0|_B D(U)|\psi_{x,+}\rangle_A|0\rangle_B \\
&= a_0(I - |\hat{0}\rangle\langle\hat{0}|)_A|\psi_{x,0}\rangle_A|0\rangle_B + a_+(I - |\hat{0}\rangle\langle\hat{0}|)_A \otimes |0\rangle\langle 0|_B D(U)|\psi_{x,+}\rangle_A|0\rangle_B \\
&= \frac{a_0}{\alpha}|w\rangle_A|0\rangle_B + \underbrace{a_+(I - |\hat{0}\rangle\langle\hat{0}|)_A \otimes |0\rangle\langle 0|_B D(U)|\psi_{x,+}\rangle_A|0\rangle_B}_{=:|\xi\rangle}, \qquad (25)
\end{aligned}$$

其中，在最后一个等式中，我们使用了引理 11 第 1 项，因为 $P_0(U)|\psi_{x,\ 0}\rangle = |\psi_{x,\ 0}\rangle$。
我们希望对 Δ 进行界定，其中

$$\begin{aligned}\Delta := \left\| \frac{|\hat{w}\rangle}{\||\hat{w}\rangle\|} - \frac{|w\rangle_A|0\rangle_B}{\sqrt{w_+(x)}} \right\| &= \left\| \frac{\frac{a_0}{\alpha}|w\rangle_A|0\rangle_B + |\xi\rangle}{\||\hat{w}\rangle\|} - \frac{|w\rangle_A|0\rangle_B}{\sqrt{w_+(x)}} \right\| \\ &\le \left| \frac{a_0}{\alpha\,\||\hat{w}\rangle\|} - \frac{1}{\sqrt{w_+(x)}} \right| \||w\rangle\| + \frac{\||\xi\rangle\|}{\||\hat{w}\rangle\|} \qquad \text{根据三角不等式。} \\ &\le \left| \frac{a_0\sqrt{w_+(x)}}{\alpha\,\||\hat{w}\rangle\|} - 1 \right| + \frac{\||\xi\rangle\|}{\||\hat{w}\rangle\|}. \end{aligned} \tag{26}$$

为了界定 $\||\xi\rangle\|$，我们有

$$\begin{aligned}\||\xi\rangle\|^2 = a_+^2 \left\|(I - |\hat{0}\rangle\langle\hat{0}|)_A \otimes |0\rangle\langle 0|_B D(U)|\psi_{x,+}\rangle_A|0\rangle_B\right\|^2 &\le \|I_A \otimes |0\rangle\langle 0|_B D(U)|\psi_{x,+}\rangle_A|0\rangle_B\|^2 \\ &\le \|P_\Theta|\psi_{x,+}\rangle\|^2 + \epsilon' \\ &\le \Theta^2\alpha^2\widetilde{W}_- + \epsilon' \le 2\epsilon', \end{aligned} \tag{27}$$

其中，第一个不等式成立是因为投影只能减小向量的范数，且$a_+ \le 1$；第二个不等式根据 引理 11 第 2 项得出，第三个不等式则来自引理15 以及我们对 Θ的选择。

接下来，为了界定 $\||\hat{w}\rangle\|$，我们对 公式（25）最后一行应用三角不等式，并结合 公式 (27) 得到

$$\frac{a_0\sqrt{w_+(x)}}{\alpha} - \sqrt{2\epsilon'} \le \||\hat{w}\rangle\| \le \frac{a_0\sqrt{w_+(x)}}{\alpha} + \sqrt{2\epsilon'}. \tag{28}$$

根据我们对 ϵ'的选择，我们有 $2\epsilon' \le 1/48$；此外，将 推论 18 应用于 公式（28），可得

$$\frac{1}{4} < \sqrt{3/16} - \sqrt{1/48} \le \||\hat{w}\rangle\| \le \sqrt{1/4} + \sqrt{1/48} < \frac{3}{4}. \tag{29}$$

重新整理公式（28）并应用公式（29），可得

$$\left| \frac{a_0\sqrt{w_+(x)}}{\alpha\,\||\hat{w}\rangle\|} - 1 \right| \le \frac{\sqrt{2\epsilon'}}{\||\hat{w}\rangle\|}. \tag{30}$$

然后将公式（27）、（29）和（30）代入公式（26），得到:

$$\Delta \le \frac{2\sqrt{2\epsilon'}}{\||\hat{w}\rangle\|} < 8\sqrt{2\epsilon'} = O(\epsilon). \tag{31}$$

现在我们分析探测阶段和状态生成阶段均成功、从而得到公式（26）中的量子态 $|\hat{w}\rangle/\||\hat{w}\rangle\|$ 的概率。首先注意到，如果在探测阶段进行足够长时间的迭代，则存在一个 α 的取值，使得只要迭代振幅估计没有失败，我们就会跳出探测阶段。具体而言，当 $w_+(x)/\alpha^2 \in [1/2, 2]$ 时，根据公式（13），有 $a_0 \in [1/3, 2/3]$。因此，根据引理 17，并且由于 $2\epsilon' \le 1/48$，测量结果 $|0\rangle_B$ 的概率属于 $[16/48, 33/48]$；在第 5 行中，如果迭代振幅估计没有失败，这会使我们离开探测阶段。由于在探测阶段的每次迭代中我们都将 α 加倍，使得 $w_+(x)/\alpha^2$ 逐渐减小，而初始时有 $w_+(x)/\alpha^2 = w_+(x)\widetilde{W}_- \ge 1$，因此对于某个 α 该情况必然会发生。[5]

[5]为证明 $w_+(x)\ \widetilde{W}_- \ge 1$，令 $N_+ =$ 最小值$\{\||w\rangle\|^2 :\ A|w\rangle = |\tau\rangle\}$，并令 $N_- =$ 最小值$\{\|\langle\omega|A\|^2 : \langle\omega|\tau\rangle = 1\}$。则$w_+(x)\ \ge N_+$，并且 $\widetilde{W}_- \ge N_-$，根据 [IJ19第 2 节4]，$N_+N_- = 1$。

因此，如果没有发生误差，则经过若干 L 个$\widetilde{\quad}$$\widetilde{\quad}$轮次后，第 5 行的条件将得到满足，其中 $L \in O(\log(w_+(x)W_-)) = O(\log(W_+W_-))$。由于单轮迭代振幅估计失败的概率为$\widetilde{\quad}$ $p \leq \delta/\log(W_+W_-)$（见 第 1 行），因此在第 5 行条件得到满足时离开探测阶段（而不是提前或延后离开）的概率至少为

$$(1-p)^L = 1 - O(\delta). \tag{32}$$

假设我们已成功离开探测阶段且未发生失败，接下来计算在状态生成阶段最多进行 $\log(M)$ 次迭代期间，获得测量结果 $1/\delta$ 的概率。获得测量结果 M 的概率下界为（根据公式（29））

$$\||\hat{w}\rangle\|^2 \geq 1/16. \tag{33}$$

因此，状态生成阶段的成功概率为

$$1 - (15/16)^{\log(1/\delta)} = 1 - O(\delta). \tag{34}$$

结合 公式（32）和（34），我们成功生成公式（26） $|\hat{w}\rangle/\||\hat{w}\rangle\|$中所示量子态的概率为

$$(1-O(\delta))(1-O(\delta)) = 1 - O(\delta). \tag{35}$$

为计算期望查询复杂度，我们首先注意到，如果我们在探测阶段第$t \in \{0, \ldots, \lceil \log \sqrt{W_+} \rceil\}$ 轮终止，则需要使用

$$\begin{aligned} &\sum_{i=0}^{t} O\left(\frac{2^i}{\sqrt{\epsilon}} \log\left(\frac{1}{\epsilon}\right) \log\left(\frac{1}{p}\right)\right) + O\left(\log\left(\frac{1}{\delta}\right) \frac{2^t}{\sqrt{\epsilon}} \log\left(\frac{1}{\epsilon}\right)\right) \\ =&O\left(\frac{2^t}{\sqrt{\epsilon}} \log\left(\frac{1}{\epsilon}\right) \log\left(\frac{1}{p\delta}\right)\right) \end{aligned} \tag{36}$$

次查询，其开销来自在探测阶段截至第 t^{th} 轮的每一轮中，将迭代振幅估计（引理12）应用于相位估计（引理 11）的成本，再加上状态转换阶段中相位估计的成本。

我们在任意轮次终止的概率 t 当我们得到一个估计值 $\hat{a}$ 不在范围 $[\frac{15}{48}, \frac{35}{48}]$内时，至多为 p。利用 公式（36），所有此类轮次对平均查询复杂度的总贡献至多为

$$\sum_{t=0}^{\lceil \log \sqrt{W_+\widetilde{W}_-} \rceil} O\left(p \frac{2^t}{\sqrt{\epsilon}} \log\left(\frac{1}{\epsilon}\right) \log\left(\frac{1}{p\delta}\right)\right) = O\left(p\sqrt{\frac{W_+\widetilde{W}_-}{\epsilon}} \log\left(\frac{1}{\epsilon}\right) \log\left(\frac{1}{p\delta}\right)\right). \tag{37}$$

其中，在求和中我们实际上纳入了所有轮次，而不仅仅是满足当 $\hat{a}$ 不在范围 $[\frac{15}{48}, \frac{35}{48}]$,内的轮次；由于我们是在推导期望查询复杂度的上界，这是可以接受的。

如果我们在某一轮终止， t^*此时 $\hat{a}$处于范围$[\frac{15}{48}, \frac{35}{48}]$,内——当迭代振幅估计在第 4 行未失败，随后在第 5 行触发中断时，就会发生这种情况。根据式 (23)，我们有 $w_+(\alpha^2)^x \in [\frac{1}{3}, 4]$，并且 $2^{t^*} = \alpha\sqrt{\widetilde{W}_-}$因此 $\sqrt{w_+(x)\widetilde{W}_-/2} \leq 2^{t^*} \leq \sqrt{3w_+(x)\widetilde{W}_-}$。由于我们在每次迭代时都将 α 加倍，因此只有常数轮数会使 $\hat{a}$ 落入适当范围内，而且显然可以将任何一轮终止的概率上界为 1。利用式 (36)，这些轮次会增加

$$O\left(\sqrt{\frac{w_+(x)\widetilde{W}_-}{\epsilon}} \log\left(\frac{1}{\epsilon}\right) \log\left(\frac{1}{p\delta}\right)\right) \tag{38}$$

至总期望查询复杂度。

结合公式 (37)和(38)，并利用我们令 p 为 $O\left(1/\sqrt{W_+\widetilde{W}_-}\right)$ (第 1 行，可得期望查询复杂度为

$$O\left(\sqrt{\frac{w_+(x)\widetilde{W}_-}{\epsilon}}\log\left(\frac{1}{\epsilon}\right)\log\left(\frac{1}{p\delta}\right)\right)=\widetilde{O}\left(\sqrt{\frac{w_+(x)\widetilde{W}_-}{\epsilon}}\log\left(\frac{1}{\delta}\right)\right). \tag{39}$$

□

4 图应用

4.1 在一条路径上查找一条边

本节考虑在 $G(x)$中的一条 st-路径上查找一条边的问题，我们将其记为 $st\text{-EDGE}_G(x)$。也就是说，给定对字符串 x 的查询访问，该字符串确定了一个 n顶点图 G的子图$G(x) = (V, E(x))$，如第2.3节所述（若 G 是完全图，则x 只是 $G(x)$的邻接矩阵）；其中 s、$t \in V$ 满足 $G(x)$中至少存在一条从s 到 t 的路径，输出一条位于从 s 到 t的一条（不重复顶点）路径上的边 $e \in E(x)$。

从经典角度看，很难想象这个问题会比查找一条路径容易多少；事实上，在我们的定理 20经典下界中，我们迫使算法先学会一条完整路径，才能找到路径上的任何一条边。然而，我们发现，在量子情况下，当路径较短或存在多条路径时，这个问题比已知的任何路径查找算法都更容易。这为改进某些情况下的量子算法带来了可能性，例如无需了解完整路径的情形，如 st第4.2节的割集算法第4.2节。

定理 19。固定 $p > 0$，以及一个由 s 和 t 个顶点组成的 n-顶点图族 G 。存在一种量子算法（算法 2），以 $1 - O(p)$ 的概率解决 $st\text{-EDGE}_G(x)$，并在输入 x 上使用 $\widetilde{O}\left(\sqrt{R_{s,t}\ G\ x}\right)$ (( )) 次期望查询。更准确地说，该算法以 $1 - O(p)$ 的概率从分布 $\hat{}q$ 中采样，使得 $\hat{}q$ 与 $q_{G(x),s,t}$ 之间的全变差距离为 $O(\sqrt{p})$，其中 $q_{G(x),s,t}(u, v)$（定义于公式 (7)）正比于 $\theta^*(u, v)^2$,，其中 θ^* 是 $G(x)$ 上的最优单位 st-流。

为得到这一结果，我们使用针对 st-连通性的跨度程序 $\mathcal{P}_{G_{st}}$，并借助定义图 $G(x)$ 的预言机 O_x 运行见证态生成算法（算法 1）；该图在 s 与 t 之间有一条路径。成功时，输出将是一个近似正比于最优流态的量子态，即 公式 (6)；根据 引理7，最优流态本身是路径上的边的叠加态。随后，根据 公式 (7)，在标准基下进行测量时，得到边 e 的概率应接近 $q_{G(x),\ s,\ t}(e)$；并且以很高的概率，我们会测得路径上的某条边。

定理 19的证明：我们分析算法 2。

如果$\texttt{WitnessGeneration}(\mathcal{P}_{G_{st}},\ O_x,\ \epsilon,\ \delta)$（见算法 1）未失败，这一事件发生的概率为 $1 - O(\delta) = 1 - O(p)$，那么根据定理 10，

$$|\hat{\theta}\rangle = |\theta^*\rangle/\||\theta^*\rangle\| + |\eta\rangle \tag{40}$$

对于某个 $|\eta\rangle$，使得 $\||\eta\rangle\|^2 = O(\epsilon)$，并由公式 (6)可得，$|\theta^*\rangle = \frac{1}{2}\sum_{e\in\vec{E}}\theta^*(e)|e\rangle$ 其中 θ^* 是 $G(x)$ 中的最优单位 st-流，因此 $\||\theta^*\rangle\| = \sqrt{\mathcal{R}_{s,\ t}(G(x))}$。

令 $P_{E(x),\ s,\ t}$ 表示投影到 $\vec{E}(x)$ 中属于从 s 到 t的（自避）路径 $\hat{}$ 的边集上。当我们在标准基下测量 $|\theta\rangle$ 时，测得此类边的概率是

$$\left\|P_{E(x),s,t}|\hat{\theta}\rangle\right\| \geq \left\|P_{E(x),s,t}|\theta^*\rangle/\||\theta^*\rangle\|\right\| - \left\|P_{E(x),s,t}|\eta\rangle\right\| = 1 - O(\sqrt{\epsilon}), \tag{41}$$

算法 2：边查找器(O_x, p, G, s, t)

输入 ：故障容忍度 $p > 0$，图 $G(x)$ 的预言机 $O_x = (V, E(x))$，$s, t \in V$ 使得存在一条从 s 到 t的路径。

输出：一个输出 e，或“失败”，使得以概率 $1 - O(p)$，e 是一条边位于一条从 s 到 t的路径上。

$\epsilon \leftarrow p^2$；$\delta \leftarrow p$

$|\hat{\theta}\rangle \leftarrow$ `WitnessGeneration`$(\mathcal{P}_{G_{st}}, O_x, \epsilon, \delta)$ (算法 1)

如果 $\hat{\theta}\rangle \neq$ “失败”则

  $e \leftarrow$测量 $|$的结果 $\hat{\theta}\rangle$ 在标准基中

返回“失败”

其中我们使用了三角不等式，以及以下事实：$P_{E(x),\ s,\ t}|\theta^*\rangle = |\theta^*\rangle$，根据引理7。继续可得概率

$$\left\| P_{E(x),s,t}|\hat{\theta}\rangle \right\|^2 \geq \left(1 - O(\sqrt{\epsilon})\right)^2 = 1 - O(\sqrt{\epsilon}). \tag{42}$$

因此，测量路径上的边的总成功概率为 $(1-O(\delta))(1-O(\sqrt{\epsilon}))$。由于我们令 ϵ 为 p^2，并令 δ 为 p，因此总成功概率为 $1 - O(p)$。

令 $\hat{q}$ 为 算法 2的输出分布。根据全变差距离与迹范数之间的关系，我们有 $d(\hat{q}, q_{G(x),s,t})$，$\hat{q}$ 与 $\hat{q}_{G(x),s,t}$之间的全变差距离至多为 $|\theta\rangle$和 $|\theta^*\rangle/\||\theta^*\rangle\|$ 的迹范数（参见例如 [NC10]），因此

$$\begin{aligned} d(\hat{q}, q_{G(x),s,t}) &\leq \sqrt{1 - \left|\langle\hat{\theta}|\theta^*\rangle / \||\theta^*\rangle\|\right|^2} \\ &= \sqrt{1 - \left|\langle\hat{\theta}|\hat{\theta}\rangle - \langle\hat{\theta}|\eta\rangle\right|^2} \\ &\leq \sqrt{1 - \left(1 - \||\eta\rangle\|\right)^2} \\ &\leq \sqrt{2\,\||\eta\rangle\|} = O(\epsilon^{1/4}) = O(\sqrt{p}). \end{aligned} \tag{43}$$

根据 定理 10，`WitnessGeneration`的期望查询复杂度，因此 算法 2的期望查询复杂度为

$$\widetilde{O}\left(\sqrt{\frac{w_+(x)\widetilde{W}_-}{\epsilon}}\log\left(\frac{1}{\delta}\right)\right) = \widetilde{O}\left(\frac{\sqrt{R_{s,t}(G(x))n}}{p}\right) \tag{44}$$

其中我们用到了以下事实：对于 $\mathcal{P}_{G_{st}}$，$w_+(x) = R_{s,\ t}(G(x))$，且 $\widetilde{W}_- = O(n^2)$ [BR12，IJ19]；并令 ϵ 为 p^2，且令 δ 为 p，如 算法 2所示。 □

我们可以利用 定理 19证明量子算法与经典算法在路径上寻找边的查询复杂度之间存在如下分离：

定理 20. 设 $G = (V, E)$ 中有 $s, t \in V$个顶点，是一个完全图，并且已知 $G(x)$ 中存在一条长度为 L 的路径，该路径连接 s 和 t，其中 L 可能依赖于 x，且不必预先知道。于是，对于输入 x，$st\text{-}\mathrm{EDGE}_G(x)$ 可通过 $\widetilde{O}(n\sqrt{L})$ 次量子查询求解（期望值），而任何经典算法的查询复杂度均为 $\Omega(n^2)$。

证明。对于量子算法，我们应用 定理 19，其出错概率有界为$p = \Omega(1)$，并利用以下事实：$R_{s,\ t}(G) = O(L)$。

对于经典下界，我们将以下问题归约到路径边查找问题：给定一个由 $N = 2^\ell$ 个比特组成的字符串 x，$(x_\sigma)_{\sigma\in\{0,1\}^\ell}$，满足存在唯一的 σ^* 使得 $x_{\sigma^*} = 1$，输出 σ^*_1。

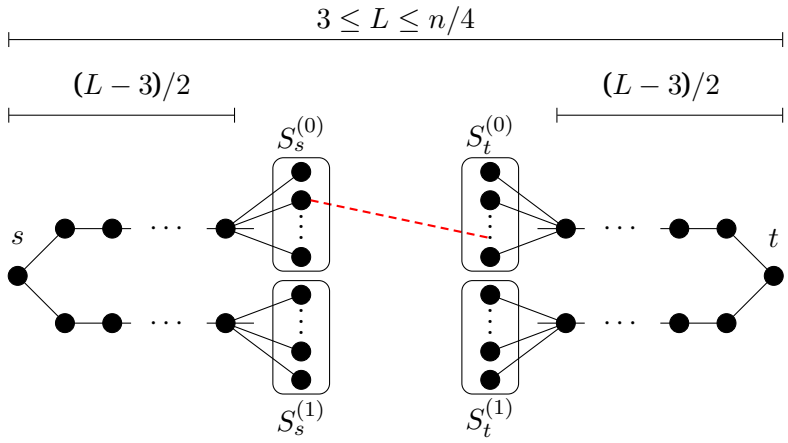


图1：实线黑线表示对于任意 x， $G(x)$ 中存在的边。此外，$G(x)$ 还包含一条连接 $S_s^{(b)}$ 中的一个顶点与 $S_t^{(b)}$ 之间的单边，其中 $b = \sigma_1^*$，如虚线红边所示，从而形成一条长度为 L 的单条路径。

也就是说，我们希望输出 x 中唯一一个值为 1 的比特的索引的第一位。通过类似于标准 OR 下界的对抗论证，该问题的有界错误随机查询复杂度为 $\Omega(N)$。我们将展示如何使用路径边查找算法，在类似于 图1 所示的图上解决该问题。

对于 $x \in \{0,1\}^N$，令 $G(x)$ 为一个包含 $n = \Theta(2^{\ell/2})$ 个顶点的图，其中存在一条长度为 L 的唯一 st-路径，对某个奇数 L 而言如图 1 所示。顶点 s 通过一条长度为 $(L-3)/2$ 的路径连接到一个顶点，该顶点还与一组 $2^{(\ell-1)/2}$ 个顶点相连，$S_s^{(0)} = \{u_{0,\sigma} : \sigma \in \{0,1\}^{(\ell-1)/2}\}$。以对称方式， s 也通过另一条长度为 $(L-3)/2$ 的不相交路径连接到一个顶点，该顶点还与一组 $2^{(\ell-1)/2}$ 个顶点相连，$S_s^{(1)} = \{u_{1,\sigma} : \sigma \in \{0,1\}^{(\ell-1)/2}\}$。同样地， t 通过一对长度为 $(L-3)/2$ 的不相交路径连接到一对顶点，这两个顶点分别还与 $S_t^{(0)} = \{v_{0,\sigma} : \sigma \in \{0,1\}^{(\ell-1)/2}\}$ 和 $S_t^{(1)} = \{v_{1,\sigma} : \sigma \in \{0,1\}^{(\ell-1)/2}\}$ 相连。到目前为止描述的所有边（图1中的黑色边）在 $G(x)$ 中始终存在（我们通过直接输出 1 来模拟查询相关的输入位）。现在描述其在 $G(x)$ 中是否存在由 x 决定的边。对于 $b \in \{0,1\}$，$u_{b,\sigma} \in S_s^{(b)}$ 与 $v_{b,\sigma'} \in S_t^{(b)}$ 中的每一对顶点之间都存在一条潜在的边，标签为 $x_{b\sigma\sigma'}$，这意味着其中恰有一条存在于 $G(x)$ 中——即具有 $\sigma^* = b\sigma\sigma'$ 的那条边。所有其余可能的边在 $G(x)$ 中均不存在（我们通过直接输出 0 来模拟查询其相关的输入位）。

我们可以通过在 $G(x)$ 上运行边查找算法，找到 σ^* 的第一位。假设输出正确，则有以下几种可能：

1. 如果算法输出的是图中间部分的一条边，那么它必定是标记为 x_{σ^*} 的那条边，因此可以完整获知 σ^*。2. 如果算法输出的是图左侧的一条边，那么它位于某个 $b \in \{0,1\}$ 所对应的 s 与 $S_s^{(b)}$ 之间的一条路径上，并且我们知道 $\sigma_1^* = b$。3. 如果算法输出的是图右侧的一条边，那么它位于某个 $b \in \{0,1\}$ 所对应的 t 与 $S_t^{(b)}$ 之间的一条路径上，并且我们知道 $\sigma_1^* = b$。

在所有情况下，我们都已知晓 σ_1^*。这为路径边查找给出了下界 $\Omega(N) = \Omega(2^\ell) = \Omega(n^2)$。

□

4.2 寻找 st-割集

给定一个图 $G(x)$，其中包含一条从 s 到 t的路径， st-割集是图 $G(x)$ 中的一个边集；从图 $G(x)$ 中移除这些边后，从 s到 t便不再存在路径。 st-割集问题就是寻找一个 st-割集。该问题可用于检测网络中的薄弱点，以便找出如何增强网络；反之，也可用于破坏网络。

我们首先注意到，对于只有一条 st-路径的图，定理 19 可立即用于寻找一个 st-割集，因为路径上的任意一条边都是一个 st-割集。不过，我们也可以分析更复杂的情况，例如以下情形：我们已知图的有效电阻上界，并且知道经过 st该 st-割集中任意一条边的最优单位流的下界：

定理 21. 对于函数 $R, g\colon \mathbb{N} \to \mathbb{R}_{>0}$，设 $G = (V, E)$（其中 $s, t \in V$）是一个由 n-顶点图组成的族，并且额外保证 $R_{s,t}(G(x)) \leq R(n)$，且存在一个st-割集 $C \subseteq E(x)$，使得对于每个 $\{u, v\} \in C$, $\theta^*(u, v)^2 \geq g(n)$，其中 θ^* 是 $G(x)$ 中的最优单位st-流。那么存在一个量子算法，以有界误差输出一个集合 C'，使得 $C \subseteq C'$，且其最坏情况查询复杂度为 $\widetilde{O}\left(\frac{R(n)^2 n}{g\ n}()^{3/2}\right)$。

不妨假设 C 在定理 21中是一个极小 st-割。虽然我们无法保证 C' 是定理 21中提到的算法输出的集合是极小的，但只要它包含 st，它仍然是一个 C-割，因为移除它会断开 s和 t。

为了证明定理 21，我们将采用下面这个著名的“集邮问题”的变体。

引理 22。考虑在有限集 $\mathcal{S}$ 上反复对随机变量 Z 进行采样。设 $C \subseteq \mathcal{S}$ 满足对每个 $e \in C$, $\mathbf{Pr}[Z = e] \geq B$。设 T 为在采到 C 的每个元素至少一次之前，采样 Z 所需的次数。则 $\mathbb{E}[T] = O\left(\frac{\log |C|}{B}\right)$。

证明。对于 $i \in \{1, \ldots, |C|\}$，在已经收集了 $i-1$ 个元素后， Z 是 C 中一个新元素的概率为 $p_i \geq (|C| - (i-1))B$。设 T_i 为在采样了 C 的 $(i-1)$ 个元素后，直到采到 C 的 i 个元素所需的采样次数，因此 T_i 是一个几何随机变量，其

$$\mathbb{E}[T_i] = 1/p_i \leq ((|C| - (i-1))B)^{-1}. \tag{45}$$

由此我们可以计算

$$\mathbb{E}[T] = \sum_{i=1}^{|C|} \mathbb{E}[T_i] \leq \sum_{i=1}^{|C|} \frac{1}{(|C| - (i-1))B} = \frac{1}{B} \sum_{j=1}^{|C|} \frac{1}{j} = \Theta\left(\frac{\log |C|}{B}\right). \tag{46}$$

□

定理 定理 21的证明。 我们使用参数 T' 和 ϵ，稍后将对其进行定义，以及 $\delta = 1/4$。我们的策略是反复运行 $\texttt{WitnessGeneration}(\mathcal{P}_{G_{st}}, O_x, \epsilon, \delta)$（算法 1），生成一个近似见证态，然后在标准基下测量所得量子态，以获得一条边 e，并将其加入 C'。我们重复此过程 T' 次，然后输出 C'。

令 Z 为定义在 $E \cup \{\text{失败}\}$ 上的随机变量，表示调用一次算法 1的测量输出。我们设定 $\epsilon = \Theta\left(\frac{g_{(n)}}{R(n)}\right)$ 足够小，使得若算~~法未~~失败，我们就能生成一个量子态 $|\theta^*\rangle / \||\theta^*\rangle\| + |\eta\rangle$ 其中 $\||\eta\rangle\|^2 \leq g(n)/R(n)$（见公式 (40) 及其后的讨论）。那么，在标准基下测量时采样到一条边 $e' \in C$ 的概率为

$$\begin{aligned} \left\| \langle e' | \left(|\theta^*\rangle / \||\theta^*\rangle\| + |\eta\rangle \right) \right\|^2 &= \|2\theta^*(e') / \sqrt{R_{s,t}(G(x))} - \langle e'|\eta\rangle\|^2 \\ &\geq \|2\sqrt{g(n)/R(n)} - \sqrt{g(n)/R(n)}\|^2 \\ &= \Omega(g(n)/R(n)). \end{aligned} \tag{47}$$

调用一次算法 1 不失败的概率为 $1-\delta=\Omega(1)$，因此，对于每个 $e'\in C$，我们有 $\Pr[Z=e']\geq B$ 对于某个 $B=\Omega(g(n)/R(n))$。因此，根据引理 22，在 算法 1 之前调用算法的期望次数至多为： $C\subseteq C'$

$$\mathbb{E}[T]=O\left(\frac{R(n)}{g(n)}\log|C|\right)=O\left(\frac{R(n)}{g(n)}\log n\right). \tag{48}$$

根据马尔可夫不等式，如果我们设定 $T'=100\mathbb{E}[T]$，该算法就会以有界误差成功。根据定理 10，每次调用算法 1 的期望查询复杂度为

$$\widetilde{O}\left(\sqrt{\frac{R_{s,t}(G(x))n^2}{\epsilon}}\right)=\widetilde{O}\left(n\sqrt{\frac{R(n)}{g(n)/R(n)}}\right)=\widetilde{O}\left(\frac{nR(n)}{\sqrt{g(n)}}\right), \tag{49}$$

因此，期望查询复杂度总计为

$$\widetilde{O}\left(T'\frac{nR(n)}{\sqrt{g(n)}}\right)=\widetilde{O}\left(\frac{R(n)}{g(n)}\frac{nR(n)}{\sqrt{g(n)}}\right)=\widetilde{O}\left(\frac{nR(n)^2}{g(n)^{3/2}}\right). \tag{50}$$

我们可以将算法运行的步数限制为期望步数的 100 倍，从而得到最坏情况算法：如果算法届时仍在运行，就停止算法并输出当前的 C'。在这种情况下，我们无法保证 C' 正确，但根据马尔可夫不等式，这种情况发生的概率仅为$1/100$。

□

我们可以利用定理 21 证明以下结果：在一类具有扩张子图且含有一条单独 st-割边的图中，寻找一个 st-割集。

推论 23。设 $G=(V,E)$ 是一个由 n 个顶点的图构成的图族，其中 $s,t\in V$，并且另外承诺 $G(x)$ 由两个互不相交的、 d-正则（对于 $d\geq 3$）且具有常数扩张率的子图组成，每个子图包含 $n/2$ 个顶点； s 和 t 总是位于不同的子图中，此外还有一条连接这两个子图的额外边。那么，存在一个量子算法~，能够以有界误差在最坏情况下通过 $O(n)$ 次查询找到 st-割边；而任何经典算法的查询复杂度均为 $\Omega(n^2)$。

证明。对于经典算法，即使该算法完全了解这两个子图，连接它们的边仍有 $\Omega(n^2)$ 个可能位置，因此问题可归约为搜索，需要 $\Omega(n^2)$ 次查询。

注意，对于量子算法，在一个 d-正则（对于 $d\geq 3$），具有常数扩张性质且包含 n个顶点的图中，任意两点之间的最大有效电阻为 $O(1/d)$ [CRR+96]。因此$R_{s,\,t}(G(x))=\Omega(1)$。此外，由于连接两个子图的边只有一条， e', $\theta^*(e')$ 上最优的单位 st-流必定等于 1。

应用定理 21 并取 $R(n)=O(1)$ 和 $g(n)=\Omega(1)$，可得最坏情况下有界的~量子查询复杂度误差 $O(n)$。

□

4.3 路径查找

本节考虑在 $G(x)$ 中寻找一条 st-路径的问题，记作 st-PATH$_G(x)$。也就是说，给定对字符串 x 的查询访问，该字符串确定了一个 n 顶点图 G 的子图 $G(x)=(V,E(x))$，如第 2.3 节所述（如果 G 是完全图，则 x 只是 $G(x)$ 的邻接矩阵）；其中 $s,t\in V$ 满足：在 $G(x)$ 中， s 与 t 之间至少存在一条路径。输出一条从 s 到 t 的路径。路径是由不同顶点组成的序列 $\vec{u}=(u_0,\ldots,u_\ell)$，满足 $s=u_0$，
$t=u_\ell$ $i\in[\ell]$ u_{i-1} u_i G x ，并且对于所有 ，
(，) $\in\vec{E}$(( ))。

为解决 st-PATH$_G$，我们或许会认为，只需多次运行 算法 2 ，记录每条边的端点，并识别已找到边的端点所对应的顶点，以缩小图的规模，直到找到一条路径。然而，这种算法可能会遇到一些挑战

从而导致运行时间较长。例如，在存在许多 st-路径的图中，算法可能会花费过多时间从不同路径中采样边，而不是集中精力完成单条路径。对于只有一条 st-路径的情况，这种策略则无法利用这样一个事实：一旦找到路径上的一条边，问题就会简化为两个连通性子问题（分别从 s 到已找到的边，以及从 t 到已找到的边），而这两个子问题的查询复杂度通常都远低于原问题。

因此，我们设计了两种算法，使我们能够证明比文献 [DHHM06] 针对最长 st-路径较短的情形所给出的更紧的期望查询复杂度界：一种适用于单条st-路径的情形，另一种适用于一般图。

在介绍用于路径检测的量子算法之前，我们先给出以下推论。通过将路径边查找归约到路径查找，该推论由 定理 20得出，并刻画了最长 st-路径较短时路径查找的经典查询复杂度：

推论 24. 设 $G=(V,E)$ 是一个具有 $s,t\in V$ 个顶点的 n 完全图，并假设已知 $G(x)$ 在 s 和 t 之间存在一条长度为 L 的路径，其中 $L\in[3,n/4]$ 。则 st-$\mathrm{PATH}_G(x)$ 的随机化查询复杂度为 $\Omega(n^2)$。

4.3.1 具有单条路径的图

当已知图 $G(x)$ 具有一条单独的 st-路径时，我们将使用分治算法来查找该路径。为了说明分治方法的实用性，我们首先考虑上述较为简单的算法：该算法使用 定理 19 来查找路径上的一条边 $\{u,v\}$；找到该边后，算法将在一个新图上运行，其中顶点 u 和 v 被合并。该过程持续进行，直到找到边 $\{s,t\}$ 。因此，如果路径的初始长度为 L，找到一条边后，路径长度将变为 $L-1$，随后在下一轮迭代中变为 $L-2$，依此类推。忽略误差，并假设算法在每一轮中都能找到一条边，根据 定理 19，第 i 轮的查询复杂度将为 $\widetilde{O}(n\sqrt{L-i})$。 在这 L 轮中，总查询复杂度将为

$$\sum_{i=0}^{L-1}\widetilde{O}(n\sqrt{L-i})=\widetilde{O}\left(nL^{3/2}\right). \tag{51}$$

对于 $L\geq n^{2/3}$，该算法甚至不如最佳经典算法；而对于$L\geq n^{1/3}$，它也不如参考文献 [DHHM06] 中的量子算法。

我们转而考虑以下分治方法，具体描述见算法 3。我们使用算法 2 来找出一个边集，其中一些边很可能位于路径上。然后，我们使用引理 8 来验证这些边中哪些确实位于路径上，并使用引理 9 确保选择一条靠近路径中心的边，这样便得到两个大小约为原来一半的子问题。最后，我们进行两次递归调用，分别找出从 s 到所找到的边的唯一路径，以及从 t 到所找到的边的唯一路径。

定理 25. 设 $p\geq 0$，并令 $G=(V,E)$ 满足 $s,t\in V$，构成一族具有 n 个顶点的图；假设已知 $G(x)$ 中包含一条长度为 L 的单一路径（ L 可能依赖于 x，且无需预先知道）。那么，存在一种量子算法（算法 3），它以概率 $1-O(p)$ 求解 st-$\mathrm{PATH}_G(x)$，并在输入 x 上使用 $\widetilde{O}(nL^{1+o(1)}\log^2(1/p))$ 次期望查询。

证明。 我们首先分析出错概率，然后在假设没有发生误差的情况下证明 算法 3 的正确性，最后分析查询复杂度。

我们将在进行 $O(n)$ 次递归调用后停止该算法。由于每次递归调用都会返回一条边，且任意路径的长度至多为 n，因此这种终止方式不会影响成功概率。接着，我们通过证明每次递归调用中的失败概率为 $O(p/n^5)$，将出错概率限定为 $O(p/n^4)=O(p)$。

算法 3：SinglePathFinder(O_x, p, G, s, t)

输入 ：故障容忍度 $p > 0$，图 $G(x) = (V, E(x))$ 的预言机 O_x，$s, t \in V$ 使得从 s 到 t 存在唯一路径。

输出：以概率 $1 - O(p)$，得到一个边集，其顶点构成一条从 s 到 $G(x)$ 中的 t。

// 基本情形

若 $s = t$，则返回 $\emptyset$

若 $\{s, t\} \in E(x)$，则 返回 $\{s, t\}$

// 寻找路径上的可能边

$\varepsilon_1 \leftarrow \frac{1}{\text{记录 } n}$ // 任意满足多对数倒数(n)的 $\varepsilon_1 = o(1)$ 均可

$S \leftarrow \emptyset$

$\ell \leftarrow \frac{2\log(n^5/p)}{\varepsilon_1}$ 对于 $i = 1$ 到 ℓ，执行

  $e \leftarrow$ 边查找器(O_x, ε_1, G, s, t) (算法 2)

  如果 $e \neq$ “失败”且 $e = (u, v) \in \overrightarrow{E(x)}$ 然后 $S = S \cup \{(u, v), (v, u)\}$

// 查找实际位于路径上的可能边

$\delta \leftarrow p/(\ell n^5)$

对于 $(u, v) \in S$ 执行

  初始化路径检测($O_x, G^-_{\{u,v\}}, s, u, \delta$) （引理 8）

  初始化路径检测($O_x, G^-_{\{u,v\}}, v, t, \delta$)

$flag \leftarrow$ 真

当标志为真时循环执行

  并行运行前一个 for 循环中初始化的每个路径检测算法，直到每个算法执行 O_x 一次或终止（对于那些算法则什么也不做此前已终止）

  对于 $(u, v) \in S$ 执行

    如果路径检测($O_x, G^-_{\{u,v\}}, s, u, \delta$) 和路径检测($O_x, G^-_{\{u,v\}}, v, t, \delta$) 有两者都在此 while 循环迭代中终止，并且随后都检测到了路径

      $\varepsilon_2 \leftarrow \sqrt{\varepsilon_1}$, $\varepsilon_3 \leftarrow 2\sqrt{\varepsilon_1}$

      $\tilde{k} \leftarrow$见证大小估计($O_x, G, s, u, \varepsilon_2, \delta$) (引理 9) // 距离估计。 s to u

      if $|\tilde{k} - L/2| \leq \varepsilon_3 L$ 然后

        $(u^*, v^*) \leftarrow (u, v)$

        $flag \leftarrow$ 假

// 递归调用

返回 $\{(u^*, v^*)\} \cup$ SinglePathFinder(O_x, p, G, s, u^*) $\cup$ SinglePathFinder(O_x, p, G, v^*, t)

如果出现以下任一情况，我们就称（某次递归调用中）发生了失败：

1. 至多 4ℓ 个路径检测算法中有一个出错。根据我们对 $\delta = p/(\ell n^5)$ 的选择，发生这种情况的概率为 $O(\ell\delta) = O(p/n^5)$。 2. 至多 $O(\ell)$ 次对见证大小估计的调用中，有一次给出的估计未达到所需的相对误差要求。发生这种情况的概率为 $O(\ell\delta) = O(p/n^5)$。 3. 边查找器的 ℓ 次迭代均未找到一条位于 st-路径上、且距路径中点不超过 $(\varepsilon_3 - \varepsilon_2)L = \sqrt{\varepsilon_1}L$ 的边。只要见证大小估计也成功，就足以保证不会发生这类失败，从而满足第 20 行中的条件。

在假设前两种情况均未发生的条件下，我们来分析最后一种情况发生的概率。令 e_0、……、e_{L-1}依次表示唯一 st-路径 $G(x)$ 上的路径边。对于 ℓ 次边查找器EdgeFinder运行，每次输出“失败”的概率为 ε_1。在边查找器EdgeFinder的输出不是“失败”的条件下，根据定理 19，我们从一个分布 $\hat{q}$ 中抽样，该分布与 $\sqrt{\varepsilon_1}$-路径上的边的均匀分布之间的全变差距离为 st。因此，我们抽到集合中的一条边的概率为

$$R = \{e_k : k \in [L/2 - (\varepsilon_3 - \varepsilon_2)L, L/2 + (\varepsilon_3 - \varepsilon_2)L]\}, \tag{52}$$

其中 e_k 是 k^{th} 路径边，即：

$$\hat{q}(R) \geq \frac{|R|}{L} - \sqrt{\varepsilon_1} = 2(\varepsilon_3 - \varepsilon_2) - \sqrt{\varepsilon_1} = 2(2\sqrt{\varepsilon_1} - \sqrt{\varepsilon_1}) - \sqrt{\varepsilon_1} = \sqrt{\varepsilon_1}. \tag{53}$$

因此，利用 $\varepsilon_1 \leq 1/2$，每个 ℓ 样本都是正确范围内的路径边的概率至少为（$1 - \varepsilon_1$）$\sqrt{\varepsilon_1} \geq \sqrt{\varepsilon_1}/2$， R。利用霍夫丁界，它们都不是正确范围内路径边的概率至多为：

$$e^{-2\ell(\sqrt{\varepsilon_1}/2)^2} = e^{-\ell\varepsilon_1/2} = e^{-\log(n^5/p)} = O(n^{-5}p) \tag{54}$$

根据我们对 $\ell = 2\log(n^5/p)/\varepsilon_1$的选择。单轮中的失败总概率至多为$O$（$p/n^5$）。

我们通过对 L（路径长度）进行归纳法来证明正确性，并假设没有发生失败。对于基本情形，如果 $L = 0$ 或 $L = 1$，我们将在第 1 行和第 2 行正确地返回该路径。

对于归纳情形，令 $L' \geq 1$。我们假设 SinglePathFinder 对所有满足 $0 \leq L \leq L'$的长度 L 都能正确工作。现在考虑一个具有 $L = L' + 1$. 的图。那么，假设没有发生失败，我们将至少采样到集合 $R = \{e_k$中的一条边（u， v）： $k \in [L/2 - (\varepsilon_3 - \varepsilon_2)L$、$L/2 + (\varepsilon_3 - \varepsilon_2)L]\}$（否则就会发生上述列表第 3 项所述类型的失败）。接着，如果 PathDetection 算法没有误差，当（u， v）对应于路径上的一条边，且 u 更靠近 s 、 v 更靠近 t时，第 16 行就会满足。这是因为运行 PathDetection 时，我们已从图中移除了$\{u, v\}$；又由于存在唯一的 st-路径，因此只会有一条从 s 到 u 的路径，而不会有从 s到 v的路径；对 t也同样如此。

然后，对于每条我们通过路径检测正确判断为位于一条路径上的边 (u, v)，我们应用见证大小估计（见引理 9）来估计 $R_{s,\,u}(G(x))$。如果 $(u, v) = e_k$，那么e_0， $\ldots, e_{k-1}$ 就是 G 中唯一的 su-路径，其长度为 k，因此 $R_{s,\,u}(G(x)) = k$，所以见证大小估计实际上是在估计 k。假设 $(u, v) \in R$（并且我们知道至少有一条这样的边满足这一条件），则有 $|k - L/2| \leq (\varepsilon_3 - \varepsilon_2)L$。接着，由于我们假设见证大小估计~不会失败，它会输出一个对 k 的估计值 k，使得 $|k - k| \leq \varepsilon_2 k \leq \varepsilon_2 L$。综合起来，这些~条件意味着 $|k - L/2| \leq \varepsilon_3 L$，从而触发 while 循环终止。我们可能会因一条不属于 R 的边而跳出循环，但至少我们知道，只要没有发生失败，就一定会因一条位于该路径上的边 (u^*, v^*) 而跳出 while 循环。

现在我们已经找到了边 $(u^*,\ v^*)$，要找到路径的其余部分，只需分别找出从 s 到 u^* 以及从 v^* 到 t的其余路径。但这两个问题的路径长度都介于 0 和 L'之间，因此根据归纳假设，第 23 行 中的递归调用将是正确的，并会返回这些路径上的边。

接下来分析期望查询复杂度，我们首先界定发生失败时对期望查询复杂度的贡献。正如刚才所述，失败发生的概率为 $O(p/n^4)$。即使发生失败，我们对边查找器、路径检测和见证大小估计的每次调用，其期望查询复杂度仍至多为 $\widetilde{O}(n^{1.5}(1/\varepsilon_1 + 1/\varepsilon_2^{3/2})\log(1/\delta)) = O(n^2\log(1/p))$，而这些调用总共有 $O(n\log(n/p)) = O(n^2\log(1/p))$ 次（对于任意 x），因此总查询开销为 $O(n^4\log^2(1/p))$。因此，错误情形对期望查询复杂度的贡献额外增加 $O(p\log^2(1/p)) = O(1)$。

接下来，假设没有发生失败，我们为期望查询复杂度建立一个递推关系。令 $\mathbb{E}[T_L]$ 表示在一个有 算法 3 作用于一个有 n 个顶点的图上，且图中只有一条路径、该路径长度为 L时的期望查询复杂度。对于 $k \in \{0,\dots,L-1\}$，令 $\tilde{q}_L(k)$ 表示我们找到的路径边 $(u^*,\ v^*)$ 为 e_k的概率。由于我们假设没有子程序˜ ˜调用失败，因此可以假设 k 是 k 的估计值，且相对误差为 ε_2，因此 $|k-k| \le \varepsilon_2 k \le \varepsilon_2 L$。˜根据 第 20 行中的条件语句，我们还得到 $|k - L/2| \le \varepsilon_3 L$。综合以上结果可得：

$$|k - L/2| \le (\varepsilon_2+\varepsilon_3)L = (\sqrt{\varepsilon_1}+2\sqrt{\varepsilon_1})L = 3\sqrt{\varepsilon_1}L. \tag{55}$$

因此，可以确定（假设没有发生失败），我们将以 $(u^*,v^*) = e_k$ 退出 while 循环，其中 $k \in [(1/2-3\sqrt{\varepsilon_1})L,\ (1/2+3\sqrt{\varepsilon_1})L]$，所以：

$$\begin{aligned}\mathbb{E}[T_L] = \widetilde{O}(\ell n\sqrt{L}/\varepsilon_1) + \widetilde{O}(\ell n\sqrt{L}\log(1/\delta)) + \widetilde{O}\left(\ell\frac{n\sqrt{L}}{\varepsilon_2^{3/2}}\log(1/\delta)\right) \\ + \sum_{k=\lceil(1/2-3\sqrt{\varepsilon_1})L\rceil}^{\lfloor(1/2+3\sqrt{\varepsilon_1})L\rfloor} \tilde{q}_L(k)\left(\mathbb{E}[T_k] + \mathbb{E}[T_{L-k-1}]\right),\end{aligned} \tag{56}$$

其中前三项分别来自：(1) 运行 边查找器 (算法 2，定理 19)ℓ 次；(2) 至多 $O(\ell)$ 个并行 路径检测 (引理 8) 算法；以及 (3) 运行见证大小估计(引理 9) $O(\ell)$ 次；最后一项则来自两次递归调用。

为了得到一个关于 L 严格递增的函数，令 $T'_L :=$ 最大值$_{k\le L}\,\mathbb{E}[T_k]$，因此特别有$\mathbb{E}[T_L] \le T'_L$，且 T'_L 也满足 式 (56) (其中以 $=$ 替换 $\le$)。那么，对于任意 $k \in [(1/2-3\sqrt{\varepsilon_1})L,\ (1/2+3\sqrt{\varepsilon_1})L]$，

$$\mathbb{E}[T_k] + \mathbb{E}[T_{L-k-1}] \le 2T'_{(1/2+3\sqrt{\varepsilon_1})L}. \tag{57}$$

因此，接续 式（56），并使用 $1/\varepsilon_1 = \log\, n$和 $1/\varepsilon_2 = 1/\sqrt{\varepsilon_1} = \sqrt{\log n},\quad \ell = 2\log(n^5/p)$ $/\varepsilon_1 = O(\log(1/p)\log^2 n)$, and $\log(1/\delta) = O(\log(\ell n/p)) = \log(1/p)\mathrm{polylog}(n,\ \log(1/p))$，可得

$$\mathbb{E}[T_L] \le T'_L \le \widetilde{O}\left(n\sqrt{L}\log^2(1/p)\right) + 2T_{(1/2+3\sqrt{\varepsilon_1})L}. \tag{58}$$

为了分析这个递推关系，我们将每次递归调用中进行的查询次数相加。在递归层级 i^{th}，有 2^i 次递归调用，每次调用本身会进行 $\widetilde{O}\left(n\sqrt{L/b^i}\log^2(1/p)\right)$次查询，其中 $b = (1/2+3\sqrt{\varepsilon_1})^{-1}$，然后再继续递归。因此

$$\begin{aligned}\mathbb{E}[T_L] &\le \widetilde{O}\left(n\sqrt{L}\log^2(1/p)\right) + \sum_{i=1}^{\log_b L} 2^i\sqrt{\frac{L}{b^i}}\cdot\widetilde{O}\left(n\log^2(1/p)\right) \\ &\le \widetilde{O}\left(n\sqrt{L}\log^2(1/p)\right) + \widetilde{O}\left(n\sqrt{L}\log^2(1/p)\right)\left(2/\sqrt{b}\right)^{\log_b L}.\end{aligned} \tag{59}$$

令 $\eta := \frac{1}{1+\frac{1}{6\sqrt{\varepsilon_1}}} = O(1/\sqrt{\log n})$，因为 $\varepsilon_1 = 1/\log n$，所以 $b = 2(1-\eta)$，我们有：

$$\begin{aligned}\log\left(2/\sqrt{b}\right)^{\log_b L} &= \left(1-\frac{1}{2}\log b\right)\frac{\log L}{\log b} = \left(\frac{1}{\log b}-\frac{1}{2}\right)\log L \\ &= \left(\frac{1}{1-\log\frac{1}{1-\eta}}-\frac{1}{2}\right)\log L = \left(\frac{1}{2}+\frac{\log\frac{1}{1-\eta}}{1-\log\frac{1}{1-\eta}}\right)\log L \qquad (60)\\ \text{so } \left(2/\sqrt{b}\right)^{\log_b L} &= L^{\frac{1}{2}+o(1)},\end{aligned}$$

这里我们用到了 $\log\frac{\frac{1}{1-\eta}}{1-\log\frac{1}{1-\eta}} = o(1)$，因为 $\log\frac{1}{1-\eta} = o(1)$，这可由 $\eta = o(1)$ 得出。因此，接着 式 (59)，我们有：

$$\mathbb{E}[T_L] = \widetilde{O}\left(n\sqrt{L}\log^2(1/p)\right)L^{\frac{1}{2}+o(1)} = \widetilde{O}\left(nL^{1+o(1)}\log^2(1/p)\right). \qquad (61)$$

□

我们注意到，尽管我们在 定理 25 中的方法优于在 式 (51)中分析的较简单、非分治算法，但对于 [DHHM06]的图而言，当 $L = \Omega(n^{1/2-o(1)})$ 时，其表现不如参考文献中的算法。因此，可以运行 算法 3，直到进行 $O\left(n^{3/2}\right)$ 次查询；如果此时还没有找到路径，则切换到参考文献 [DHHM06]中的算法。

4.3.2 任意图中的路径查找

对于更一般的情形，即 st-PATH$_G(x)$，当 $G(x)$ 不确定是否只有一条 st-路径时，尽管类似于 算法 3 的算法可能可行，但我们尚无法有效地界定其运行时间。这是因为，对于单条路径的情形，一旦找到该路径上的一条中间边，从 s 和 t 到该边的最长路径必定短于从 s 到 t的最长路径。这确保了子问题的耗时短于原问题。对于多条路径的情形，我们不再能保证这一点。

不过，我们提供了另一种方法，虽然速度不如 算法 3快，但仍优于 [DHHM06] 所提出的算法，适用于所有从 s 到 t 的（自避）路径都很短的图。我们的方法不将路径边采样算法用作子程序，而是使用 引理 8 中的路径检测算法，判断路径是否经过各种子图，然后利用这些信息，按顺序找出路径上的每条边，从 s 到 t. 。这样，我们就避免了子问题规模大于原问题的问题，因为如果从 s 到 t 的最长路径长度为 L，且我们在路径上找到的第一条边是（s，u），那么从 u 到 t 且不经过 s 的最长路径长度至多为 $L-1$. 。不过，我们失去了分治方法的优势。

为了找到路径上的第一条边，我们采用群测试方法。我们将 G 中 s 的邻居分成两组，S_1 和 S_2，并在 G 的两个子图上并行运行路径检测算法（x）：一个子图删除了来自 s 的边，但保留通向 S_1 中顶点的边（即 $G^-_{\{\{s,u\}\in E:\ u\in S_1\}}$）；另一个子图删除了来自 s 的边，但保留通向 S_2 中顶点的边。我们将检测这两个子图中哪一个包含路径，由此便能知道存在一条路径，其第一条边从 s 指向相应集合（S_1 或 S_2）中的某个顶点。然后，我们再将该集合二等分并重复这一过程，直到将集合缩小到只剩一个顶点 u；该顶点必定是从 s 到 t. 的一条路径上的第一个顶点。

此时，我们已经找到了从 s 到 t 的路径上的第一条边。接着考虑 G^-_s，它是移除顶点 s 后得到的 G，并递归地重复这一过程，以找到第一条边

一条从 u到 t的路径上。

算法 4： GeneralPathFinder(O_x, G, s, t, p)

输入 ：故障容忍度 p，图 $G(x) = (V, E(x))$ 的预言机 O_x， $s, t \in V$使得从 s 到 t存在一条路径。

输出：以概率 $1 - O(p)$，一系列边，其顶点构成一条路径从 s 到 t的 $G\ (x)$

$\delta \leftarrow p/\ (n^4 \log n)$

// 基本情形

如果 $s = t$，则返回 $\emptyset$

// 查找从 s 到 t的路径中的第一条边

S、$E_s \leftarrow \{\{s, v\} :\ \{s, v\} \in E\}$

当 $|S| > 1$ 时

  将 S 划分为两个大小近似相等且不相交的集合： S_1 和 S_2

  并行运行以下两个算法，使得由其执行的查询

  在任何时刻两个算法执行的查询数相差不超过 1，直到其中一个输出 1

  - 路径检测($O_x, G^-_{E_s \setminus S_1}$ $s,\ t,\ \delta$) （引理 8）
  - 路径检测($O_x, G^-_{E_s \setminus S_2}$ $s,\ t,\ \delta$) (引理 8)

  如果 $G^-_{E_s \setminus S_1}$ 算法输出 1，则

    $S \leftarrow S_1$

  else

    $S \leftarrow S_2$

  如果 *PathDetection*调用的输出均不是 1，则返回“失败”

返回 $((s, u))$ $\frown$ GeneralPathFinder(O_x, G^-_s, u, t, p) // $\frown$ 表示序列连接

定理 26。设 $p \geq 0$ 和 $G = (V, E)$（其中 $s, t \in V$）是一族 n-顶点图，并假设已知在 $G(x)$ 中存在一条从 s 到 t 的路径。对于输入 x，如果 $G(x)$ 中最长的 st-路径长度为 L （L 无需预先知道），则存在一个量子算法（算法 4），以 $1 - O(p)$ 的概率返回一条路径上的边，并使用 $\widetilde{O}(nL^{3/2}\log(1/p))$ 次期望查询。

我们注意到，算法 4 在以下情况下的表现不如参考文献 [DHHM06] 中的算法：图的参数为 $L > n^{1/3}$。因此，可以先运行此算法，直到执行 $O\left(n^{3/2}\right)$ 次查询；如果仍未找到路径，则切换到参考文献 [DHHM06]中的算法。

证明。我们首先分析 算法 4的出错概率。在算法运行过程中，将进行 $O(n)$ 次递归调用（因为每次递归调用都会返回一条边）。我们将出错概率限制为 $O(p/n^3) = O(p)$，方法是证明每次递归调用的失败概率为 $O(p/n^4)$。

如果 $O(\log n)$ 次 PathDetection 调用中任意一次失败，我们就认为递归调用发生了错误。根据我们对 $\delta = p/(n^4 \log n)$ 的选择，每次调用的失败概率为 $O(p/(n^4 \log\ n)$，因此所有这些调用均成功的概率为

$$(1 - O(p/(n^4 \log n))^{O(\log n)} = 1 - O(p/n^4), \tag{62}$$

因此，至少有一次调用失败的概率为 $O(p/n^4)$，而任意一次调用失败的概率为$O(p/n^3)$。

即使在失败的情况下，该算法的期望查询复杂度也至多为$O(n^3 \log(1/p))$，因为在整个过程中，最多会调用 PathDetection $O(n\log\ n)$ 次

算法，每次调用的期望查询复杂度为 $O(n^{3/2}\log(n/p))$（对于 任意 x）。因此，在错误情形下，算法 4 对期望查询复杂度的总体贡献至多为 $O((p/n^3)n^3\log(1/p)) = O(1)$。

因此，我们可以在假设没有发生错误的情况下，分析算法 4 的期望查询复杂度。当 s 与 t 之间的最长路径长度为 L 时，并行运行的两个路径检测子程序中至少有一个的期望查询复杂度为$\widetilde{O}(n\sqrt{L}\log(1/\delta))$。这是因为，只要没有发生错误，长度至多为 L 的路径的第一条边必定包含在 S_1 或 S_2 中，因此两个并行子程序中必有一个存在路径；它将在经过 $\widetilde{O}(n\sqrt{L}\log(1/\delta))$ 次期望查询后终止，因为对于任意 G'，$R_{s,\,t}(G')$ 都不超过 G' 中任意 st-路径的长度。

令 $\mathbb{E}[T_L]$ 表示当 算法 4 中的所有 st-路径在 $G(x)$ 中的长度至多为 L时的期望查询复杂度。则期望查询复杂度满足以下递推关系：

$$\mathbb{E}[T_L] = \widetilde{O}(n\sqrt{L}\log(1/p)) + \mathbb{E}[T_{L-1}], \qquad T_0 = O(1). \tag{63}$$

$\widetilde{O}(n\sqrt{L}\log(1/p))$ 来自对路径检测进行的 $O(\log\ n)$ 次迭代，每次迭代的期望查询复杂度至多为 $\widetilde{O}(n\sqrt{L}\log(1/\delta)) = \widetilde{O}(n\sqrt{L}\log(1/p))$。求解此递推关系可得：

$$\mathbb{E}[T_L] = \widetilde{O}(nL^{3/2}\log(1/p)). \tag{64}$$

最后，我们通过归纳最长路径的长度，证明 s 到 t 之间的路径不存在任何误差时，算法 4 的正确性。对于基本情形，如果 $L = 0$，我们将在第 2 行正确返回该路径。

对于归纳情形，令 $k \geq 0$，并假设`GeneralPathFinder`对于所有从 s 到 t 的最长路径长度为 L的图都能正确运行，其中 $0 \leq L \leq k$。现在考虑一个包含$L = k + 1$. 那么，只要 $2\lceil$个 $n\rceil$ 次路径检测在第 6 行的迭代都没有失败，我们就会找到一条边 $\{s, u\}$，它位于一条从 s 到 t的路径上。这是因为在第 6 行的每次迭代中，我们都会找到一个顶点集，并且知道其中包含从 s之后的第一个顶点（路径上的第二个顶点），该路径从s 到 t。每次迭代中，我们掌握这一信息的顶点集大小都会减半，直到集合中只剩下一个顶点；它必定是路径上 s之后的下一个顶点。

一旦找到路径的第一条边 $\{s, u\}$，我们就有了一个新问题：在移除了ut的图上寻找一条 s 路径。不过，由于从 s 到 t 的最长路径至多为 L，因此从 u 到 t 且不经过 s 的最长路径至多为 $L - 1$。所以，根据归纳假设，`GeneralPathFinder` 在第 7 行中的递归调用会正确执行；该调用在移除了顶点 ut的图上寻找一条 s 路径。 □

致谢 我们感谢 Jana Sot´akov´a 和 Mehrdad Tahmasbi 就通过边采样进行路径查找展开了富有见地的讨论。SK 和 SJ 的研究由美国陆军研究办公室资助，本研究是在资助编号 W911NF-20-1-0327 项目下完成的。本文件所载观点和结论均为作者所有，不应被解读为代表美国陆军研究办公室或美国政府明示或暗示的官方政策。尽管本文中有任何版权声明，美国政府仍有权为政府用途复制和分发重印本。SJ 获得 NWO Klein 项目（项目编号 OCENW.Klein.061）以及欧盟（欧洲研究委员会、ASC-Q、101040624）的支持。然而，文中表达的观点和意见仅代表作者本人，并不一定反映欧盟或欧洲研究委员会的立场。欧盟和资助机构均不对此承担责任。SJ 是量子信息科学项目的 CIFAR 研究员。

参考文献

[Aar21] Scott Aaronson。与量子查询复杂度相关的开放问题。《ACM 量子计算汇刊》，2(4):1–9，2021。1[ACK+23] Noel T. Anderson、Jay-U Chung、Shelby Kimmel、Da-Yeon Koh 和 Xiaohan Ye。简单输入上的量子查询复杂度改进。arXiv 预印本 arXiv:2303.00217，2023。2，7[AP22] Simon Apers 和 Stephen Piddock。精灵、树与量子游走。arXiv 预印本 arXiv:2211.16379，2022。3[Bel12] Aleksandrs Belovs。用于 k-重态判定的基于学习图的量子算法。载于第 53 届计算机科学基础年度研讨会论文集（FOCS 2012），第 207–216 页。IEEE，2012。3[BR12] Aleksandrs Belovs 和 Ben W. Reichardt。用于 st-连通性和爪检测的跨度程序与量子算法。载于第 20 届欧洲算法研讨会论文集（ESA 2012），第 193–204 页。Springer，2012。2，3，4，6，16[BT20] Salman Beigi 和 Leila Taghavi。基于经典决策树的量子加速。《Quantum》，4:241，2020。3，4[BTT22] Salman Beigi、Leila Taghavi 和 Artin Tajdini。基于决策树的时间与查询最优量子算法。《ACM 量子计算汇刊》，3(4):1–31，2022。4[CCD+03] Andrew M. Childs、Richard Cleve、Enrico Deotto、Edward Farhi、Sam Gutmann 和 Daniel A. Spielman。量子游走带来的指数级算法加速。载于第 35 届 ACM 计算理论年度研讨会论文集（STOC 2003），第 59–68 页，2003。1[CCG22] Andrew M. Childs、Matthew Coudron 和 Amin Shiraz Gilani。量子算法与遗忘能力。arXiv 预印本 arXiv:2211.12447，2022。3，4[CEMM98] Richard Cleve、Artur Ekert、Chiara Macchiavello 和 Michele Mosca。重新审视量子算法。《伦敦皇家学会会刊 A 辑：数学、物理与工程科学》，454(1969):339–354，1998。9[CJOP20] Arjan Cornelissen、Stacey Jeffery、Maris Ozols 和 Alvaro Piedrafita。跨度程序与量子时间复杂度。载于第 45 届数学基础国际研讨会论文集（MFCS 2020），第 26:1–26:14 页，2020。4[CLG07] Denis X. Charles、Kristen E. Lauter 和 Eyal Z. Goren。基于扩展图的密码学哈希函数。《密码学杂志》，22:93–113，2007。1[CLM20] Titouan Carette、Mathieu Lauri`ere 和 Fr´ed´eric Magniez。用于三角形查找的扩展学习图。《Algorithmica》，82(4):980–1005，2020。3[CMB18] Chris Cade、Ashley Montanaro 和 Aleksandrs Belovs。用于环检测和二分性测试的时间与空间高效量子算法。《量子信息与计算》，18(1-2):18–50，2018。3[CRR+96] Ashok K. Chandra、Prabhakar Raghavan、Walter L. Ruzzo、Roman Smolensky 和 Prasoon Tiwari。图的电阻刻画了其往返时间和覆盖时间。《计算复杂性》，6(4):312–340，1996。19

[DHHM06] Christoph D¨urr、Mark Heiligman、Peter Høyer 和 Mehdi Mhalla。《若干图问题的量子查询复杂度》。SIAM 计算杂志，35(6):1310–1328，2006。1, 4, 20, 24, 25[DJP14] Luca De Feo、David Jao 和 J´ero ˆme Plˆut。《基于超奇异椭圆曲线同源构建抗量子密码系统》。数学密码学杂志，8:209–247，2014。1[DKW19] Kai DeLorenzo、Shelby Kimmel 和 R. Teal Witter。《 st-连通性量子算法的应用》。载于第14届量子计算、通信与密码学理论会议（TQC 2019）论文集，莱布尼茨国际信息学会议录（LIPIcs）第135卷，第6:1–6:14页，2019。3[GGZW21] Dmitry Grinko、Julien Gacon、Christa Zoufal 和 Stefan Woerner。《迭代量子振幅估计》。npj 量子信息，7(1):52，2021年3月。9[GV18] Steven D. Galbraith 和 Frederik Vercauteren。《超奇异椭圆曲线同源中的计算问题》。量子信息处理，17(265)，2018。1[IJ19] Tsuyoshi Ito 和 Stacey Jeffery。《近似跨度程序》。Algorithmica，81(6):2158–2195，2019。4, 6, 7, 8, 9, 10, 13, 16[Jef22a] Stacey Jeffery。《量子子程序组合》。arXiv 预印本 arXiv:2209.14146，2022。3[Jef22b] Stacey Jeffery。《跨度程序与量子空间复杂度》。计算理论，18(1):1–49，2022。4[JJKP18] Michael Jarret、Stacey Jeffery、Shelby Kimmel 和 Alvaro Piedrafita。《连通性及相关问题的量子算法》。载于第26届欧洲算法研讨会（ESA 2018）论文集，莱布尼茨国际信息学会议录（LIPIcs）第112卷，第49:1–49:13页，2018。2, 5, 6[JK17] Stacey Jeffery 和 Shelby Kimmel。《图连通性与公式求值的量子算法》。Quantum，1:26，2017。2, 3[JZ22] Stacey Jeffery 和 Sebastian Zur。《多维量子游走及其在 k-distinctness中的应用》。arXiv 预印本 arXiv:2208.13492，2022。3[Kit95] A. Yu Kitaev。《量子测量与阿贝尔稳定子问题》。arXiv:quant-ph/9511026，1995。9[Koo11] Woong Kook。《图的组合格林函数及其在网络中的应用》。应用数学进展，46:417–423，2011。31[KW93] Mauricio Karchmer 和 Avi Wigderson。《论跨度程序》。载于第8届IEEE复杂性理论结构年会论文集，第102–111页，1993。4, 6[LMR+11] Troy Lee、Rajat Mittal、Ben W. Reichardt、Robert ˇSpalek 和 Mario Szegedy。《状态转换的量子查询复杂度》。载于第52届IEEE计算机科学基础年会（FOCS 2011）论文集，第344–353页，2011。3, 9

[LMS11] Troy Lee、Fr´ed´eric Magniez 和 Miklos Santha。《一种用于查找常数规模子图的基于学习图的量子查询算法》。《芝加哥理论计算机科学杂志》，18(1)，2011。3[LP17] Russell Lyons 和 Yuval Peres。《树与网络上的概率》。剑桥统计与概率数学丛书。剑桥大学出版社，2017。31[MNRS11] Fr´ed´eric Magniez、Ashwin Nayak、J´er´emie Roland 和 Miklos Santha。《通过量子漫步进行搜索》。SIAM 计算杂志，40(1):142–164，2011。9[NC10] Michael A Nielsen 和 Isaac L Chuang。《量子计算与量子信息》。剑桥大学出版社，2010。16[Rei11] Ben W. Reichardt。《量子查询算法的反射》。载于2011年ACM-SIAM离散算法年会论文集（SODA 2011），第560–569页，2011。3, 4[Rei14] Ben W. Reichardt。《跨度程序等价于量子查询算法》。SIAM 计算杂志，43(3):1206–1219，2014。4[SD84] J. Laurie Snell 和 Peter G. Doyle。《随机游走与电网络》，第22卷。AMS/MAA，1984。31[Tan09] Seiichiro Tani。《使用量子游走的爪形查找算法》。《理论计算机科学》，410:5285–5297，2009。1

A 流性质的证明

在本附录中，我们列出并证明若干关于图上流的结果。首先，我们重述并证明 引理7，它指出，对于图 $G(x$，其关于 x 在 $\mathcal{P}_{G_s\text{中的正见证}t}$所对应的最优流态 $|\theta^*\rangle/\,\||\theta^*\rangle\|$，也就是在算法 2的步骤 2 中近似得到的量子态，仅支撑在属于（自避） st-路径的边上。

接着，在 附录A.1中，我们介绍一些从图论量的角度对流的诠释，这有助于直观理解测量流态时得到的边分布。在附录 A.2 中，我们进一步给出一些此类诠释，这些诠释适用于串并联图。

引理7. st-路径在 $G(x)$ 中是由不同顶点组成的序列 $\vec{u} = (u_0, \ldots, u_\ell)$，满足 $s = u_0$, $t = u_\ell$，且对所有 $i \in [\ell]$，$(u_{i-1}, u_i) \in \vec{E}(G(x))$。根据 $\vec{u}$，我们定义

$$|\rho_{\vec{u}}\rangle = \frac{1}{\sqrt{2}} \sum_{i=0}^{\ell-1} (|u_i, u_{i+1}\rangle - |u_{i+1}, u_i\rangle) \tag{8}$$

并将所有此类量子态称为 $G(x)$ 的 st-路径量子态。那么，如果 $|\theta^*\rangle$ 是 $\mathcal{P}_{G_{s,\ t}}$ 中 x 的最优正见证，它就是 $G(x)$ 中 st-路径量子态的线性组合。

证明。对于任意 $(u, v) \in \vec{E} = \vec{E}(G)$，定义

$$|e_{u,v}\rangle := \frac{1}{\sqrt{2}} (|u, v\rangle - |v, u\rangle) = -|e_{v,u}\rangle, \tag{65}$$

从而，特别地，$|\rho_{\vec{u}}\rangle = \sum_{i=0}^{\ell-1} |e_{u_i,\ u_{i+1}}\rangle$。令

$$H^-(x) := \mathrm{span}\{|e_{u,v}\rangle : (u, v) \in \vec{E}(G(x))\} \tag{66}$$

并注意到，$\{|e_{u,v}\rangle : (u,v) \in \overrightarrow{E}(G(x))\ u < v\}$ 是 $H^{-}(x)$ 的一组标准正交基

我们首先证明 $|\theta^*\rangle$ 属于 $H^{-}(x)$。为此，注意到

$$H^{-}(x)^{\perp} \cap H(x) = \mathrm{span}\{|u,v\rangle + |v,u\rangle : (u,v) \in \overrightarrow{E}(G(x))\} \subseteq \ker(A) \cap H(x). \tag{67}$$

一个最优见证 $|\theta^*\rangle$ 必须与 $\ker(A) \cap H(x)$ 正交（否则，我们可以通过减去它在 $\ker(A) \cap H(x)$上的投影，在保持其为见证的同时使其更小），因此 $|\theta^*\rangle \in H^{-}(x)$，这意味着对于 $(u,v) \in \overrightarrow{E}(G(x))$，有 $\theta^*(u,v) = -\theta^*(v,u)$。由此可见：

$$|\theta^*\rangle = \frac{1}{\sqrt{2}} \sum_{(u,v)\in\overrightarrow{E}(G(x)):u<v} \theta^*(u,v)|e_{u,v}\rangle. \tag{68}$$

注意到

$$A|e_{u,v}\rangle = \frac{1}{\sqrt{2}}\left(|u\rangle - |v\rangle - (|v\rangle - |u\rangle)\right) = \sqrt{2}(|u\rangle - |v\rangle). \tag{69}$$

因此，我们可以将 $A\Pi_{H^{-}(x)}$ 表示为

$$A\Pi_{H^{-}(x)} = A \sum_{(u,v)\in\overrightarrow{E}(G(x)):u<v} |e_{u,v}\rangle\langle e_{u,v}| = \sqrt{2} \sum_{(u,v)\in\overrightarrow{E}(G(x)):u<v} (|u\rangle - |v\rangle)\langle e_{u,\ v}|. \tag{70}$$

然后，对于 $u \in V$，我们可以计算：

$$\begin{aligned}\langle u|A\Pi_{H^{-}(x)} &= \langle u| \sum_{(u',v)\in\overrightarrow{E}(G(x)):u'<v} \sqrt{2}(|u'\rangle - |v\rangle)\langle e_{u',v}| \\ &= \sqrt{2} \sum_{v:(u,v)\in\overrightarrow{E}(G(x)),u<v} \langle e_{u,v}| - \sqrt{2} \sum_{v:(v,u)\in\overrightarrow{E}(G(x)),v<u} \langle e_{u,v}| = \sqrt{2} \sum_{v:(u,v)\in\overrightarrow{E}(G(x))} \langle e_{u,v}|,\end{aligned} \tag{71}$$

由于 $|e_{u,\ v}\rangle = -|e_{v,\ u}\rangle$。由于 $|\theta^*\rangle$ 是一个正见证，因此我们有 $A\Pi_{H^{-}(x)}$
$|\theta^*\rangle = A|\theta^*\rangle = |s\rangle - |t\rangle$，由此可推导出以下约束，它们等价地说明 θ^* 必须是单位st-流：

$$\forall u \in V, \sum_{v:(u,v)\in\overrightarrow{E}(G(x))} \langle e_{u,v}|\theta^*\rangle = \begin{cases} 1/\sqrt{2} & \text{if } u = s \\ -1/\sqrt{2} & \text{if } u = t \\ 0 & \text{otherwise.} \end{cases} \tag{72}$$

对于 $|\psi\rangle \in H^{-}(x)$，如果 $|\psi\rangle$ 满足以下线性约束，我们就称其为循环流：

$$\forall u \in V, \sum_{v:(u,v)\in\overrightarrow{E}(G(x))} \langle e_{u,v}|\psi\rangle = 0. \tag{73}$$

由这类向量构成的 $H^{-}(x)$ 子空间记为 $\mathcal{C}(x)$。令 $\overline{G}(x)$ 为图 $G(x)$，但添加一条边 $\{s,t\}$（如果该边原本不存在）。我们默认假设 $\{s,t\} \in E(G)$；这不失一般性，因为我们总可以给这条边指定一个标签，使其不出现在任何 $G(x)$ 中，因此 $\overline{G}(x)$ 是 G 的子图。若在式 (73) 的每个约束中用 $\overline{G}(x)$ 替换 $G(x)$，则可定义 $H^{-}(x)$ 的一个张成空间 $+\mathrm{span}\{|e_{s,t}\rangle\}$，记为$\mathcal{C}'(x)$。由式 (71) 可得 $\mathcal{C}(x) \subseteq \mathcal{C}'(x) \subseteq \ker(A)$。

现在我们来论证

$$|\psi\rangle := |\theta^*\rangle - \frac{1}{\sqrt{2}}|e_{s,t}\rangle \in \mathcal{C}'(x). \tag{74}$$

对于任意 $u \in V \setminus \{s,t\}$：

$$\sum_{v:(u,v)\in\overrightarrow{E}(\overline{G}(x))} \langle e_{u,v}|\psi\rangle = \sum_{v:(u,v)\in\overrightarrow{E}(G(x))} \langle e_{u,v}|\theta^*\rangle - \frac{1}{\sqrt{2}} \sum_{v:(u,v)\in\overrightarrow{E}(\overline{G}(x))} \langle e_{u,v}|e_{s,t}\rangle = 0 - 0, \tag{75}$$

根据式（72）。对于 $u=s$,

$$\sum_{v:(u,v)\in\overrightarrow{E}(\overline{G}(x))}\langle e_{u,v}|\psi\rangle=\sum_{v:(s,v)\in\overrightarrow{E}(G(x))}\langle e_{s,v}|\theta^*\rangle-\frac{1}{\sqrt{2}}\langle e_{s,t}|e_{s,t}\rangle=\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}=0, \tag{76}$$

再次由 式（72），对于 $u=t$ 也可用完全类似的方法证明。这就得到了 式（74）。

令 $\mathcal{P}'_{s,\ t}(x$ 为 st-路径量子态在 $\overline{G}(x$ 中张成的空间。那么由 式（74），可得:

$$|\theta^*\rangle\in\mathcal{P}'_{s,t}(x)+\mathcal{C}'(x). \tag{77}$$

假设 $\{s,t\}\notin E(G(x))$（另一种情况更简单），此时 $\mathcal{P}'_{s,\ t}(x)=\mathcal{P}_{s,\ t}(x)$ $\oplus$张成空间$\{|e_{s,t}\rangle\}$，其中 $\mathcal{P}_{s,\ t}(x)$ 是 st-路径量子态在 $G(x)$ 中张成的空间。于是

$$|\theta^*\rangle\in\mathcal{P}_{s,t}(x)\oplus\operatorname{span}\{|e_{s,t}\rangle\}+\mathcal{C}'(x). \tag{78}$$

由于 $\{s,t\}\notin E(G(x))$, $|\theta^*\rangle$ 与 $|e_{s,\ t}\rangle$ 正交。此外，由于 $|\theta^*\rangle$ 的最优性，$|\theta^*\rangle$ 与 $H(x)$ $\cap\ker(A)$ 正交，因此特别地，它与 $\mathcal{C}'(x)$ $\subseteq$ $H'(x)$ $\cap\ker(A)$ $\subseteq$张成空间$\{|e_{s,t}\rangle\}$ $\oplus(H(x)$ $\cap\ker(A))$ 正交。由此可得 $|\theta^*\rangle\in\mathcal{P}_{s,\ t}(x)$。 □

A.1 一般图上的流

引理 27 ([SD84])。 θ 是 G 中最优的单位 st-流。对于任意 u、$v\in V$，令 $Z_{u,v}$ 表示从 s 出发并持续游走直至到达 t 的随机游走者从顶点 u 移动到顶点 v 的次数。则 $\theta(u,v)$ $=\mathbb{E}[Z_{u,v}]-\mathbb{E}[Z_{v,u}]$。

引理 28 ([LP17])。 令 θ 为最优单位 st-流，且位于 G中。令 $\mathcal{T}_G$ 为 G 的生成树集合；对于任意 $\{u,v\}\in E$，令 $\mathcal{N}_G(u,v)$ 为 G 的生成树集合，其中唯一的st-路径包含有向边 (u,v)。那么

$$\theta(u,v)=\frac{|\mathcal{N}_G(u,v)|-|\mathcal{N}_G(v,u)|}{|\mathcal{T}_G|}.$$

我们对量 $q_{u,v}$ 的含义作如下解释：$=\ ^{\theta}(\frac{u\ v\ ^2}{\mathcal{R}_{s,t}\ G},),()$，这是我们的边查找算法 算法 2 对 $\{u,v\}$ （通过测量 (u,v) 或 (v,u)）进行采样的概率:

引理 29。假设 $\{s,t\}\notin E(G)$，令 $\overline{G}$ 为图 G 加上一条额外的 $\{s,t\}$ 边所得的图，并令 $\overline{G}/\{s,t\}$ 为将这条边收缩后的 $\overline{G}$，也就是将顶点 s 和 t 合并后的 G。那么

$$q_{u,v}=\frac{(|\mathcal{N}_G(u,v)|-|\mathcal{N}_G(v,u)|)^2}{|\mathcal{T}_G|\cdot|\mathcal{T}_{\overline{G}/\{s,t\}}|}.$$

证明。对于一条边 $e\in E(G)$，我们用 G/e 表示将边 e 在 G 中收缩后得到的图。注意，对任意 $e\in E(G)$， $\mathcal{T}_G=\mathcal{T}_{G/e}\cup\mathcal{T}_{G\setminus e}$——也就是说， $\mathcal{T}_G$ 是以下两部分的（不相交）并集：(1) 包含 e 的生成树集合，它们与 G/e的生成树同构；(2) 不包含 e的生成树集合，它们与 $G\setminus e$的生成树同构。特别地，这意味着$|\mathcal{T}_{\overline{G}/\{s,t\}}|=|\mathcal{T}_{\overline{G}}|-|\mathcal{T}_G|$，因为$G=\overline{G}\setminus\{s,t\}$。由于$\{s,t\}\in E(\overline{G})$，根据 [Koo11定理 6],

$$R_{s,t}(\overline{G})=\frac{|\mathcal{T}_{\overline{G}/\setminus\{s,t\}}|}{|\mathcal{T}_{\overline{G}}|}=\frac{|\mathcal{T}_{\overline{G}}|-|\mathcal{T}_G|}{|\mathcal{T}_{\overline{G}}|}=1-\frac{|\mathcal{T}_G|}{|\mathcal{T}_{\overline{G}}|}. \tag{79}$$

由于 $\overline{G}$ 是 G 与一条边 $\{s,t\}$ 的并联组合，且并联电导相加，因此我们得到

$$R_{s,t}(\overline{G})=\frac{1}{\frac{1}{R_{s,t}(G)}+\frac{1}{1}}=1-\frac{1}{R_{s,t}(G)+1}. \tag{80}$$

由此可得：

$$\begin{aligned} R_{s,t}(G)+1 &= \frac{1}{1-R_{s,t}(\overline{G})} = \frac{|\mathcal{T}_{\overline{G}}|}{|\mathcal{T}_G|} \\ R_{s,t}(G) &= \frac{|\mathcal{T}_{\overline{G}}|-|\mathcal{T}_G|}{|\mathcal{T}_G|} = \frac{|\mathcal{T}_{\overline{G}/\{s,t\}}|}{|\mathcal{T}_G|}. \end{aligned} \tag{81}$$

因此，根据 引理 28：

$$q_{u,v} = \frac{(|\mathcal{N}_G(u,v)|-|\mathcal{N}_G(v,u)|)^2}{|\mathcal{T}_G|^2}\frac{|\mathcal{T}_G|}{|\mathcal{T}_{\overline{G}/\{s,t\}}|}, \tag{82}$$

由此即可得出引理的结论。 □

A.2 串并联图上的流

在串并联图中，对于每条边 $\{u,v\}$，都存在唯一的方向，即 (u,v) 或 (v,u)，使得每条经过该边 $\{u,v\}$ 的（自避） st-路径都沿该方向行进。我们将其称为 $\{u,v\}$ 的 st-方向。

引理30. 设 G 是一个串并联图。对于任意边 $\{u,v\}\in E(G)$，若其 st-方向为 (u,v)，

$$q_{u,v} = \frac{|\mathcal{N}_G(u,v)|^2}{|\mathcal{T}_G|\cdot|\mathcal{T}_{\overline{G}/\{s,t\}}|} = p_{u,v}\cdot p'_{u,v},$$

其中 $p_{u,\,v}$ 是均匀随机生成树在其唯一的 st-路径上包含 (u,v) 的概率，而 $p'_{u,\,v}$ 是从 G 中随机抽取的、将 s 和 t 分隔开的双分支生成森林在其唯一的 st-割中包含 (u,v) 的概率。

证明。由于（自避） st-路径只能使用（u，v），而不能使用（v，u），因此有 $\mathcal{N}_G(v,\,u)=\emptyset$。由此可根据 引理 29 得出

$$q_{u,v} = \frac{|\mathcal{N}_G(u,v)|^2}{|\mathcal{T}_G|\cdot|\mathcal{T}_{\overline{G}/\{s,t\}}|} = \frac{|\mathcal{N}_G(u,v)|}{|\mathcal{T}_G|}\frac{|\mathcal{N}_G(u,v)|}{|\mathcal{T}_{\overline{G}/\{s,t\}}|}. \tag{83}$$

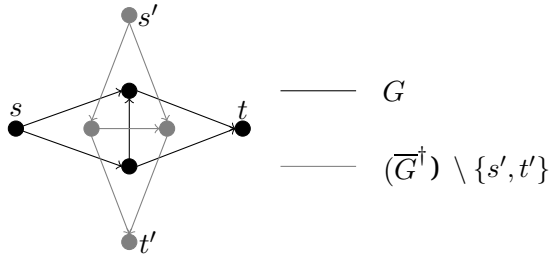
根据定义，$|\mathcal{N}_G(u,v)|/|\mathcal{T}_G|$ 是从 $\mathcal{T}_G$ 中随机抽取的生成树在其唯一的 st-路径上包含 (u,v) 的概率，$p_{u,\,v}$。注意，$\mathcal{T}_{\overline{G}/\{s,t\}}$ 与包含 $\{s,t\}$的 $\overline{G}$ 的生成树集合同构，而后者又与 G 的双分支生成森林集合同构，其中 s 和 t 位于不同的分支中。类似地，$\mathcal{N}_G(u,v)$ 与 G 的双分支生成森林集合同构（通过移除边 $\{u,v\}$），这些森林中 s 和 t 位于不同的分支中，且其补集中唯一的 st-割包含 (u,v)。因此，$|\mathcal{N}_G(u,v)|/|\mathcal{T}_{\overline{G}/\{s,t\}}|$ 是 $p'_{u,\,v}$。

□

通过简单的归纳论证可知，任何串并联图都是平面的。给定 G 的一个隐式平面嵌入，我们令 $G^\dagger$ 表示其平面对偶图，定义如下。

定义31（对偶图）。对于平面嵌入图 G，其对偶图是图 $G^\dagger$，其顶点集为 $V(G^\dagger)$，被精确定义为 G 的各个面（相对于其隐含的固定嵌入），当且仅当面 f 和 f' 被一条边 $e\in E(G)$ 分隔时，面 f、$f'\in V(G^\dagger)$ 之间存在一条边 $\{f,f'\}$，此时记为 $e=\{f,f'\}^\dagger$。如果 $e=\{u,v\}$，且 f' 是（u，v）的顺时针侧上的面（也就是说，当（u，v）指向上方时，位于其右侧），则记为（u，v）$^\dagger=$（f，f'）。

我们将考虑图 $(\overline{G}^{\dagger}) \setminus \{s', t'\}$，它是通过向 G 添加一条边 $\{s, t\}$（从而得到 $\overline{G}$），取其对偶图，然后移除边 $\{s', t'\} = \{s, t\}^{\dagger}$ 而得到的。下图展示了这样一个图的示例。我们还为 G 中的每条边指定了一个定向，以展示对偶图中的相应定向。请注意，这个示例图是平面的，但不是串并联图。



引理 32。设 G 是一个串并联图。则 $q_{u,\,v} = p_{u,\,v} p^{\dagger}_{u,\,v}$，其中 $p_{u,\,v}$ 是从 G 的均匀随机生成树中，u、v位于其唯一 st路径上的概率；而$p^{\dagger}_{u,\,v}$是从 $(\overline{G}^{\dagger}) \setminus \{s', t'\}$ 的均匀随机生成树中，u、$v^{\dagger}$ 位于其唯一 $s't'$路径上的概率，其中 $(s', t') = (s, t)^{\dagger}$。

证明。我们将用到以下观察：任取一个平面图 G，其中 s和 t位于同一个面上。对于每个 $T \in \mathcal{T}_G$，令 $T^{\dagger}$为 $G^{\dagger}$的子图，使得 $e \in E(G) \setminus E(T)$ 当且仅当 $e^{\dagger} \in E(T^{\dagger})$。那么 $T \mapsto T^{\dagger}$ 是 $\mathcal{T}_G$ 与 $\mathcal{T}_{G^{\dagger}}$之间的双射。为此，注意到 T 中存在一个环，当且仅当 $T^{\dagger}$ 有多个连通分支——环内的子图与环外的子图不连通。类似地， T 有多个连通分量，当且仅当 $T^{\dagger}$中存在一个环。因此 $T^{\dagger} \in \mathcal{T}_{G^{\dagger}}$，且该映射显然是一个双射。

由于 $\overline{G}^{\dagger} \setminus \{s', t'\} = (\overline{G}/\{s, t\})^{\dagger}$，上述观察表明存在从 $\mathcal{T}_{\overline{G}/\{s,t\}}$ 到 $\mathcal{T}_{(\overline{G}^{\dagger}) \setminus \{s', t'\}}$ 的双射，从而证明

$$|\mathcal{T}_{\overline{G}/\{s,t\}}| = |\mathcal{T}_{(\overline{G}^{\dagger}) \setminus \{s', t'\}}|. \tag{84}$$

接下来，我们将证明

$$|\mathcal{N}_G(u, v)| = |\mathcal{N}_{(\overline{G}^{\dagger}) \setminus \{s', t'\}}((u, v)^{\dagger})| \tag{85}$$

通过构造一个双射，并结合式（84），引理结论很容易由引理30推出。首先，注意到 $\mathcal{N}_{\overline{G}}(u, v) = \mathcal{N}_G(u, v)$，因为 $\mathcal{N}_{\overline{G}}(u, v)$ 中的任何树都不能包含 $\{s, t\}$，否则， st-路径上的唯一一条边将是 (s, t)。映射 $\phi(T) = T^{\dagger}$ 将 $\mathcal{N}_{\overline{G}}(u, v)$ 双射地映射到 $\overline{G}^{\dagger}$ 的生成树集合中那些包含 $\{s', t'\}$ 但不包含 $\{u, v\}^{\dagger} = \{u', v'\}$ 的生成树，而且，(s', t') 位于该树的唯一 $u'v'$-路径上。根据我们之前的观察，这是一个双射。最后，定义 $\phi'(T^{\dagger})$ 为从 $T^{\dagger}$ 中移除 $\{s', t'\}$ 并加入 $\{u', v'\}$。接着我们声称， $\phi' \circ \phi$ 是从 $\mathcal{N}_{\overline{G}}(u, v)$ 到 $\mathcal{N}_{\overline{G}^{\dagger}}(u', v') = \mathcal{N}_{\overline{G}^{\dagger} \setminus \{s', t'\}}(u', v')$ 的双射。 □