1 Verification of matrix products

(a) 假设我们取出 A 完整的 a 行，b 完整的 b 行。

花费 $(a+b)\,O(n)$ queries

但最多能验证 C 中 ab 个点位

故要求 $\frac{ab}{n^2} \geq \frac{2}{3}$

$\text{queries} = (a+b)\,\Omega(n) \geq 2\sqrt{ab}\cdot\Omega(n) = \Omega(n^2)$

(b) 考虑 Freivalds' algorithm:

Step 1：选 $r \overset{i.i.d}{\sim} \{0,1\}^n$

Step 2：计算 $A\cdot(B\cdot r)$ 及 $C\cdot r$，花费 $\Theta(n^2)$ 时间

Step 3：若 $A\cdot(B\cdot r) = C\cdot r$ 返回成立

否则返回不成立

若 $A\cdot B = C$ 则出错概率 $p=0$

若 $A\cdot B \neq C$

设 $P = (AB-C)r := (p_1 \cdots p_n)^T$ 记 $D = AB-C$

$\exists\, i,j,\ d_{ij} \neq 0$

$p_i = \sum_{k=1}^{n} d_{ik} r_k = d_{ij} r_j + y$

$$
\begin{aligned}
Pr[p_i = 0] &= Pr[p_i=0 \mid y=0]\,Pr[y=0] + Pr[p_i=0 \mid y\neq 0]\,Pr[y\neq 0] \\
&= Pr[r_j=0]\,Pr[y=0] + Pr[r_j=1,\ d_{ij}=-y]\,Pr[y\neq 0] \\
&\leq \frac{1}{2}\,Pr[y=0] + \frac{1}{2}(1-Pr[y=0]) = \frac{1}{2}
\end{aligned}
$$

$Pr[P=0] = Pr[p_1=0, \cdots p_n=0] \leq Pr[p_i=0] \leq \frac{1}{2}$

故只需运行 2 次，成功概率 $\geq 1-\frac{1}{2^2} \geq \frac{2}{3}$ #

(Reference: Wikipedia)

(c) 计算 $y=B_i x$ 及 $z=C_i x$ 的 queries 是 $O(mn)$

使用 Grover Search 验证 $Ay=z$ 的 queries 是 $O(n\sqrt{n})$

其 subroutine V_i queries $O(mn+n^{\frac{3}{2}})$

由 amplitude amplification,

总共 $O\left((mn+n^{\frac{3}{2}})\cdot\sqrt{\frac{n}{m}}\right)$

$$=O\left(n^{\frac{3}{2}}\sqrt{m}+n^2\frac{1}{\sqrt{m}}\right)$$

$$\geq O\left(n^{\frac{7}{4}}\right)$$ 当且仅当 $m=\sqrt{n}$

故最佳 $m=\sqrt{n}$ 上界 $O(n^{\frac{7}{4}})$

(d) $S=\underset{\text{准备 }P_R A_R}{O(mn)}+\underset{\text{准备 }B_s\, \&\, s}{O(mn)}+\underset{\text{准备 }P_R C_{R,s}\, \&\, s}{O(m^2)}=O(mn+m^2)$

$U=\underset{\substack{\text{准备 }P_R A_R,\\ \text{只需读取变列}}}{O(n)}+\underset{\text{准备 }B_s\, \&\, s}{O(n)}+\underset{\text{准备 }P_R C_{R,s}\, \&\, s}{O(m)}=O(m+n)$

$C=0$

(e) 先计算 ε：假设 (r,s) 位乘法不同,

$r\in R, s\in S$, 那么 $A_R B_s - C_{R,S}\neq 0$, 该顶点 marked (with high probability)

故 $\varepsilon\geq\frac{(n^m-(n-1)^m)^2}{n^{2m}}$ （考虑所有至少包含 (r,s) 的顶点）

下面计算 δ.

记 $A_0 = (J-I)\otimes I \otimes \cdots \otimes I + \cdots + I \otimes \cdots \otimes (J-I)$

$A = A_0 \otimes A_0$ 为 $H(n,m) \otimes H(n,m)$ 的 adjacency matrix

$J-I$ 特征值为 $n-1$ or 1

$$n-1 \downarrow \quad |\psi_0\rangle = \frac{1}{\sqrt{n}}\sum_{i=1}^{n} |i\rangle \qquad 1 \downarrow \quad |\psi_1\rangle \cdots |\psi_{n-1}\rangle$$

A 特征值形如 $|\psi_{i_1}\rangle \cdots |\psi_{i_m}\rangle \otimes |\psi_{j_1}\rangle \cdots |\psi_{j_m}\rangle$

$i_1 \cdots i_m$ 有 k_1 个为 0, $j_1 \cdots j_m$ 有 k_2 个

A 的谱为 $\{[(n-1)k_1 + (-1)(m-k_1)][(n-1)k_2 + (-1)(m-k_2)]\}$

$= \{(nk_1 - m)(nk_2 - m)\}$

$\delta_A = n(nm-m)$

Stochastic matrix $P = \frac{A}{\deg(i)} = \frac{A}{m^2(n-1)^2}$

$\Rightarrow \delta_P = \frac{n}{m(n-1)}$

(e) quantum queries 即 $O\left(s(n) + \frac{1}{\sqrt{\varepsilon\delta}}(U+C)\right)$

$L = O\left(mn + m^2 + \frac{1}{1-(1-\frac{1}{n})^m}\sqrt{\frac{m(n-1)}{n}}(m+n)\right)$ (因为 $(1-\frac{1}{n})^m \le 1-\frac{m}{n}$)

$= O\left(mn + m^2 + n\sqrt{m} + \frac{n^2}{\sqrt{m}}\right)$

设 $m = n^\alpha$

$L \geqslant O\left(mn + \frac{n^2}{2\sqrt{m}} \times 2\right) \geqslant O\left(\sqrt[3]{\frac{1}{4}n^5}\right) = O(n^{\frac{5}{3}})$

仅当 $m = O(n^{\frac{2}{3}})$

故最佳 $m = O(n^{\frac{2}{3}})$ quantum queries complexity 上界 $O(n^{\frac{5}{3}})$ #

2 Triangle Finding

(a) 经典算法的 query complexity is $\Theta(n^2)$

首先直接读取所有 (V_i, V_j)，$i,j \in [n]$ 即可，所以至多 $O(n^2)$

其次考虑二部图 $K(\frac{n}{2}, \frac{n}{2})$，在某部里连一条边。设 $|E| = \binom{n}{2}$.

设随机算法每次挑 k 个边，运行 m 次，queries $O(km)$

每次失败概率 $\geq \frac{\binom{|E|-1}{k}}{\binom{|E|}{k}} = \frac{|E|-k}{|E|}$

成功概率 $\frac{2}{3} \leq P \leq 1-(1-\frac{k}{|E|})^m \simeq \frac{km}{|E|}$

故 $km \geq \frac{2}{3}|E| = \Omega(n^2)$

故 queries 复杂度 $\Theta(n^2)$ #

(b) 设已知某条边为 (i,j)，$i,j \in [V]$

对 $k \in [V]$，$k \neq i,j$，记 $f(k) = \begin{cases} 1 & \text{if } (i,k) \in E, (j,k) \in E \\ 0 & \text{else} \end{cases}$

那么由 Grover Search (及其 optimality)，我们知道 quantum query complexity 是 $\Theta(\sqrt{n})$

(Algorith: Do Grover on f (Search for $f=1$), returns k

If $f(k)=1$：输出存在

Else：输出不存在

该算法复杂度与 Grover 一样，高概率成功).

(c) 固定 $v \in V$ 设 $U \subset V$，$|U| = m$

对 $u \in U$，记 $f(u) = \begin{cases} 1 & \text{if } (u,v) \in E \\ 0 & \text{else} \end{cases}$

考虑 Johnson graph $J(m, m^{\frac{2}{3}})$ 上的 quantum walk

spectral gap $\delta = \frac{m}{m^{\frac{2}{3}}(m-m^{\frac{2}{3}})} = O(m^{-\frac{2}{3}})$ (A.E. Brower. Spectra of graphs. Springer 2012)

标记一个点如果存在 $u, v \in U$，$f(u) = f(v) = 1$ 且 $(u,v) \in E$

若存在以 v 为顶点，其边在 U 中的 triangle

我们有标记比例

$$\varepsilon \geq \frac{\binom{m-2}{m^{\frac{2}{3}}-2}}{\binom{m}{m^{\frac{2}{3}}}} = O(m^{-\frac{2}{3}})$$

setup cost $S(m) = O(m^{\frac{2}{3}})$ (query (u, v) , u 遍历 Johnson Graph 节点上)

update cost $U(m) = O(1)$ (同上)

checkup cost $C(m) = 0$

由 quantum many step walk framework,

为 $O(m^{\frac{2}{3}} + m^{\frac{2}{3}} \cdot 1) = O(m^{\frac{2}{3}})$

再对 $v \in V$ 使用 amplitude amplification,

总复杂度 $O(m^{\frac{2}{3}}\sqrt{n})$ #

(d) 这个 quantum walk set up cost $S(m) = O(m^2)$ (获取 m 阶子图信息)

update cost $U(m) = O(m)$ (确定新顶点和之前顶点连接状况)

check cost $C(m) = O(m^{\frac{2}{3}}\sqrt{n})$ (由 (c))

考虑 marked item 占比 ε 和 spectral gap δ.

若图里至少有一条 triangle edge, 那么 $\varepsilon \geq \frac{\binom{n-2}{m-2}}{\binom{n}{m}} = \frac{m(m-1)}{n(n-1)} = O(\frac{m^2}{n^2})$

Johnson graph $J(n,m)$ 的 spectral gap 是 $\delta = \frac{n}{m(n-m)}$

$$\frac{1}{\sqrt{\delta}} = O(\sqrt{m})$$

根据 quantum many walk framework

quantum query complexity 为 $S(m) + \frac{1}{\sqrt{\varepsilon}}\left(\frac{1}{\sqrt{\delta}} U(m) + C(m)\right)$

$$= O\left(m^2 + \frac{n}{m}\left(m^{\frac{3}{2}} + m^{\frac{2}{3}}\sqrt{n}\right)\right)$$

#

(e) quantum query complexity

$L = O\left(m^2 + n \cdot m^{\frac{1}{2}} + n\sqrt{n}\, m^{-\frac{1}{3}}\right)$

记 $m = n^{\alpha}$

$\alpha \le \frac{2}{3}$ 时

$L \geq O\left(\frac{n}{2} m^{\frac{1}{2}} + \frac{n}{2} m^{\frac{1}{2}} + \frac{n\sqrt{n}}{3} m^{-\frac{1}{3}} + \frac{n\sqrt{n}}{3} m^{-\frac{1}{3}} + \frac{n\sqrt{n}}{3} m^{-\frac{1}{3}}\right)$

$\geq O\left(5 \sqrt[5]{\frac{1}{2^2 3^3} n^{\frac{13}{2}}}\right) = O\left(n^{\frac{13}{10}}\right)$ 当且仅当 $\alpha = \frac{3}{5}$ 取等

$\alpha > \frac{2}{3}$ 时

$L \geq O\left(m^2 + \frac{n\sqrt{n}}{6} m^{-\frac{1}{3}} \times 6\right)$

$\geq O\left(n^{\frac{4}{3}}\right)$ (AM-GM 取不了等) $> O\left(n^{1.3}\right)$

综上，最佳 $m = n^{\frac{3}{5}}$ 该问题上界 $O\left(n^{\frac{13}{10}}\right)$ #

Reference

[1] Quantum Verification of Matrix Products. SODA 2006

[2] Quantum Algorithm For the Triangle Problem SIAM. J. Computing 2007