Lower bounds analysis for quantum linear algebras

邵长鹏

中科院数学院—数学机械化重点实验室
Based on joint works with Ashley Montanaro and Nikhil Mande

2024 年 5 月 22 日
清华大学

量子线性代数

- 量子线性代数在量子算法设计和量子优势探索方面起到了重要作用。

量子线性代数

- 量子线性代数在量子算法设计和量子优势探索方面起到了重要作用。
- 哈密顿模拟问题：制备 $|e^{iAt}b\rangle$。能够体现量子优势的一个重要问题。

量子线性代数

- 量子线性代数在量子算法设计和量子优势探索方面起到了重要作用。
- 哈密顿模拟问题：制备 $|e^{iAt}b\rangle$。能够体现量子优势的一个重要问题。
- 求解线性方程组的 HHL 算法：制备 $|A^{-1}b\rangle$。极大促进了量子线性代数的发展(包括应用)，如
  机器学习，例如推荐系统：制备 $|A_{\geq\delta}i\rangle$
  微分方程组求解：制备 $|e^{At}b\rangle$

量子线性代数

- 量子线性代数在量子算法设计和量子优势探索方面起到了重要作用。
- 哈密顿模拟问题：制备 $|e^{iAt}b\rangle$。能够体现量子优势的一个重要问题。
- 求解线性方程组的 HHL 算法：制备 $|A^{-1}b\rangle$。极大促进了量子线性代数的发展(包括应用)，如
  机器学习，例如推荐系统：制备 $|A_{\geq\delta}i\rangle$
  微分方程组求解：制备 $|e^{At}b\rangle$
- 这些问题都可以简述成矩阵函数的语言：给定函数 $f(x)$，矩阵 A，态 $|b\rangle$，制备 $|f(A)b\rangle$。

量子线性代数

- 量子线性代数在量子算法设计和量子优势探索方面起到了重要作用。
- 哈密顿模拟问题：制备 $|e^{iAt}b\rangle$。能够体现量子优势的一个重要问题。
- 求解线性方程组的 HHL 算法：制备 $|A^{-1}b\rangle$。极大促进了量子线性代数的发展(包括应用)，如
  机器学习，例如推荐系统：制备 $|A_{\geq\delta}i\rangle$
  微分方程组求解：制备 $|e^{At}b\rangle$
- 这些问题都可以简述成矩阵函数的语言：给定函数 $f(x)$，矩阵 A，态 $|b\rangle$，制备 $|f(A)b\rangle$。
- 量子奇异值变换可有效用来制备 $|f(A)b\rangle$。

量子奇异值变换 (Gilyén, Su, Low, Wiebe STOC 2019)

给定矩阵 A 和酉矩阵

$$U = \begin{pmatrix} A/\alpha & * \\ * & * \end{pmatrix}$$

设 f 是在 $[-1,1]$ 上有界的一个多项式，则存在量子电路实现

$$\widetilde{U} = \begin{pmatrix} f(A/\alpha) & * \\ * & * \end{pmatrix}$$

这个量子电路使用了 $O(\deg(f))$ 次 U。

量子奇异值变换 (QSVT)

- 如果 f 不是多项式，则可以考虑其多项式逼近。

量子奇异值变换 (QSVT)

- 如果 f 不是多项式，则可以考虑其多项式逼近。
- 直接应用：制备 $|f(A/\alpha)b\rangle$。如
  $f(x) = x^{-1}$，则对应于求解线性方程组
  $f(x) = e^{ixt}$，则对应于哈密顿模拟

量子奇异值变换 (QSVT)

- 如果 f 不是多项式，则可以考虑其多项式逼近。
- 直接应用：制备 $|f(A/\alpha)b\rangle$。如
  $f(x) = x^{-1}$，则对应于求解线性方程组
  $f(x) = e^{ixt}$，则对应于哈密顿模拟
- 很多时候得到的量子算法最优，复杂度为 $O(\widetilde{\deg}_\varepsilon(f))$，这里逼近次数 (approximate degree)

$$\widetilde{\deg}_\varepsilon(f) = \min\{d : |f(x) - g(x)| \le \varepsilon, \forall x \in [-1,1], \\ g(x) \text{ 是一个次数为 } d \text{ 的多项式}\}.$$

QSVT 的复杂度下界为 $\Omega(\max_{x\in[-1,1]} |f'(x)|)$。

块嵌入 (block-encoding)

需要假定 $U = \begin{pmatrix} A/\alpha & * \\ * & * \end{pmatrix}$，称为 A 的块嵌入 (block-encoding)。在一些情形下存在有效构造方式：

块嵌入 (block-encoding)

需要假定 $U = \begin{pmatrix} A/\alpha & * \\ * & * \end{pmatrix}$，称为 A 的块嵌入 (block-encoding)。在一些情形下存在有效构造方式：

- A 是稀疏的 (这时 $\alpha = s\|A\|_{\max}$)
- A 是密度矩阵或是 POVM 算子 (这时 $\alpha = 1$)
- A 存储在 QRAM 数据结构中 (这时 $\alpha = \|A\|_F$)
  若经典情形下使用类似数据结构，则存在多项式时间算法“计算” $f(A/\alpha)b$
  [Tang STOC 2018] $\Rightarrow$ 无指数量子加速!
- 通过块嵌入的线性组合或乘法运算来构造新的块嵌入

本报告内容：矩阵函数的复杂度下界的一些新的结果和方法

1. 量子奇异值变换的最优性 [with A. Montanaro, arXiv:2311.06999, STOC 2024]
2. 量子通信复杂度下的量子奇异值变换 [with A. Montanaro, arXiv:2210.01601, QIP 2023]
3. 量子查询复杂度和量子通信复杂度的关联 [with N. Mande, arXiv:2402.15686]

矩阵函数

定义

设 A 是一个厄米矩阵，特征值分解为 $A = UDU^T$。设 $f(x)$ 是一个在 D 上有定义的函数，则[1]

$$f(A) := Uf(D)U^T$$

其中若 $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$，则 $f(D) = \mathrm{diag}(f(\lambda_1), \ldots, f(\lambda_n))$

例

- 设 $f = x^k$，则 $f(A) = A^k$
- 设 $f = e^x$，则 $f(A) = e^A$
- 设 $f = 1/x$，则 $f(A) = A^{-1}$

[1] Nicholas Higham, Functions of Matrices: Theory and Computations. SIAM 2008

矩阵函数在量子计算领域

在量子计算领域，一个非常重要的函数是 $f(x) = e^{ixt}$，则

$$f(A) = e^{iAt}.$$

对应于哈密顿模拟问题，是量子计算领域最基本也是最重要的问题之一。

矩阵函数在量子计算领域

在量子计算领域，一个非常重要的函数是 $f(x) = e^{ixt}$，则

$$f(A) = e^{iAt}.$$

对应于哈密顿模拟问题，是量子计算领域最基本也是最重要的问题之一。

定理 (Low & Chuang, 2017)

假定 A 稀疏，$\|A\| \leq 1$，则计算 $e^{iAt}|\psi\rangle$ 的量子复杂度为

$$\Theta\left(t + \frac{\log(1/\varepsilon)}{\log\log(1/\varepsilon)}\right).$$

矩阵函数在量子计算领域

在量子计算领域，一个非常重要的函数是 $f(x) = e^{ixt}$，则

$$f(A) = e^{iAt}.$$

对应于哈密顿模拟问题，是量子计算领域最基本也是最重要的问题之一。

定理 (Low & Chuang, 2017)

假定 A 稀疏，$\|A\| \leq 1$，则计算 $e^{iAt}|\psi\rangle$ 的量子复杂度为

$$\Theta\left(t + \frac{\log(1/\varepsilon)}{\log\log(1/\varepsilon)}\right).$$

该问题是 BQP-完全问题（也即能够在量子计算机上有效解决的最困难的一类问题）

矩阵函数在量子计算领域

- 另外一个 BQP-完全问题是计算 $A^{-1}|b\rangle$。对应于求解线性方程组，这里的 $f(x) = 1/x$ [Harrow, Hassidim, Lloyd 2008]

矩阵函数在量子计算领域

- 另外一个 BQP-完全问题是计算 $A^{-1}|b\rangle$。对应于求解线性方程组，这里的 $f(x) = 1/x$ [Harrow, Hassidim, Lloyd 2008]
- 假定 A 是稀疏的，则量子算法的复杂度为 $\widetilde{\Theta}(\kappa)$，其中 κ 为 A 的条件数 [Ambainis 2010]

矩阵函数在量子计算领域

- 另外一个 BQP-完全问题是计算 $A^{-1}|b\rangle$。对应于求解线性方程组，这里的 $f(x) = 1/x$ [Harrow, Hassidim, Lloyd 2008]
- 假定 A 是稀疏的，则量子算法的复杂度为 $\widetilde{\Theta}(\kappa)$，其中 κ 为 A 的条件数 [Ambainis 2010]
- 这些问题都可以使用量子奇异值变换求解，且所得到的量子算法最优。那一般情形下呢？

矩阵函数问题

问题

设 A 是一个稀疏的厄米矩阵，$\|A\| \leq 1$，设 $f : [-1, 1] \to [-1, 1]$ 是一个函数，对任意给定的两个指标 i, j，研究计算 $f(A)_{i,j} \pm \varepsilon$ 的复杂度，尤其是复杂度下界。

矩阵函数问题

问题

设 A 是一个稀疏的厄米矩阵，$\|A\| \le 1$，设 $f:[-1,1] \to [-1,1]$ 是一个函数，对任意给定的两个指标 i,j，研究计算 $f(A)_{i,j} \pm \varepsilon$ 的复杂度，尤其是复杂度下界。

定义 (查询复杂度 (query complexity))

设 $A = (A_{i,j})_{n\times n}$ 是一个稀疏的厄米矩阵，给定两个 Oracle

$$(i,j) \longrightarrow \boxed{\mathcal{O}_1} \longrightarrow p_{i,j}$$

$$(i,j) \longrightarrow \boxed{\mathcal{O}_2} \longrightarrow A_{i,j}$$

其中 $p_{i,j}$ 是第 i 行第 j 个非零元素的位置。查询复杂度定义为逼近 $f(A)_{i,j}$ 所使用的 $\mathcal{O}_1, \mathcal{O}_2$ 的最少个数。

定理 (基于量子奇异值变换)

假定 $\|A\| \leq 1-\delta$，这里 $\delta > 0$。对任意 $|x\rangle, |y\rangle$，存在量子算法计算 $\langle x|f(A)|y\rangle \pm \varepsilon$，其复杂度为

$$O(\frac{C}{\varepsilon}\widetilde{\deg}_\varepsilon(f))$$

其中 $C = \frac{s}{\delta}\log(\frac{s}{\varepsilon}\widetilde{\deg}_\varepsilon(f))$，这里 s 为稀疏度（即每行/列非零元素个数 $\leq s$）。

注：假定 $\|A\| \leq 1-\delta$ 是希望得到如下的 block-encoding

$$U = \begin{pmatrix} A & * \\ * & * \end{pmatrix}$$

例子：矩阵幂次 A^d

经典算法：

- 设 A 的稀疏度为 s。按定义

$$(A^d)_{i,j} = \sum_{k_1} \sum_{k_2} \cdots \sum_{k_{d-1}} A_{i,k_1} A_{k_1,k_2} \cdots A_{k_{d-1},j}$$

由于稀疏性，复杂度为 $O(s^{d-1})$

例子：矩阵幂次 A^d

经典算法：

- 设 A 的稀疏度为 s。按定义

$$(A^d)_{i,j} = \sum_{k_1} \sum_{k_2} \cdots \sum_{k_{d-1}} A_{i,k_1} A_{k_1,k_2} \cdots A_{k_{d-1},j}$$

  由于稀疏性，复杂度为 $O(s^{d-1})$

- 对于 x^d，存在次数为 $\Theta(\sqrt{d})$ 的逼近多项式，因此结果可改进到 $s^{O(\sqrt{d})}$ [Sachdeva & Vishnoi, 2014]

例子：矩阵幂次 A^d

经典算法：

- 设 A 的稀疏度为 s。按定义

$$(A^d)_{i,j} = \sum_{k_1} \sum_{k_2} \cdots \sum_{k_{d-1}} A_{i,k_1} A_{k_1,k_2} \cdots A_{k_{d-1},j}$$

  由于稀疏性，复杂度为 $O(s^{d-1})$

- 对于 x^d，存在次数为 $\Theta(\sqrt{d})$ 的逼近多项式，因此结果可改进到 $s^{O(\sqrt{d})}$ [Sachdeva & Vishnoi, 2014]
- 该问题是 BQP-完全问题 [Janzing & Wocjan, 2007]

例子：矩阵幂次 A^d

经典算法：

- 设 A 的稀疏度为 s。按定义

$$(A^d)_{i,j} = \sum_{k_1} \sum_{k_2} \cdots \sum_{k_{d-1}} A_{i,k_1} A_{k_1,k_2} \cdots A_{k_{d-1},j}$$

  由于稀疏性，复杂度为 $O(s^{d-1})$

- 对于 x^d，存在次数为 $\Theta(\sqrt{d})$ 的逼近多项式，因此结果可改进到 $s^{O(\sqrt{d})}$ [Sachdeva & Vishnoi, 2014]
- 该问题是 BQP-完全问题 [Janzing & Wocjan, 2007]
- 我们的结果：$\widetilde{\Omega}((s/2)^{(\sqrt{d}-1)/6})$

例子：矩阵幂次 A^d

经典算法：

- 设 A 的稀疏度为 s。按定义

$$(A^d)_{i,j} = \sum_{k_1} \sum_{k_2} \cdots \sum_{k_{d-1}} A_{i,k_1} A_{k_1,k_2} \cdots A_{k_{d-1},j}$$

  由于稀疏性，复杂度为 $O(s^{d-1})$

- 对于 x^d，存在次数为 $\Theta(\sqrt{d})$ 的逼近多项式，因此结果可改进到 $s^{O(\sqrt{d})}$ [Sachdeva & Vishnoi, 2014]
- 该问题是 BQP-完全问题 [Janzing & Wocjan, 2007]
- 我们的结果：$\widetilde{\Omega}((s/2)^{(\sqrt{d}-1)/6})$

例子：矩阵幂次 A^d

经典算法：

- 设 A 的稀疏度为 s。按定义

$$(A^d)_{i,j} = \sum_{k_1} \sum_{k_2} \cdots \sum_{k_{d-1}} A_{i,k_1} A_{k_1,k_2} \cdots A_{k_{d-1},j}$$

  由于稀疏性，复杂度为 $O(s^{d-1})$

- 对于 x^d，存在次数为 $\Theta(\sqrt{d})$ 的逼近多项式，因此结果可改进到 $s^{O(\sqrt{d})}$ [Sachdeva & Vishnoi, 2014]
- 该问题是 BQP-完全问题 [Janzing & Wocjan, 2007]
- 我们的结果：$\widetilde{\Omega}((s/2)^{(\sqrt{d}-1)/6})$

量子算法：

- 复杂度上界 $O(s\sqrt{d}/\varepsilon)$ [Gilyén, Su, Low, Wiebe, 2018]

例子：矩阵幂次 A^d

经典算法：

- 设 A 的稀疏度为 s。按定义

$$(A^d)_{i,j} = \sum_{k_1} \sum_{k_2} \cdots \sum_{k_{d-1}} A_{i,k_1} A_{k_1,k_2} \cdots A_{k_{d-1},j}$$

  由于稀疏性，复杂度为 $O(s^{d-1})$

- 对于 x^d，存在次数为 $\Theta(\sqrt{d})$ 的逼近多项式，因此结果可改进到 $s^{O(\sqrt{d})}$ [Sachdeva & Vishnoi, 2014]
- 该问题是 BQP-完全问题 [Janzing & Wocjan, 2007]
- 我们的结果：$\widetilde{\Omega}((s/2)^{(\sqrt{d}-1)/6})$

量子算法：

- 复杂度上界 $O(s\sqrt{d}/\varepsilon)$ [Gilyén, Su, Low, Wiebe, 2018]
- 我们的结果：复杂度下界 $\Omega(\sqrt{d})$

一般性结果

设 f 连续，A 稀疏厄米，则计算 $f(A)_{i,j} \pm \varepsilon$ 的复杂度如下

	量子算法	经典算法
复杂度上界	$O(sd/\varepsilon)$	$O(s^{d-1})$
复杂度下界	$\Omega(d)$	$\Omega((s/2)^{(d-1)/6})$

其中 $d = \widetilde{\deg}_\varepsilon(f)$。

关键定理

定理

设 $f(x):[-1,1]\to[-1,1]$ 是连续函数，设 $f_{\mathrm{odd}}(x), f_{\mathrm{even}}(x)$ 是奇、偶部分。则

- 存在对称的三对角阵 A 满足 $\|A\|\le 1$ 使得 $f(A)_{1,n}=\varepsilon$，其中 $n=\widetilde{\deg}_{\varepsilon}(f_{\mathrm{odd}})+O(1)$
- 存在对称的三对角阵 A 满足 $\|A\|\le 1$ 使得 $f(A)_{2,n-1}=\varepsilon$，其中 $n=\widetilde{\deg}_{\varepsilon}(f_{\mathrm{even}})+O(1)$

证明：线性半无限规划问题 + 对偶多项式方法 + 三对角阵的性质。 □

量子算法的复杂度下界

奇偶性判定问题（Parity problem）：给定 $x_1, \ldots, x_n \in \{0,1\}$，计算 $x_1 \oplus \cdots \oplus x_n$。经典/量子算法复杂度都为 $\Theta(n)$

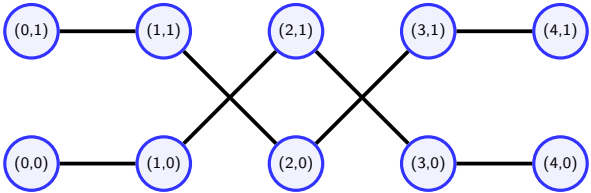
量子算法的复杂度下界

奇偶性判定问题（Parity problem）：给定 $x_1, \ldots, x_n \in \{0,1\}$，计算 $x_1 \oplus \cdots \oplus x_n$。经典/量子算法复杂度都为 $\Theta(n)$

构造带权图 G：

- **顶点**：(i,t)，其中 $i \in \{0,1,\ldots,n\}, t \in \{0,1\}$
- **边**：$(i-1,t)$ 和 $(i, t \oplus x_i)$ 之间存在一条边

例如 $(x_1, x_2, x_3, x_4) = (0,1,1,0)$，则 G 为



量子算法的复杂度下界

本质上，G 由两条道路构成

$$(0,0)-(1,x_0)-(2,x_0\oplus x_1)-\cdots-(n,x_0\oplus\cdots\oplus x_{n-1})$$
$$(0,1)-(1,1\oplus x_0)-(2,1\oplus x_0\oplus x_1)-\cdots-(n,1\oplus x_0\oplus\cdots\oplus x_{n-1})$$

量子算法的复杂度下界

本质上，G 由两条道路构成

$$(0,0)-(1,x_0)-(2,x_0\oplus x_1)-\cdots-(n,x_0\oplus\cdots\oplus x_{n-1})$$
$$(0,1)-(1,1\oplus x_0)-(2,1\oplus x_0\oplus x_1)-\cdots-(n,1\oplus x_0\oplus\cdots\oplus x_{n-1})$$

设 A 是图的邻接矩阵（本质上是两个三对角型矩阵），则

- **情形 1**：若 $x_1\oplus x_2\oplus\cdots\oplus x_n=0$，则 $\langle 0,0|f(A)|n,1\rangle=0$

量子算法的复杂度下界

本质上，G 由两条道路构成

$$(0,0)-(1,x_0)-(2,x_0\oplus x_1)-\cdots-(n,x_0\oplus\cdots\oplus x_{n-1})$$
$$(0,1)-(1,1\oplus x_0)-(2,1\oplus x_0\oplus x_1)-\cdots-(n,1\oplus x_0\oplus\cdots\oplus x_{n-1})$$

设 A 是图的邻接矩阵（本质上是两个三对角型矩阵），则

- **情形 1**：若 $x_1\oplus x_2\oplus\cdots\oplus x_n=0$，则 $\langle 0,0|f(A)|n,1\rangle=0$
- **情形 2**：若 $x_1\oplus x_2\oplus\cdots\oplus x_n=1$，则希望选取合适的权重，使得 $\langle 0,0|f(A)|n,1\rangle\geq\varepsilon$，权重由关键定理给出

经典算法的复杂度下界

Forrelation 问题 (Aaronson & Ambainis, 2015)：

给定 $g_1, g_2 : \{0,1\}^n \to \{\pm 1\}$，令 $D_i = \mathrm{diag}(g_i(x) : x \in \{0,1\}^n)$，$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$。

设

$$\begin{aligned} \Phi(g_1, g_2) &:= \langle 0^n | H^{\otimes n} D_1 H^{\otimes n} D_2 H^{\otimes n} | 0^n \rangle \\ &= \frac{1}{2^{3n/2}} \sum_{x,y \in \{0,1\}^n} (-1)^{x \cdot y} f(x) g(y). \end{aligned}$$

目标是计算 $\Phi(g_1, g_2) \pm 1/3$

经典算法的复杂度下界

Forrelation 问题 (Aaronson & Ambainis, 2015)：

给定 $g_1, g_2 : \{0,1\}^n \to \{\pm 1\}$，令 $D_i = \mathrm{diag}(g_i(x) : x \in \{0,1\}^n)$，$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$。

设

$$\begin{aligned} \Phi(g_1, g_2) &:= \langle 0^n | H^{\otimes n} D_1 H^{\otimes n} D_2 H^{\otimes n} | 0^n \rangle \\ &= \frac{1}{2^{3n/2}} \sum_{x,y \in \{0,1\}^n} (-1)^{x \cdot y} f(x) g(y). \end{aligned}$$

目标是计算 $\Phi(g_1, g_2) \pm 1/3$

关于该问题，经典算法的复杂度下界为 $\Omega(\sqrt{2^n}/n)$，量子算法的复杂度上界为 $O(1)$

Feynman 的 Clock 构造法

设 $U = U_{N-1} \cdots U_2 U_1$ 是一个酉算子，令

$$A = \begin{pmatrix} 0 & b_1 U_1^\dagger & & \\ b_1 U_1 & 0 & b_2 U_2^\dagger & \\ & b_2 U_2 & \ddots & \ddots \\ & & \ddots & \ddots \end{pmatrix}$$

Feynman 的 Clock 构造法

设 $U = U_{N-1} \cdots U_2 U_1$ 是一个酉算子，令

$$A = \begin{pmatrix} 0 & b_1 U_1^\dagger & & \\ b_1 U_1 & 0 & b_2 U_2^\dagger & \\ & b_2 U_2 & \ddots & \ddots \\ & & \ddots & \ddots \end{pmatrix}$$

设 $|\psi_t\rangle := |t\rangle \otimes U_t \cdots U_1 |0\rangle$，则

$$A|\psi_t\rangle = b_{t-1}|\psi_{t-1}\rangle + b_{t+1}|\psi_{t+1}\rangle$$

因此在子空间 $\{|\psi_t\rangle : t = 0, 1, \ldots, N-1\}$ 中，A 是一个三对角阵

经典算法的复杂度下界

在 Forrelation 问题中，$U = H^{\otimes n} D_1 H^{\otimes n} D_2 H^{\otimes n}$，为确保 A 的稀疏性，视

$$H^{\otimes n} = (H \otimes I \otimes \cdots \otimes I)(I \otimes H \otimes \cdots \otimes I) \cdots (I \otimes I \otimes \cdots \otimes H)$$

经典算法的复杂度下界

在 Forrelation 问题中，$U = H^{\otimes n} D_1 H^{\otimes n} D_2 H^{\otimes n}$，为确保 A 的稀疏性，视

$$H^{\otimes n} = (H \otimes I \otimes \cdots \otimes I)(I \otimes H \otimes \cdots \otimes I) \cdots (I \otimes I \otimes \cdots \otimes H)$$

这时 $N = 3n + 2$,

$$\begin{aligned} |\psi_0\rangle &= |0\rangle \otimes |0\rangle \\ |\psi_{N-1}\rangle &= |N-1\rangle \otimes H^{\otimes n} D_1 H^{\otimes n} D_2 H^{\otimes n} |0\rangle \end{aligned}$$

经典算法的复杂度下界

在 Forrelation 问题中，$U = H^{\otimes n} D_1 H^{\otimes n} D_2 H^{\otimes n}$，为确保 A 的稀疏性，视

$$H^{\otimes n} = (H \otimes I \otimes \cdots \otimes I)(I \otimes H \otimes \cdots \otimes I) \cdots (I \otimes I \otimes \cdots \otimes H)$$

这时 $N = 3n + 2$,

$$\begin{aligned} |\psi_0\rangle &= |0\rangle \otimes |0\rangle \\ |\psi_{N-1}\rangle &= |N-1\rangle \otimes H^{\otimes n} D_1 H^{\otimes n} D_2 H^{\otimes n} |0\rangle \end{aligned}$$

令 $|\phi_{N-1}\rangle = |N-1\rangle \otimes |0\rangle$，则

$$\langle \phi_{N-1} | f(A) | \psi_0 \rangle = \langle \psi_{N-1} | f(A) | \psi_0 \rangle \cdot \Phi(g_1, g_2)$$

经典算法的复杂度下界

在 Forrelation 问题中，$U = H^{\otimes n} D_1 H^{\otimes n} D_2 H^{\otimes n}$，为确保 A 的稀疏性，视

$$H^{\otimes n} = (H \otimes I \otimes \cdots \otimes I)(I \otimes H \otimes \cdots \otimes I) \cdots (I \otimes I \otimes \cdots \otimes H)$$

这时 $N = 3n + 2$,

$$\begin{aligned} |\psi_0\rangle &= |0\rangle \otimes |0\rangle \\ |\psi_{N-1}\rangle &= |N-1\rangle \otimes H^{\otimes n} D_1 H^{\otimes n} D_2 H^{\otimes n} |0\rangle \end{aligned}$$

令 $|\phi_{N-1}\rangle = |N-1\rangle \otimes |0\rangle$，则

$$\begin{array}{ccccc} \langle \phi_{N-1} | f(A) | \psi_0 \rangle & = & \langle \psi_{N-1} | f(A) | \psi_0 \rangle & \cdot & \Phi(g_1, g_2) \\ \downarrow & & \downarrow & & \downarrow \\ f(A) \text{ 的一个分量} & & \text{易} & & \text{难} \end{array}$$

第一部分总结

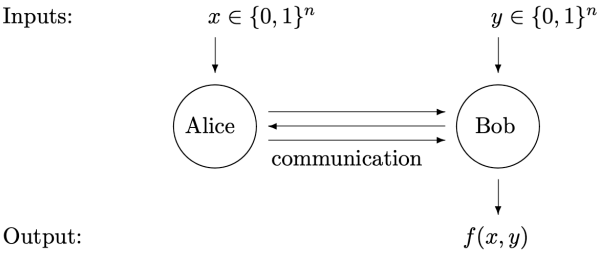
- 对于矩阵函数问题，我们有

	量子算法	经典算法
复杂度上界	$O(sd/\varepsilon)$	$O(s^{d-1})$
复杂度下界	$\Omega(d)$	$\Omega((s/2)^{(d-1)/6})$

- 关于逼近次数 d，证明了量子算法的最优性
- 对于矩阵函数问题，证明了量子和经典算法的差距是指数级
- 对精度 ε 的下界估计，$\Omega(1/\varepsilon)$?

通信复杂度 (communication complexity)

- 由姚期智先生提出，在很多领域有着重要应用，尤其是在复杂度下界证明方面。
- 问题：Alice 有 $x = (x_1, \ldots, x_n) \in \{0,1\}^n$, Bob 有 $y = (y_1, \ldots, y_n) \in \{0,1\}^n$, 目标是计算 $f(x, y)$。



- 通信复杂度:= 计算 $f(x, y)$ 所传递的比特数。

通信复杂度

局部计算代价 (也即 Alice 或 Bob 本身计算的代价) 不计入通信复杂度中。

在量子情形下，也有类似的定义，这时传递的是量子信息 (如量子态)，量子通信复杂度指代的是量子比特的传递个数。

例 (正交性问题, Disjointness problem)

Alice 有 $(x_1, \ldots, x_n)$, Bob 有 $(y_1, \ldots, y_n)$, 目标是判定是否存在 i 使得 $x_i = y_i = 1$.

$$\text{经典 vs 量子} = \Theta(n) \text{ vs } \Theta(\sqrt{n})$$

通信复杂度: multi-player case

Multi-player 情形：设 $i \in \{1, \ldots, s\}$, player P_i 有矩阵 $A_i \in \mathbb{R}^{m_i \times n}$ 和向量 $b_i \in \mathbb{R}^{m_i}$, 令

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_s \end{pmatrix}, \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_s \end{pmatrix}.$$

Coordinator model

假定存在 coordinator C 可与 player P_i 双向交流

$$\begin{tikzcd}
P_1 \arrow[dr, leftrightarrow] & P_2 \arrow[dr, leftrightarrow] & P_3 \arrow[d, leftrightarrow] & \cdots \arrow[dl, leftrightarrow] & P_s \arrow[dll, leftrightarrow] \\
 & & C & &
\end{tikzcd}$$

目标：给定函数 $f(x)$, coordinator C 输出量子态 $|f(A)b\rangle \pm \varepsilon$。

主要结果

定理 (QSVT w.r.t. communication complexity)

In the quantum coordinator model, there is a quantum protocol for the referee to use

$$\widetilde{U} = \begin{pmatrix} f(A/\alpha) & * \\ * & * \end{pmatrix}$$

once with $O(sd\log n)$ *qubits communication, where* $d = \widetilde{\deg}_\varepsilon(f)$ *and*

$$\alpha = \sqrt{\sum_{i=1}^{s} \|A_i\|^2} = O(\sqrt{s}\|A\|).$$

证明简述: LCU 方法回顾

给定酉矩阵 $U_1, \ldots, U_s$ 和正实数 $\alpha_1, \ldots, \alpha_s$, 目标是实现 $\sum \alpha_i U_i |\psi\rangle$.

- 初始态，令 $\alpha = \sum_i \alpha_i$ 和 $V|0\rangle = \frac{1}{\sqrt{\alpha}} \sum_{i=1}^{s} \sqrt{\alpha_i} |i\rangle$. 制备

$$\frac{1}{\sqrt{\alpha}} \sum_{i=1}^{s} \sqrt{\alpha_i} |i\rangle |\psi\rangle.$$

- 受控作用 $\sum_i |i\rangle\langle i| \otimes U_i$

$$\frac{1}{\sqrt{\alpha}} \sum_{i=1}^{s} \sqrt{\alpha_i} |i\rangle\, U_i |\psi\rangle.$$

- 使用 V^{-1}

$$\frac{1}{\alpha} \sum_{i=1}^{s} \alpha_i |0\rangle\, U_i |\psi\rangle + |\perp\rangle.$$

证明简述

1. P_i 构造 $U_i = \begin{pmatrix} A_i/\|A_i\| & * \\ * & * \end{pmatrix}$，回顾 $A = \begin{pmatrix} A_1 \\ \vdots \\ A_s \end{pmatrix}$
2. 利用 LCU 方法来构造 A 的 block-encoding，也即实现 $\sum_i \|A_i\| |i\rangle \otimes U_i$:

$$U = \left(\sum_{i=1}^{s} |i\rangle\langle i| \otimes U_i \right) (V \otimes I_2 \otimes I_n)$$

   其中 $V|0\rangle = \frac{1}{\alpha} \sum_{i=1}^{s} \|A_i\| \, |i\rangle$.
3. QSVT 的量子电路形如:

$$\widetilde{U} = W_0 U W_1 U^\dagger W_2 U W_3 U^\dagger \cdots W_d U$$

应用：线性回归问题 (取 $f(x) \approx 1/x$)

推论

求解线性回归问题的量子通信复杂度为 $\widetilde{O}(s^{1.5}\kappa)$，其中 κ 是矩阵 A 的条件数。

应用：线性回归问题 (取 $f(x) \approx 1/x$)

推论

求解线性回归问题的量子通信复杂度为 $\widetilde{O}(s^{1.5}\kappa)$，其中 κ 是矩阵 A 的条件数。

注：由量子奇异值变换，求解线性回归问题的时间/查询复杂度为 $\widetilde{O}(T_A\alpha/\sigma_{\min})$，其中 $\sigma_{\min}$ 是最小非零奇异值，T_A 是构造 block-encoding

$$U = \begin{pmatrix} A/\alpha & * \\ * & * \end{pmatrix}$$

的代价。在通信复杂度情形下，其实有 $T_A = O((s/\sigma_{\min})\log n)$, $\alpha = O(\sqrt{s}\sigma_{\max})$。

应用：线性回归问题 (取 $f(x) \approx 1/x$)

推论

求解线性回归问题的量子通信复杂度为 $\widetilde{O}(s^{1.5}\kappa)$，其中 κ 是矩阵 A 的条件数。

注：由量子奇异值变换，求解线性回归问题的时间/查询复杂度为 $\widetilde{O}(T_A\alpha/\sigma_{\min})$，其中 $\sigma_{\min}$ 是最小非零奇异值，T_A 是构造 block-encoding

$$U = \begin{pmatrix} A/\alpha & * \\ * & * \end{pmatrix}$$

的代价。在通信复杂度情形下，其实有 $T_A = O((s/\sigma_{\min})\log n)$, $\alpha = O(\sqrt{s}\sigma_{\max})$。

一个好处：对于 QSVT，“Block-encoding 假定”在量子通信复杂度下很容易实现。

查询复杂度和通信复杂度的关系

- 查询复杂度 (布尔函数情形)：给定布尔函数 f 和一个布尔输入 $x = (x_1, \ldots, x_n)$，目标是计算 $f(x)$。假定只有一个 Oracle $O : i \to x_i$。需要调用多少次 O。

查询复杂度和通信复杂度的关系

- 查询复杂度 (布尔函数情形)：给定布尔函数 f 和一个布尔输入 $x = (x_1, \ldots, x_n)$，目标是计算 $f(x)$。假定只有一个 Oracle $O : i \to x_i$。需要调用多少次 O。
- 通信复杂度：Alice 有 $x = (x_1, \ldots, x_n)$，Bob 有 $y = (y_1, \ldots, y_n)$，目标是计算 $f(x, y)$。

查询复杂度和通信复杂度的关系

- 查询复杂度 (布尔函数情形)：给定布尔函数 f 和一个布尔输入 $x = (x_1, \ldots, x_n)$，目标是计算 $f(x)$。假定只有一个 Oracle $O : i \to x_i$。需要调用多少次 O。
- 通信复杂度：Alice 有 $x = (x_1, \ldots, x_n)$，Bob 有 $y = (y_1, \ldots, y_n)$，目标是计算 $f(x, y)$。
- Buhrman, Cleve, Wigderson [STOC '98]:
  设 $g : \{0,1\}^n \to \{0,1\}$，$\star$ 是一个二元运算 (例如 $\oplus, \wedge$)，令 $f(x, y) := g(x \star y)$。如果存在一个查询复杂度为 T 的量子算法可计算 g，则存在一个量子通信方案，其通信复杂度为 $C = T(2 \log n + 4)$，可计算 f。

查询复杂度和通信复杂度的关系

- 查询复杂度 (布尔函数情形)：给定布尔函数 f 和一个布尔输入 $x = (x_1, \ldots, x_n)$，目标是计算 $f(x)$。假定只有一个 Oracle $O : i \to x_i$。需要调用多少次 O。
- 通信复杂度：Alice 有 $x = (x_1, \ldots, x_n)$，Bob 有 $y = (y_1, \ldots, y_n)$，目标是计算 $f(x, y)$。
- Buhrman, Cleve, Wigderson [STOC '98]:
  设 $g : \{0,1\}^n \to \{0,1\}$，$\star$ 是一个二元运算 (例如 $\oplus, \wedge$)，令 $f(x, y) := g(x \star y)$。如果存在一个查询复杂度为 T 的量子算法可计算 g，则存在一个量子通信方案，其通信复杂度为 $C = T(2 \log n + 4)$，可计算 f。
- 这一结果的价值是两方面的：
  1. 可用量子查询算法来设计量子通信方案；
  2. 可用量子通信复杂度来估计量子查询复杂度的下界。

一个例子

搜索问题 (查询复杂度)：计算布尔函数 $x_1 \vee \cdots \vee x_n$。

一个例子

搜索问题 (查询复杂度)：计算布尔函数 $x_1 \vee \cdots \vee x_n$。

正交性问题 (通信复杂度)：Alice 有 $(x_1, \ldots, x_n)$, Bob 有 $(y_1, \ldots, y_n)$，目标是判定是否存在 i 使得 $x_i = y_i = 1$。也即计算布尔函数 $(x_1 \wedge y_1) \vee \cdots \vee (x_n \wedge y_n)$。

一个例子

搜索问题 (查询复杂度)：计算布尔函数 $x_1 \vee \cdots \vee x_n$。

正交性问题 (通信复杂度)：Alice 有 $(x_1, \ldots, x_n)$, Bob 有 $(y_1, \ldots, y_n)$，目标是判定是否存在 i 使得 $x_i = y_i = 1$。也即计算布尔函数 $(x_1 \wedge y_1) \vee \cdots \vee (x_n \wedge y_n)$。

利用 Grover 算法可得到一个量子通信方案求解正交性问题，复杂度为 $O(\sqrt{n} \log n)$，可改进到 $O(\sqrt{n})$ [Aaronson, Ambainis FOCS '03]。

一个例子

搜索问题 (查询复杂度)：计算布尔函数 $x_1 \vee \cdots \vee x_n$。

正交性问题 (通信复杂度)：Alice 有 $(x_1, \ldots, x_n)$, Bob 有 $(y_1, \ldots, y_n)$，目标是判定是否存在 i 使得 $x_i = y_i = 1$。也即计算布尔函数 $(x_1 \wedge y_1) \vee \cdots \vee (x_n \wedge y_n)$。

利用 Grover 算法可得到一个量子通信方案求解正交性问题，复杂度为 $O(\sqrt{n}\log n)$，可改进到 $O(\sqrt{n})$ [Aaronson, Ambainis FOCS '03]。

正交性问题的通信复杂度下界为 $\Omega(\sqrt{n})$, 因此可得到搜索问题的查询复杂度下界为 $\Omega(\sqrt{n}/\log n)$，可改进到 $\Omega(\sqrt{n})$ [Razborov, 2003]。

量子查询算法

设 A 是一个矩阵，且存在酉矩阵满足

$$U = \begin{pmatrix} A/\alpha & * \\ * & * \end{pmatrix}$$

一个查询复杂度为 T 的量子算法形如:

$$W_1 \widetilde{U} W_2 \widetilde{U} W_3 \widetilde{U} \cdots W_T \widetilde{U} W_{T+1},$$

其中 W_i 是与 U 无关的酉矩阵，$\widetilde{U} \in \{U, U^{-1}, cU, cU^{-1}\}$.

主要结论

定理 (关于矩阵)

设 *Alice* 和 *Bob* 分别有矩阵 A_1, A_2 和酉矩阵 $U_1 = \begin{pmatrix} A_1/\alpha_1 & * \\ * & * \end{pmatrix}$, $U_2 = \begin{pmatrix} A_2/\alpha_2 & * \\ * & * \end{pmatrix}$. 令 $A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix} \in \mathbb{C}^{m\times n}$, 则存在一个量子通信方案可让 *Alice* 和 *Bob* 使用酉矩阵 $U = \begin{pmatrix} A/\sqrt{\alpha_1^2+\alpha_2^2} & * \\ * & * \end{pmatrix}$。调用一次的量子通信复杂度为 $O(\log(mn))$.

主要结论

定理 (关于向量)

设 *Alice* 和 *Bob* 分别有向量 b_1, b_2 和酉矩阵 W_1, W_2 可制备 $|b_1\rangle, |b_2\rangle$. 令 $b = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \in \mathbb{C}^m$，则存在一个量子通信方案可让 *Alice* 和 *Bob* 使用酉矩阵 W 可制备 $|b\rangle$, 调用一次的量子通信复杂度为 $O(\log(m))$.

主要结论

定理

假定同上，如果存在一个查询复杂度为 T 的量子算法求解矩阵-向量 A, b 的问题，则存在一个量子通信方案解决同一问题，其复杂度为 $O(T\log(mn))$。

主要结论

定理

假定同上，如果存在一个查询复杂度为 T 的量子算法求解矩阵-向量 A, b 的问题，则存在一个量子通信方案解决同一问题，其复杂度为 $O(T\log(mn))$。

一个特殊情况：Alice 有 A, Bob 有 b. 这时算法

$$W_1 \widetilde{U} W_2 \widetilde{U} W_3 \widetilde{U} \cdots W_T \widetilde{U} W_{T+1}$$

中 Alice 可调用 $\widetilde{U}$，Bob 可调用 W_i。

一些例子：求解线性方程组

求解线性方程组：$A\mathbf{x} = b$. 关于该问题，其查询复杂度下界为 $\Omega(\kappa)$，其中 κ 是 A 的条件数。

一些例子：求解线性方程组

求解线性方程组：$A\mathbf{x} = b$. 关于该问题，其查询复杂度下界为 $\Omega(\kappa)$，其中 κ 是 A 的条件数。

考虑正交性问题：Alice 有 $(x_1, \ldots, x_n)$, Bob 有 $(y_1, \ldots, y_n)$，目标是判定是否存在 i 使得 $x_i = y_i = 1$。

一些例子：求解线性方程组

求解线性方程组：$A\mathbf{x} = b$. 关于该问题，其查询复杂度下界为 $\Omega(\kappa)$，其中 κ 是 A 的条件数。

考虑正交性问题：Alice 有 $(x_1, \ldots, x_n)$, Bob 有 $(y_1, \ldots, y_n)$，目标是判定是否存在 i 使得 $x_i = y_i = 1$。

构造 A, b：A 是对角阵：$A_{ii} = \begin{cases} 1/\sqrt{n} & x_i = 1 \\ 1 & x_i = 0 \end{cases}$，$b$ 是向量 $(y_1, \ldots, y_n)^T$。则方程解为

$$x_i = \begin{cases} \sqrt{n} & x_i = y_i = 1 \\ 1 & x_i = 0, y_i = 1 \\ 0 & y_i = 0 \end{cases}$$

一些例子：求解线性方程组

求解线性方程组：$A\mathbf{x} = b$. 关于该问题，其查询复杂度下界为 $\Omega(\kappa)$，其中 κ 是 A 的条件数。

考虑正交性问题：Alice 有 $(x_1, \ldots, x_n)$, Bob 有 $(y_1, \ldots, y_n)$，目标是判定是否存在 i 使得 $x_i = y_i = 1$。

构造 A, b：A 是对角阵：$A_{ii} = \begin{cases} 1/\sqrt{n} & x_i = 1 \\ 1 & x_i = 0 \end{cases}$，$b$ 是向量 $(y_1, \ldots, y_n)^T$。则方程解为

$$x_i = \begin{cases} \sqrt{n} & x_i = y_i = 1 \\ 1 & x_i = 0, y_i = 1 \\ 0 & y_i = 0 \end{cases}$$

如果可得到解的量子态，则观测时将以概率 $\approx 1/2$ 得到 i 满足 $x_i = y_i = 1$. 这时 $\kappa = \sqrt{n}$. 因此，求解线性方程组的查询复杂度下界为 $\Omega(\kappa/\log n)$。

一些例子：矩阵指数

给定矩阵 A 满足 $\|A\| \leq 1$，计算 $e^{At}b$。复杂度上界为 $O(e^t)$。

一些例子：矩阵指数

给定矩阵 A 满足 $\|A\| \leq 1$，计算 $e^{At}b$。复杂度上界为 $O(e^t)$。
根据正交性问题，构造 A, b：A 是对角阵，把 x 放在对角线上。b 还是向量 $(y_1, \ldots, y_n)^T$。取 $t = \frac{1}{2}\ln(n)$。则

$$(e^{At}b)_i = \begin{cases} e^t & x_i = y_i = 1 \\ 1 & x_i = 0, y_i = 1 \\ 0 & y_i = 0 \end{cases}$$

一些例子：矩阵指数

给定矩阵 A 满足 $\|A\| \le 1$，计算 $e^{At}b$。复杂度上界为 $O(e^t)$。
根据正交性问题，构造 A, b：A 是对角阵，把 x 放在对角线上。b 还是向量 $(y_1, \ldots, y_n)^T$。取 $t = \frac{1}{2}\ln(n)$。则

$$(e^{At}b)_i = \begin{cases} e^t & x_i = y_i = 1 \\ 1 & x_i = 0, y_i = 1 \\ 0 & y_i = 0 \end{cases}$$

如果有 $e^{At}b$ 的量子态，则观测时将以概率 $\approx 1/2$ 得到 i 满足 $x_i = y_i = 1$. 这时 $e^t = \sqrt{n}$. 因此，计算 e^{At} 的查询复杂度下界为 $\Omega(e^t/\log n)$。

第二部分总结

- 给出了量子通信复杂度模型下的 QSVT 的实现方案
  $\Rightarrow$ 有望从通信复杂度角度得到更多关于量子优势的发现
- 关于矩阵函数，建立了量子查询复杂度和通信复杂度的关系
  $\Rightarrow$ 提供了证明量子查询复杂度的一个新方法

第二部分总结

- 给出了量子通信复杂度模型下的 QSVT 的实现方案
  $\Rightarrow$ 有望从通信复杂度角度得到更多关于量子优势的发现

- 关于矩阵函数，建立了量子查询复杂度和通信复杂度的关系
  $\Rightarrow$ 提供了证明量子查询复杂度的一个新方法

非 常 感 谢!