arXiv:2303.10244v1 [quant-ph] 17 Mar 2023

一个奇特技巧收紧量子对抗者界，尤其适用于成功概率接近 $1/2$ 的情形

Duyal Yolcu*

2023年3月21日

摘要

函数求值的教科书式对抗界 [1, 5, 6] 指出，要在量子查询模型中以 $\frac{1}{2}+\delta$ 的成功概率求出函数 $f\colon\ D \to C$，至少需要$(2\delta - \sqrt{1-4\delta^2})$Adv (f) 次查询，其中 Adv (f) 是某个优化问题的最优值。当$\delta \ll 1$时，即使采用重复运行并多数表决的论证，也只能得到 $\theta\left(\delta^2 \text{Adv}\,(f)\right)$ 的界。相比之下，多项式方法有时可以证明一个在 $\delta \to 0$时不趋于 0 的界。我们改进了依赖于 δ 的前置因子，得到 2δAdv (f)的界。证明思路是“将输出条件转化为输入条件”：对于一个将完全与输入无关的初始态变换为无法完美区分的最终态的算法，我们通过投影到“正确的”最终子空间并进行反计算，构造出一个查询次数相同的算法，将无法完美地与输入无关的初始态变换为可完美区分的最终态。由此得到的、依赖于 δ的初始格拉姆矩阵条件，与原算法对最终格拉姆矩阵的条件相比，使我们能够推出收紧后的前置因子。

1 概述

- 第 2 节介绍量子查询模型中的函数求值问题；表1列出了其中定义的符号，供读者参考。
- 第3节证明引理 1，阐述了本文的核心新思想：假设存在一个能够解决此类问题的算法，我们可以修改其作用的初始态，使得到的修改后的最终态能够以 0 的错误概率解决该问题。

*https://github.com/qudent

- 表 2 介绍了更通用的线性代数记号，这些记号与后续各节相关。第4节证明引理 2，这是一个关于矩阵范数的技术性引理，我们可以将其代入对抗界。证明用到了来自 [4] 的一个结果。

- 第5节介绍用于状态转换的对抗界。

- 第6节汇总前面的结果，得出定理 3，也就是本文的核心结果。

- 第7节讨论该结果，并将其与之前的证明及其他证明进行比较。

2 问题：函数求值

$f\colon\ D \to C$	目标函数，$D \subseteq \mathbb{Z}_2^n$, $n \in \mathbb{N}$, $\lvert C\rvert < \infty$
$x \in D$	输入值
$\mathbb{C}^Q$	查询空间，$Q := \{0, 1, \ldots n\}$
$O_x \in \mathbb{C}^{Q\times Q}$	输入 $x \in D$ 对应的酉预言机如方程1–2所示
$\mathbb{C}^W$	辅助空间，W 任意地大型
$U^0, \ldots, U^T \in \mathbb{C}^{(Q\times W)\times(Q\times W)}$	初始，…，最终算法 unitary，如公式 3 所示
$\lvert\xi\rangle \in \mathbb{C}^{Q\times W}$	初始态
$\lvert\tau_x\rangle \in \mathbb{C}^{Q\times W}$	输入 $x \in D$ 的最终态，如公式 3
P_c	最终测量中的投影算子，测量结果 $c \in C$，公式—式 4
$\left\lvert\sqrt{p_{\text{true}}}\right\rangle \in \mathbb{C}^D$	元素为平方根的向量成功概率的平方根，即 $\left\langle x\middle\lvert\sqrt{p_{\text{true}}}\right\rangle := \left\lVert P_{f(x)}\lvert\tau_x\rangle\right\rVert$
$\delta > 0$	成功偏差 ，即.....的下界成功概率减去 $1/2$，对于全部 $x \in D$ 如公式 4 所示

表1：第 2 节中引入的符号。表 2 包含更多在第4节之前未使用的符号。

我们介绍该模型；表1列出了本节中引入的符号以供参考。我们将查询问题描述为由目标函数$f\colon\ D \to C$定义，其中 $D \subseteq \mathbb{Z}_2^n$ 是长度为 $n < \infty$ 的比特串集合， C 是一个有限集。我们定义查询空间 $\mathbb{C}^Q$，其中 $Q := \{0, 1, \ldots n\}$；在一个问题

实例中，输入 $x \in D$ 被编码在相位预言机酉算子 O_x: $\mathbb{C}^Q \to \mathbb{C}^Q$中，其定义如下:

$$O_x |j\rangle := (-1)^{x_j} |j\rangle \qquad \text{for } j < n, \tag{1}$$
$$O_x |n\rangle := |n\rangle . \tag{2}$$

求解该问题的量子查询算法作用于查询空间与辅助空间 $\mathbb{C}^W$ 的组合上，其中辅助空间可以任意大（换言之，计算机使用的内部存储器大小不受限制）。算法以一个与 $x \in D$ 无关的初始态 $|\xi\rangle \in \mathbb{C}^{Q\times W}$ 开始，并依次施加一系列酉算子 U^0、U^1、U^2、.....、U^T: $\mathbb{C}^{Q\times W} \to \mathbb{C}^{Q\times W}$ 这些酉算子与预言机酉算子 O_x 交替作用（其中 O_x 在辅助空间上起平凡作用 $\mathbb{C}^W$）。对于给定的 $x \in D$，这会得到一个状态

$$|\tau_x\rangle = U^T O_x U^{T-1} O_x \dots U^1 O_x U^0 |\xi\rangle . \tag{3}$$

该算法的目标是对于给定的 $\delta > 0$ 和任意 $x \in D$，以至多为 $1/2 - \delta$ 的错误概率确定 $f(x)$。根据标准量子信息论，[2] 我们不失一般性地可以假设，算法通过在施加最后一个酉算子后进行一次投影值测量（PVM）来实现这一目标，测量结果取自 C。因此，如果算法成功，就存在一组投影算子 $(P_c)_{c\in C}$，其中每个 P_c 都作用于 $\mathbb{C}^{Q\times W}$，$P_c P_{c'} = 0$ 对任意 $c \neq c'$ 均成立，并且

$$\left\| P_{f(x)} |\tau_x\rangle \right\|^2 \geq \frac{1}{2} + \delta \qquad \forall x \in D. \tag{4}$$

假设有一组 $|\tau_x\rangle$ 和 P_c，我们定义一个向量 $\left|\sqrt{p_{\text{true}}}\right\rangle \in \mathbb{C}^D$，其各项为成功概率的平方根，即

$$\langle x|\sqrt{p_{\text{true}}}\rangle := \left\| P_{f(x)} |\tau_x\rangle \right\|. \tag{5}$$

3 新引理：从完美初始态到完美最终态

至此，我们已经可以用下面的引理来正式阐述本文方法的新颖之处:

引理 1。给定 f: $D \to C$，考虑使用第 2 节所述的标准预言机计算 f 的问题。假设存在一个量子查询算法，能在 T 次查询内解决此问题，且成功偏差为 $\delta > 0$；也就是说，该查询算法根据公式 3 将 $|\xi\rangle$ 转换为 $(|\tau_x\rangle)_{x\in D}$，使得

[1]在传统设定中；正如我们将看到的，推广形式允许初始态依赖于输入。[2]更准确地说，根据延迟测量原理，以及辅助空间 $\mathbb{C}^W$ 可以任意大这一事实，任何量子正算子值测量（POVM）都可以通过一个酉算子来实现：该酉算子作用于初始化为某个确定态的辅助空间，并进行投影值测量，参见 [8]。

存在满足公式 4 的投影算子 $(P_c)_{c\in C}$，对应于该 δ。那么，存在归一化的修正初始态和最终态集合 $(|\xi'_x\rangle)_{x\in D}$、$(|\tau'_x\rangle)_{x\in D}$，使得

1. 将算法应用于 $(|\xi'_x\rangle)_{x\in D}$，会得到最终态 $(|\tau'_x\rangle)_{x\in D}$，即

$$|\tau'_x\rangle = U^T O_x U^{T-1} O_x \dots U^1 O_x U^0 |\xi'_x\rangle \qquad \forall x \in D, \tag{6}$$

2. 对应于不同函数值的状态 $(|\tau'_x\rangle)_{x\in D}$ 彼此正交，也就是说可以被完美区分：

$$\langle \tau'_x | \tau'_{x'} \rangle = 0 \qquad \forall x, x' \in D \colon f(x) \neq f(x'), \tag{7}$$

3. 修改后的初始态 $(|\xi'_x\rangle)_{x\in D}$ 与 $|\xi\rangle$高度重叠，具体而言，

$$\langle \xi | \xi'_x \rangle = \left\| P_{f(x)} |\tau_x\rangle \right\| = \langle x | \sqrt{p_{\text{succ}}} \rangle \geq \sqrt{1/2 + \delta} \qquad \forall x \in D. \tag{8}$$

证明。对于任意 $x \in D$，引入简写

$$A_x := U^T O_x U^{T-1} O_x \dots U^1 O_x U^0$$

表示酉的总演化算子，并定义

$$|\tau'_x\rangle := \frac{P_{f(x)} |\tau_x\rangle}{\left\| P_{f(x)} |\tau_x\rangle \right\|}, \tag{9}$$

$$|\xi'_x\rangle := A_x^\dagger |\tau'_x\rangle . \tag{10}$$

换句话说，我们通过将 $(|\tau_x\rangle)_{x\in D}$ 投影到“正确”的子空间并重新归一化，定义了 $(|\tau'_x\rangle)_{x\in D}$；而 $(|\xi'_x\rangle)_{x\in D}$ 则通过反计算定义。根据这些定义以及 A_x 是酉算子（即它的厄米共轭也是其逆算子）这一事实，性质1和2显然成立。为证明性质3，利用公式3和4计算得

$$\langle \xi | \xi'_x \rangle = \langle \xi | A_x^\dagger |\tau'_x\rangle = (A_x |\xi\rangle)^\dagger |\tau'_x\rangle = \langle \tau_x | \tau'_x \rangle \tag{11}$$

$$= \frac{\langle \tau_x | P_{f(x)} |\tau_x\rangle}{\left\| P_{f(x)} |\tau_x\rangle \right\|} = \left\| P_{f(x)} |\tau_x\rangle \right\| \geq \sqrt{1/2 + \delta}. \tag{12}$$

□

4 一个矩阵范数不等式

使用表 2 中的记号，本节的任务是证明以下引理，我们将用它来证明主要定理 3。

[3]我对这个证明并不满意，希望能找到一种更简单的方法——或许可以参考其他文献中的结果。

$\mathbb{H}^D$	厄米复数 $D \times D$的集合 矩阵
$\mathbb{S}^D$	半正定复数集合- 数 $D \times D$ 矩阵
$H[x, x']$	矩阵第 x行、第 x'列的元素 矩阵 H
$G_\xi \in \mathbb{S}^D$	Gram 状态集合矩阵 （$\|\xi_x\rangle$）$_{x\in D}$，即 $G_\xi[x, x'] :=$ $\langle\xi_x\|\xi_{x'}\rangle$；始终在 $\mathbb{S}^D$ by [4, 第 1.1 章，条目（vi）]
$H_1 \circ H_2$	Hadamard（逐项）乘积 矩阵 H_1、H_2
$\|H\|$	矩阵范数（最大奇异 值） $H \in \mathbb{C}$的 $^{D\times D}$

表 2：通用线性代数记号，从第4节开始相关。另请参见表1。

引理 2. 设 $G_{\xi'}$ 是状态集合 $(|\xi'_x\rangle)_{x\in D}$ 的格拉姆矩阵，该状态集合由引理 1 在某个 $\delta > 0$ 下得到，即满足该引理的性质 3，且对应某个归一化的 $|\xi\rangle \in \mathbb{C}^D$。那么对于任意 $\Gamma \in \mathbb{H}^D$,

$$2\delta\|\Gamma\| \leq \|\Gamma \circ G_{\xi'}\|. \tag{13}$$

我们首先将这个引理归约为其他引理。

思路。根据三角不等式,

$$\begin{aligned} \|\Gamma \circ |\sqrt{p_{\text{true}}}\rangle\langle\sqrt{p_{\text{true}}}|\| &= \|\Gamma \circ (G_{\xi'} - (G_{\xi'} - |\sqrt{p_{\text{true}}}\rangle\langle\sqrt{p_{\text{true}}}|))\| &(14)\\ &\leq \|\Gamma \circ G_{\xi'}\| + \|\Gamma \circ (G_{\xi'} - |\sqrt{p_{\text{true}}}\rangle\langle\sqrt{p_{\text{true}}}|)\|. &(15)\end{aligned}$$

这意味着

$$\|\Gamma \circ |\sqrt{p_{\text{true}}}\rangle\langle\sqrt{p_{\text{true}}}|\| - \|\Gamma \circ (G_{\xi'} - |\sqrt{p_{\text{true}}}\rangle\langle\sqrt{p_{\text{true}}}|)\| \leq \|\Gamma \circ G_{\xi'}\|. \tag{16}$$

引理3和引理4分别给出了左侧两个加项的下界。结合起来，它们意味着 $\|\Gamma \circ G_{\xi'}\|$ 的下界为

$$\left(2\min_{x\in D} |\langle x|\sqrt{p_{\text{true}}}\rangle|^2 - 1\right)\|\Gamma\|, \tag{17}$$

而它又以下式 $2\delta\|\Gamma\|$为下界。 □

接下来需要陈述并证明引理3和引理4。我们的方法关键依赖于 Schur 的一个定理，现不加证明地陈述如下:

定理 1（[4, 定理1.4.1]）。设 $\Gamma \in \mathbb{H}^D$ 为厄米矩阵，且 $S \in \mathbb{S}^D$为半正定矩阵。则

$$\|\Gamma \circ S\| \leq \max_{x\in D} S[x, x]\|\Gamma\|. \tag{18}$$

引理 3。设 $\left|\sqrt{p_{\text{true}}}\right\rangle \in \mathbb{C}^D$ 的所有元素均非零，且 $\Gamma \in \mathbb{H}^D$。则

$$\min_{x\in D} \left|\langle x|\sqrt{p_{\text{true}}}\rangle\right|^2 \|\Gamma\| \leq \|\Gamma \circ \left|\sqrt{p_{\text{true}}}\right\rangle \left\langle\sqrt{p_{\text{true}}}\right|\|. \tag{19}$$

证明。设 $\Gamma' := \Gamma \circ \left|\sqrt{p_{\text{true}}}\right\rangle \left\langle\sqrt{p_{\text{true}}}\right|$。令 $\left|\sqrt{p_{\text{true}}}^{-1}\right\rangle \in \mathbb{C}^D$ 为一个向量，其各个分量分别是 $\left|\sqrt{p_{\text{true}}}\right\rangle$ 对应分量的倒数。则该命题等价于

$$\left\|\Gamma' \circ \left|\sqrt{p_{\text{true}}}^{-1}\right\rangle \left\langle\sqrt{p_{\text{true}}}^{-1}\right|\right\| \leq \frac{\|\Gamma'\|}{\min_{x\in D} \left|\left\langle x\middle|\sqrt{p_{\text{true}}}\right\rangle\right|^2} \tag{20}$$

$$= \max_{x\in D} \left(\left|\sqrt{p_{\text{true}}}^{-1}\right\rangle \left\langle\sqrt{p_{\text{true}}}^{-1}\right|\right)[x,x] \, \|\Gamma'\|. \tag{21}$$

由于 $\left|\sqrt{p_{\text{true}}}^{-1}\right\rangle \left\langle\sqrt{p_{\text{true}}}^{-1}\right|$ 是半正定的，这属于定理 1 的一种情形。

□

引理 4。设 $\Gamma \in \mathbb{H}^D$ 和 $G_{\xi'}$ 是引理 1 中状态集合的格拉姆矩阵。则

$$-\left(1 - \min_{x\in D} \left|\langle x|\sqrt{p_{\text{true}}}\rangle\right|^2\right) \|\Gamma\| \leq -\|\Gamma \circ (G_{\xi'} - \left|\sqrt{p_{\text{true}}}\right\rangle \left\langle\sqrt{p_{\text{true}}}\right|)\|. \tag{22}$$

证明。设 $\Delta G := G_{\xi'} - \left|\sqrt{p_{\text{true}}}\right\rangle \left\langle\sqrt{p_{\text{true}}}\right|$。我们根据定理 1 和以下两个事实推出该命题：

1. ΔG 是半正定的。为此，请回忆 $x \in D$ 全都满足 $\langle\xi'_x|\xi\rangle = \left\langle x\middle|\sqrt{p_{\text{true}}}\right\rangle$，且 ΔG 的元素满足

$$\Delta G[x,x'] = \langle\xi'_x|\xi'_{x'}\rangle - \langle\xi'_x|\xi\rangle \langle\xi|\xi'_{x'}\rangle \tag{23}$$

$$= \langle\xi'_x| I - P_\xi \mid \xi'_{x'}\rangle \,. \tag{24}$$

因此， ΔG 是向量 $\left((I - P_\xi)\,|\xi'_x\rangle\right)_{x\in D}$ 的格拉姆矩阵，所以它是半正定的。

2. ΔG 的对角元素至多为

$$1 - \min_{x\in D} \left|\langle x|\sqrt{p_{\text{true}}}\rangle^2\right| = \max_{x\in D} \left(1 - \left|\langle x|\sqrt{p_{\text{true}}}\rangle^2\right|\right). \tag{25}$$

这是因为向量 $|\xi'_x\rangle$ 已经归一化，所以 $G_{\xi'}$ 的对角元素为 1。

□

5 状态转换的对抗界

状态转换的对抗界 [7] 给出了完成所谓状态转换任务所需查询次数的下界。我们需要的版本可由该文中的引理 4.7 得出，但请注意，它采用了略有不同的约定：它定义了一个“过滤 γ_2 范数”，其值是我们所称对抗界的两倍。另一个参考来源是 [2, 定理 10 和注释 9]。

定理 2（由 [7, 引理 4.7]推出）。对于 $0 \le i < n$，定义 $\Delta_i \in \mathbb{H}^D$ 如下$\Delta_i[x,x']$：$= 0$ 若 $x_i = x'_i$，则取该值，否则取 2。[4] 那么，任何将一个依赖于 $x \in D$的初始态集合（$|\xi_x\rangle$）$_{x\in D}$ 转换为最终态集合（$|\tau_x\rangle$）$_{x\in D}$ 的量子查询算法，至少需要

$$\mathrm{Adv}\,(G_\xi - G_\tau) := \max_{\Gamma\in\mathbb{H}^D} \frac{\|\Gamma\circ(G_\xi - G_\tau)\|}{\max_{0\le i<n}\|\Delta_i\circ\Gamma\|} \tag{26}$$

查询，其中 G_ξ、 $G_\tau \in \mathbb{H}^D$ 是表 2 中 $(|\xi_x\rangle)_{x\in D}$ 和 $(|\tau_x\rangle)_{x\in D}$ 的格拉姆矩阵。

6 将其整合起来

利用引理 1 和 2 以及状态转换的对抗界（定理 2），我们现在证明本文的核心结论。我们在下一个定理的陈述中定义函数求值的对抗界；不过请注意，它比 [5] 中使用的定义小 2 倍。

定理 3. 考虑使用标准预言机求值 f 的问题：对于所有 $x \in D$，成功概率至少为 $1/2+\delta$，条件如第 2 节所述。设 $\mathbb{F}_f \subset \mathbb{H}^D$ 是厄米矩阵构成的空间，其中当 $f(x) = f(x')$ 时，(x,x') 项为 0。令 Δ_i 如定理 2 中所述，

$$2\delta\mathrm{Adv}\,(f) := 2\delta \max_{\Gamma\in\mathbb{F}_f} \frac{\|\Gamma\|}{\max_{0\le i<n}\|\Delta_i\circ\Gamma\|} \tag{27}$$

给出了求解该问题的算法必须进行的查询次数的下界。

证明。考虑 $\Gamma \in \mathbb{F}_f$，其中

$$\max_{0\le i<n}\|\Delta_i\circ\Gamma\| \le 1, \tag{28}$$

并假设该问题可以通过 T 次查询求解。利用引理 1，找到一个进行 T 次查询的量子算法，将 $(|\xi'_x\rangle)_{x\in D}$ 转换为 $(|\tau'_x\rangle)_{x\in D}$，如该引理所述。根据定理 2，这意味着

$$\|\Gamma\circ(G_{\xi'} - G_{\tau'})\| \le T. \tag{29}$$

对于所有满足 $f(x) \ne f(x')$ 的 $x,x' \in D$，都有 $G_{\tau'}[x,x'] = 0$（引理 1 的性质 2）。此外，根据假设，对于所有满足 $f(x) = f(x')$ 的 $x,x' \in D$，都有 $\Gamma[x,x'] = 0$。这意味着 $\Gamma\circ G_{\tau'} = 0$，而方程 29 推出

$$\|\Gamma\circ G_{\xi'}\| \le T. \tag{30}$$

利用引理 2，我们得出

$$2\delta\|\Gamma\| \le \|\Gamma\circ G_{\xi'}\| \le T. \tag{31}$$

由于任何 $\Gamma \in \mathbb{F}_f$ 都可以通过对满足方程 28 的某个 $\Gamma \in \mathbb{F}_f$ 进行缩放得到，因此定理得证。 □

[4] 换言之，通过查询查询寄存器的第 i 个位置，来判断是否能够区分 x 和 x'。

7 讨论与展望

此前证明定理 3 的类似结论（使用旧的系数）的方法，实质上是对以下量进行界定：

$$\|\Gamma \circ (G_\xi - G_\tau)\|, \tag{32}$$

换言之，这指的是将算法应用于真实初始态（而非我们从引理 1 得到的修改后初始态）时所对应的状态转换对抗界。在标准推导中，这会导出旧的系数 $2\delta - \sqrt{1-4\delta^2}$；对于布尔函数，则为 $1 - \sqrt{1-4\delta^2}$ [5, 6]。据我理解（尽管我没有证明），方程 32 不满足某个界，因为它是本文的结果。

对抗界是用初始态和最终态的格拉姆矩阵来描述的，证明也可以用这些矩阵来解释（例如， [9] 中有相关讨论）。不过，与 [3, 9],的通用查询算法类似，事实证明，同时从“格拉姆矩阵图景”和“状态与酉算子图景”来思考很有成效；我们借助后者，将所考虑的格拉姆矩阵变换为更方便的形式。在我们的情形中，便利之处来自修改后的最终态具有完美可区分性，这对应于元素恰好全为 0 的格拉姆矩阵。这两种图景之间的相互作用，以及在证明中同时运用二者所带来的益处，至今仍令我困惑。

如前所述，我觉得引理 2 的证明似乎过于复杂，因此并不满意。虽然我想到了一些其他证明思路，但目前看来它们并没有更简单。我希望有人能以更优雅的方式证明引理 2，无论是否借助文献中的结果。这样或许就能从头推导出函数求值对抗界，而且比例如 [5] 中给出的方法更简洁。

在对抗界的发展历程中，一个反复出现的主题是：进展源于对输出条件的深入理解，也就是能够以非零误差确定函数值的状态集合所必须满足的条件。例如， [6] 的负权对抗方法之所以成为可能，便是得益于更精细的输出条件。本文也属于这一主题。Belovs [2] 引入了“净化器”，这是处理有限误差概率问题的另一种方法，但无法给出常数因子。值得探究的是，该常数因子与教科书中的结果相比如何，以及能否将净化器框架与这一结果结合起来。

8 致谢

感谢 Aleksandrs Belovs 就这一主题进行的有益讨论。

参考文献

[1] Andris Ambainis. 通过量子论证得到的量子下界。载于《第三十二届美国计算机协会计算理论年会论文集》，第 636–643 页，2000 年。[2] Aleksandrs Belovs. 量子对抗方法的变体。arXiv 预印本 arXiv:1504.06943，2015 年。[3] Aleksandrs Belovs 和 Duyal Yolcu. 拉斯维加斯单程票与量子对抗方法。arXiv 预印本 arXiv:2301.02003，2023 年。[4] Rajendra Bhatia. 正定矩阵。载于《正定矩阵》。普林斯顿大学出版社，2009 年。[5] Andrew M. Childs. 量子算法讲义。[6] Peter Hoyer、Troy Lee 和 Robert Spalek. 负权重使对抗方法更强。载于《第三十九届美国计算机协会计算理论年会论文集》（STOC '07），第 526–535 页，美国纽约州纽约市，2007 年。美国计算机协会。[7]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《2011 年电气电子工程师学会第 52 届计算机科学基础年会论文集》，第 344–353 页。电气电子工程师学会，2011 年。[8] Michael A Nielsen 和 Isaac Chuang. 量子计算与量子信息，2002 年。[9] Duyal Yolcu. 重新审视对抗界：从最优查询算法到最优控制。arXiv 预印本 arXiv:2211.16293，2022 年。