arXiv:2301.03763v1 [quant-ph] 10 Jan 2023

通过改进的动态吉布斯采样加速求解零和博弈

Adam Bouland、Yosheb Getachew、Yujia Jin、Aaron Sidford、Kevin Tian*
{abouland,yoshebg,yujiajin,sidford}@stanford.edu, tiankevin@microsoft.com

摘要

我们提出了一种量子算法，用于计算零和博弈的 ϵ-近似纳什均衡，其中收益矩阵为 $m \times n$，且矩阵元素有界。给定用于访问收益矩阵的标准量子预言机，我们的算法运行时间为 $\widetilde{O}(\sqrt{m+n} \cdot \epsilon^{-2.5} + \epsilon^{-3})$，并输出该 ϵ-近似纳什均衡的经典表示。这一结果优于此前由 $\widetilde{O}(\sqrt{m+n} \cdot \epsilon^{-3})$ 得到的最佳量子运行时间（作者为 [vAG19] ），也优于 $\widetilde{O}((m+n) \cdot \epsilon^{-2})$ 这一由 [GK95] 提出的经典运行时间，适用于 $\epsilon = \Omega((m+n)^{-1})$。我们通过设计新的量子数据结构，实现了从缓慢变化的吉布斯分布中高效采样，从而得到这一结果。

*部分工作是在斯坦福大学期间完成的。

1 引言

如今，机器学习和快速数值线性代数领域已涌现出一大类量子算法 [BWP+17]，这些算法建立在许多量子算法原语之上，例如 [BHMT02、HHL09、GSLW19]。更具体地说，研究已表明，对于范围广泛的问题，量子算法在某些参数条件下可以实现更快的运行时间。[1] 这些量子算法的运行时间在维度依赖性方面优于经典算法，但往往以对误差容限的依赖性更差和／或只能隐式访问解为代价（例如，只能通过查询或采样访问解的各个条目）。因此，本文旨在探讨以下问题。

> 量子优化算法在精度与维度依赖之间是否存在内在权衡？这种权衡可以通过哪些算法技术加以改善？

本文针对零和博弈中计算ϵ-近似纳什均衡这一基本优化问题，探讨上述问题。我们的主要结果是改善了求解零和博弈的量子算法对 ϵ 的依赖，使其非常接近相应经典算法的依赖。此外，我们还证明，对于我们的算法，以经典表示形式获得解无需额外的渐近成本。我们的工作建立在 [vAG19、LCW19],的基础上。该工作通过设计量子数据结构，高效实现求解零和博弈的算法，已经在回答上述问题方面迈出了重要的一步。

值得注意的是，为了获得我们的结果，我们改进了量子算法，用于解决一个动态数据结构问题：从缓慢变化的吉布斯分布中采样。这类动态采样问题自然出现在求解零和博弈的随机梯度方法中。我们通过改进 [vAG19]提出的吉布斯采样子程序，实现了加速。我们设计了一种新的动态量子数据结构，可在 $\widetilde{O}(\epsilon^{-\frac{1}{2}})$时间内完成所需的吉布斯采样，比 $\widetilde{O}(\epsilon^{-1})$ 快；后者是 [vAG19]实现的运行时间。除了解决这一问题本身的效用之外，我们希望改进后的吉布斯采样器能展现出这样的潜在算法见解：通过寻求改善量子优化算法的误差依赖关系，可以获得新的认识。此外，我们希望这项工作能推动对高效优化量子数据结构的研究与设计。

1.1 零和博弈

对于矩阵 $\mathbf{A} \in \mathbb{R}^{m\times n}$，其对应的零和博弈 等价于以下一对优化问题

$$\min_{u\in\Delta^m}\max_{v\in\Delta^n} u^\top \mathbf{A} v = \max_{v\in\Delta^n}\min_{u\in\Delta^m} u^\top \mathbf{A} v, \text{ where } \Delta^k := \{x \in \mathbb{R}^k_{\geq 0} : \textstyle\sum_{i\in[k]} x_i = 1\}.$$

在此类博弈中，我们将 $\mathbf{A}$ 称为收益矩阵，并将 m 维和 n 维单纯形（即 Δ^m 和 Δ^n）视为分别对应于 $[m]$ 和 $[n]$ 上分布的空间。从这一视角来看，$u^\top \mathbf{A} v$（称为 (u, v) 的收益 或效用 ）是从对应于 u 和 v 的分布中独立抽取 $i \in [m]$ 和 $j \in [n]$ 时，$\mathbf{A}_{ij}$ 的期望值。因此，零和博弈描述的是一种双人博弈，其中最小化玩家力求将收益降至最低，同时最大化玩家力求将其最大化。

本文研究零和博弈中计算近似纳什均衡的经典问题。给定收益矩阵 $\mathbf{A} \in \mathbb{R}^{m\times n}$，我们称一对 $(u, v) \in \Delta^m \times \Delta^n$ 为 ϵ- 近似纳什均衡（*NE*），当且仅当 $\epsilon \in \mathbb{R}_{>0}$

$$\left(\max_{v'\in\Delta^n} u^\top \mathbf{A} v'\right) - \left(\min_{u'\in\Delta^m} (u')^\top \mathbf{A} v\right) \leq \epsilon.$$

[1]请注意，由于输入/输出开销、不同的访问模型 [Aar15], 以及经典去量子化算法 [Tan19、CGL+20、GLG22],

我们假设收益矩阵 A 和误差容忍度作为算法的输入，并且为简便起见，$\|A\|_{\max} \le 1$，即 A 的最大元素的绝对值至多为 1（不失一般性，因为可以通过缩放 $A \leftarrow \|A\|^{-1}_{\max} A$ 和 $\epsilon \leftarrow \|A\|^{-1}_{\max} \epsilon$）。本文的主要目标是设计改进的零和博弈求解器，即能够计算 ϵ-近似纳什均衡的算法。

零和博弈是理论计算机科学、优化和经济学的基础。近似求解零和博弈这一问题，是近似线性规划（LP）的一种自然表述，因此也是检验新优化技术的重要试验平台。过去几十年来，在对问题参数作出各种假设的条件下，求解零和博弈的计算复杂度取得了诸多进展（综述见第1.3节）。线性规划内点法（IPM）的最新进展，例如[vdBLL+21] 及其中的参考文献（第1.3节将对此作更详细的讨论），可在 $\widetilde{O}(mn + \min(m,n)^{2.5})$时间内求解零和博弈。[2] 此外，[vdB20], 的线性规划算法表明，零和博弈可以在 $O((m+n)^{\omega})$时间内确定性地求解，其中 $\omega < 2.373$ 是当前的矩阵乘法常数 [AW21],；若不使用快速矩阵乘法，则可在 $\widetilde{O}((m+n)^3)$时间内求解。本文主要关注用于近似求解纳什均衡的次线性时间算法。

由[GK95] 提出的著名算法，其运行时间为 $O((m+n)\epsilon^{-2})$，在不对问题作出任何假设的情况下，经典算法中具有最先进水平的次线性运行时间。近期研究表明，量子算法能够显著提升求解零和博弈及其推广问题的运行效率 [LCW19、vAG19、LWCW21]。具体而言，在 2019Li、Chakrabati 和 Wu [LCW19] 提出了一个用于求解零和博弈的量子算法，运行时间为 $O(\sqrt{m+n}\epsilon^{-4})$；与此同时，van Apeldoorn 和 Gilyen [vAG19] 提出了一个运行时间为$\widetilde{O}(\sqrt{m+n}\cdot\epsilon^{-3})$的算法。这些算法在维度依赖性方面，相较于最佳经典算法实现了二次改进，但误差依赖性更高。

[LCW19、vAG19、LWCW21] 均使用针对A的标准量子预言机（形式化定义见第2节），通过该预言机可以在叠加态中查询A 的各个条目。本文余下部分将重点讨论 [vAG19] 的算法，因为我们着重于改善误差依赖性。[vAG19] 算法推广了 Grigoriadis 和 Khachiyan 的经典算法 [GK95], ，并通过加速 [GK95] 方法所需的关键动态吉布斯采样子程序，缩短了运行时间。正如我们将在第3节详细讨论的那样，van Apeldoorn 和 Gilyen 提出了一种量子数据结构，能够以在维度方面快二次的速度高效完成这种采样，这是其算法加速的核心。

我们的结果。我们提出了一种求解零和博弈的新量子算法，其运行时间优于由[vAG19]提出的先前最先进的量子算法。

定理 1（非正式表述，详见定理 4）。设 $A \in \mathbb{R}^{m\times n}$ 满足 $\|A\|_{\max} \le 1$，且 $\epsilon \in (0, 1)$。给定关于 A 的量子预言机（定义见第 2 节），存在一个 $\widetilde{O}(\sqrt{m+n}\cdot\epsilon^{-2.5} + \epsilon^{-3})$ 时间算法，可产生经典输出 $(u, v) \in \Delta^m \times \Delta^n$，且以高概率为一个 ϵ-近似纳什均衡。

我们的新算法同时改进了已知最佳的量子 [vAG19] 算法和经典[GK95] 算法，适用于内点法不优于次线性算法的参数范围。具体而言，当 $\epsilon^{-1} = \widetilde{O}(m+n)$时，其运行时间快于经典算法 [GK95] 的 $\widetilde{O}((m+n)\cdot\epsilon^{-2})$运行时间；这包括[GK95] 优于 $O((m+n)^{\omega})$运行时间的[vdB20] 内点法的参数范围，具体如 $\omega < 3$所示。相比之下，先前量子算法 [vAG19], 的运行时间在次线性算法

[2]我们使用 $\widetilde{O}$ 记号，在行文方便时隐去问题参数的多对数依赖；更详细的隐藏参数说明见第 2 节。非正式定理表述中的“以高概率”表示对失败概率存在多对数依赖。

目前比内点法更可取。例如，当 $m \approx n$ 且（忽略对数因子）$\epsilon \in [n^{-c}, n^{-\frac{1}{2}}]$ 其中 $c = \frac{1}{2}(\omega - 1)$时，[GK95] 优于 [vAG19] 以及最先进的内点法 [vdB20、CLS21]。[3]

1.2 动态吉布斯采样

我们通过构造一种更快的新型量子数据结构来执行[vAG19], 算法中使用的吉布斯采样，从而改进了零和博弈求解器对误差的依赖性。这种数据结构本身也可能具有独立的研究价值。吉布斯采样是一种基础算法原语——其基本任务是给定向量 $v \in \mathbb{R}^n$，从与$\exp(v)$成正比的概率分布中采样。吉布斯采样被用作许多量子和经典优化算法中的子程序，例如 [BS17]及其后续研究。一般而言，量子算法可以利用振幅估计更高效地完成这一任务，因为振幅估计能够提高拒绝采样方案的接受概率。这一策略由 [vAG19], 实现：该方法利用量子最大值查找 $v_{\max}$ 来近似 v的最大元素[DH 96], 均匀采样 $i \in [n]$，并以$\exp(v_i - v_{\max}) \leq 1$ 为接受概率，使用量子拒绝采样接受该样本。我们将在第 [vAG19] 节中更详细地介绍吉布斯采样器及其复杂性分析。3.2。

我们给出一种数据结构，可将 [vAG19] 吉布斯采样子程序的运行时间对误差的依赖性改善一个二次方，从 $\widetilde{O}(\sqrt{m+n} \cdot \epsilon^{-1})$ 每个样本降低到摊销 $\widetilde{O}(\sqrt{m+n}\,\epsilon^{-\frac{1}{2}})$ 每个样本。实现这一改进的关键在于：在[GK95] 的零和博弈求解器中，所采样的吉布斯分布会随时间缓慢变化：基向量 v在每次迭代中只接收有界稀疏更新。通过存储关于吉布斯分布的部分信息，也就是一个可高效计算的、对其各项的上界估计，并且该估计在连续多次迭代中始终有效，我们得到了一个改进的动态吉布斯采样器。我们还在第3.2节中对其作了详细概述。

现在，我们定义近似吉布斯采样器的概念，然后陈述我们所考虑的动态采样问题。该问题自然出现在运行时间为次线性的零和博弈算法中。

定义 1 (近似吉布斯预言机)。 对于 $v \in \mathbb{R}^n$，其对应的吉布斯分布为 $p_v \in \Delta^n$，满足对所有 $i \in [n]$，$[p_v]_i \propto \exp(v_i)$。我们称 $\mathcal{O}_v^{\text{gibbs}}$为一个 δ-近似吉布斯预言机，若它以 $\|\tilde{p} - p_v\|_1 \leq \delta$的概率从 $\tilde{p} \in \Delta^n$ 中采样。

问题 1 (采样维护)。 设 $\eta > 0, \delta \in (0,\ 1)$，并假设我们有一个用于 $\mathbf{A} \in \mathbb{R}^{m \times n}$ 的量子预言机。考虑对动态向量 $x \in \mathbb{R}^m_{\geq 0}$ 执行一系列 T 更新 操作，每次操作的形式为 $x_i \leftarrow x_i + \eta$，其中 $i \in [m]$ 满足某个条件。在采样维护问题中，我们必须以每次更新 摊销$\mathcal{T}_{\text{update}}$ 时间维护一个针对 $\mathbf{A}^\top x$ 的 δ-近似吉布斯预言机 $\mathcal{O}_{\text{samp}}$，该预言机在最坏情况下可于 $\mathcal{T}_{\text{samp}}$ 时间内查询。

我们的结果。 我们提出了一种量子算法来求解问题 1，其运行时间优于 [vAG19] 的算法中相应部分所隐含的运行时间。

定理 2 (非正式表述，参见定理 3)。 存在一种量子算法，能够以高概率求解问题 *1*，其运行时间为 $\max(\mathcal{T}_{\text{samp}},\ \mathcal{T}_{\text{update}}) = \widetilde{O}\left(\sqrt{n} \cdot T\eta^{1.5}\right)$，且初始化成本为 $\widetilde{O}\left(\eta^3 T^3\right)$。

定理 2 改进了由 [vAG19] 所隐含的采样维护问题 1 的解，使其提升了 $\eta^{-\frac{1}{2}}$ 倍；在 [GK95] 求解器的设定下，其中 $T = \widetilde{O}(\epsilon^{-2})$ 且 $\eta = \Theta(\epsilon)$，这带来了 $\epsilon^{-\frac{1}{2}}$ 倍的改进。概括而言，我们的改进通过存储一个提示实现，该提示由一个高估真实吉布斯分布的向量和一个近似

[3]有证据表明，$\omega = 2$ 使用当前技术无法实现，例如 [Alm21]。

表 1： **用于计算零和博弈的 ϵ 近似纳什均衡的算法**。隐藏多对数因子，并假设 $\mathbf{A} \in \mathbb{R}^{m\times n}$ 满足 $\|\mathbf{A}\|_{\max} \leq 1$。

方法	查询模型	总运行时间
内点法 [CLS21]	经典	$\max(m,n)^{\omega}$
内点法 [vdBLL+21]	经典	$mn + \min(m,n)^{2.5}$
外梯度法 [Nem04,Nes07]	经典	$mn \cdot \epsilon^{-1}$
随机镜像下降（SMD）[GK95]	经典	$(m+n) \cdot \epsilon^{-2}$
方差缩减随机镜像下降[CJST19]	经典	$mn + \sqrt{mn(m+n)} \cdot \epsilon^{-1}$
[vAG19]	量子	$\sqrt{m+n} \cdot \epsilon^{-3}$
定理1 (**我们的工作**)	量子	$\sqrt{m+n} \cdot \epsilon^{-2.5} + \epsilon^{-3}$

Tab表 2： **问题 1的解**, $T = \epsilon^{-2}$, $\eta = \epsilon$。 隐藏多对数因子 .

方法	查询模型	$\mathcal{T}_{\text{samp}}$	$\mathcal{T}_{\text{update}}$
显式更新 [GK95]	经典	1	$m+n$
基于最大值的拒绝采样 [vAG19]	量子	$\sqrt{m+n} \cdot \epsilon^{-1}$	$\sqrt{m+n} \cdot \epsilon^{-1}$
定理 2(**我们的工作**)	量子	$\sqrt{m+n} \cdot \epsilon^{-\frac{1}{2}}$	$\sqrt{m+n} \cdot \epsilon^{-\frac{1}{2}}$

归一化因子组成，且二者都很少更新。我们维护的提示满足以下理想性质：(i) 它在一批连续迭代中保持有效，以及 (ii) 高估程度有界。前一性质确保较快的摊销更新时间，后一性质则通过为我们的量子拒绝采样器提供接受概率下界，确保较快的采样时间。我们维护改进提示的总体策略是，反复调用采样访问来准确估计吉布斯分布中的较大项，并利用分布在问题 1的设定下的稳定性。我们将在第 1 节更详细地讨论动态吉布斯采样器，并将其与以往解决问题 3.2的方法进行比较。

定理 2 的初始化成本源于当前量子奇异值变换（SVT）框架 [GSLW19]在数值稳定实现方面的最新进展。这一成本也是定理 $\widetilde{O}(\epsilon^{-3})$ 中加性项的原因。我们在附录 D中讨论了这一成本；对 [GSLW19]数值稳定实现的改进，将体现在定理 1 和 2的运行时间中。

1.3 相关工作

量子优化与机器学习。 量子优化和机器学习领域存在大量量子算法，它们利用了振幅放大等基本算法基元 [BHMT02], 、HHL 算法 [HHL09], 以及量子奇异值变换 [GSLW19]。例如，已有多项工作针对各种机器学习任务提出了基于 HHL 的算法，例如主成分分析 [LMR14], 、支持向量机 [RML14], 和推荐系统[KP16]。更多详情请参阅 [BWP+17]的综述文章。

与我们当前工作最相关的是用于优化问题的量子算法。例如，Brandao 和 Svore [BS17] 提出了一种基于 Arora-

Kale 算法 [AK07], , 后来由 [VAGGdW20b]进行了改进。此外，也有用于线性规划和半定规划的基于量子内点法的方法 [KP20]。另外，一系列研究探讨了用于一般凸优化的量子算法 [CCLW20、vAGGdW20a], , 这些算法利用 Jordan 算法快速进行梯度估计 [Jor05、GAW19]。

在零和博弈领域，除了前文提到的工作 [vAG19之外，LCW19]还研究了 ℓ_1-ℓ_1 博弈（其中双方玩家都受到 ℓ_1约束）。此外，还有一些工作考虑了零和博弈的不同变体。例如，Li、Chakrabati 和 Wu [LCW19] 提出了用于 ℓ_2-ℓ_1 博弈的量子算法，使维度方面的复杂度提升了二次。随后，Li、Wang、Chakrabati 和 Wu [LWCW21] 将该算法扩展到更一般的 ℓ_q-ℓ_1 博弈，并获得了 $q \in (1, 2]$。

零和博弈。零和博弈是优化、经济学和机器学习中的经典建模工具[Neu28]。经典的外梯度法（镜像近端法） [Nem04，Nes07] 可在 ϵ时间内计算出一个 $\widetilde{O}(mn \cdot \epsilon^{-1})$精度的近似纳什均衡；如前所述， [GK95] 的随机镜像下降法可在 $\widetilde{O}((m+n) \cdot \epsilon^{-2})$时间内达到相同精度。最近， [CJST19] 利用方差缩减获得了介于两者之间的运行时间，详见表1。

针对矩阵 $\mathbf{A}$ 的更精细刻画（例如稀疏性，即每行或每列非零元素的数量；或数值稀疏性，即行和列的 ℓ_1-至-ℓ_2 范数比有界）可带来更快的运行时间 [CJST20]。值得注意的是， [GK95] 算法在稀疏性假设下也能缩短运行时间，[vAG19] 的算法在某些稀疏性与精度比值范围内也有此效果。本文关注一般情形下的纳什均衡算法（不作进一步的稀疏性或数值稀疏性假设）。

与此同时，针对求解线性规划的内点法的一系列改进研究 [Kar84, Ren88, LS14, LS19, vdBLSS20, JSWZ21]催生了多种零和博弈求解器，其运行时间对问题精度的依赖为对数多项式级 ϵ。目前最先进的内点法变体包括 [CLS21] 和 [vdBLL+21]，其运行时间分别为 $O(\max(m,n)^\omega)$ 和 $\widetilde{O}(mn + \min(m,n)^{2.5})$。详细比较请参见表 1。最后，对于强多项式运行时间（即不依赖于 ϵ）的算法——这超出本文讨论范围——请参见 [DNV20] 及其中引用的文献。

1.4 未来工作

定理 1的 ϵ依赖关系与经典对应方法相比，差距在 $\epsilon^{-\frac{1}{2}}$倍以内。据我们所知，消除这一 $\epsilon^{-\frac{1}{2}}$开销将意味着，首次出现一种针对自然优化问题的量子算法，能够在所有参数范围内优于经典对应方法。

我们的工作和 [vAG19] 都通过利用 GSLW中提出的一种强大的、基于多项式近似的技术来解决问题 [GSLW19], , 该技术称为量子奇异值变换（ QSVT ）。在这两种情况下，QSVT 都与一个次数为 $\widetilde{O}(\epsilon^{-1})$ 的多项式结合使用。值得注意的是，在密切相关的经典情形中（见 [SV14]），基于切比雪夫多项式的逼近可以使次数降低为原来的二次方根。然而，由于量子门的谱带来的有界性要求，无法将这些构造直接应用于 QSVT。绕过这一障碍是改进我们工作的一个自然方向，我们将其留作一个开放问题。

更一般地，确定动态吉布斯采样（例如，问题 1）的最优预言机查询复杂性以及求解零和博弈，是我们的工作留下的关键开放问题。这些问题可能比确定紧确的时间复杂度刻画更容易处理。例如，在定理 ~1 的背景下，能否将 $\max(\mathcal{T}_{\text{samp}}, \mathcal{T}_{\text{update}})$ 改进为 $O(\sqrt{n})$ ，或者我们能否在查询模型中排除这种改进?

1.5 组织结构

在第 2 节中，我们介绍全文使用的记号，以及所假设的（经典和量子）计算模型。在第 3 节中，我们简要概述用于证明定理 1 的算法的核心组成部分：我们的方法所基于的随机梯度法，以及利用一种新型动态吉布斯采样器对关键子程序进行的高效量子实现。最后，在第 4 节中，我们给出新的量子采样器，并证明定理 2。

我们旨在第 3 节中对我们的算法作出自包含但简化的描述，以提升论文的可读性，使具有优化背景但不熟悉量子计算的读者，以及熟悉量子计算但不熟悉优化的读者，都能更轻松地阅读。具体而言，我们将先前工作中开发的核心优化机制（随机镜像下降）和量子机制（量子奇异值变换）抽象为命题 1 和 2的陈述，并重点说明如何将这些陈述作为黑盒来构建更快的算法。这些陈述的证明见附录 A 和 B。

2 预备知识

~通用记号。O 隐藏了问题维度（记为 m和 n）、目标精度（记为 ϵ）以及失败概率（记为 α）中的对数因子。在讨论问题 ~lem 1 的运行时间时，我们还使用 O 来隐藏参数 η, T中的对数因子。对于所有 $i \in [n]$，我们令$e_i \in \mathbb{R}^n$ 表示 $i \in [n]$ 对应的 i^{th} 标准基向量（当 n 明确时）。 $\|\cdot\|_p$ 表示向量的 ℓ_p 范数。对于 $\mathbf{A} \in \mathbb{R}^{m\times n}$，其 i^{th} 行和 j^{th} 列分别为 $\mathbf{A}_{i:}$、$\mathbf{A}_{:j}$。对于 $v \in \mathbb{R}^n$，$\mathbf{diag}\,(v)$ 是以 v 为对角元素的对角 $n \times n$ 矩阵。$\mathbf{A}$ 的共轭转置记为 $\mathbf{A}^*$；当矩阵为实数矩阵时，记为 $\mathbf{A}^\top$。维度为 n 的全1向量和全0向量分别为 $\mathbf{1}_n$ 和$\mathbf{0}_n$。最后，全文中：$= \lceil \log_2 m \rceil$，且$= \lceil \log_2 n \rceil$，因此 $[m] \subseteq [2^a]$ 和 $[n] \subseteq [2^b]$。

计算模型。 我们假设 $\mathbf{A}$ 的各个元素是 w 位实数，且 $w = O(\log(mn))$，并在字RAM模型下工作，其中 w 位算术运算耗时 $O(1)$；为简单起见，我们假设三角函数和根式等数学运算也可以针对 w 位字在 $O(1)$ 时间内精确实现。下文中，“量子态”均指单位向量，“量子门”或“预言机” $\mathcal{O}$ 均指酉矩阵。我们采用标准记号，并将标准基向量 e_i 表示为 $i \in [n]$的 $|i\rangle$，即一个 a量子比特态，其中 i 以二进制表示（即更严格地说，$|i\rangle = |\mathbf{bin}(i)\rangle$，为简洁起见省略 bin）。我们考虑预言机的标准量子访问模型，其中预言机 $\mathcal{O}$由其对所有 $\{0,1\}^*$ 值的 s （长度由上下文明确）在 $|s\rangle$ 上的运算定义，并且可以在叠加态中查询。如果 $\mathcal{O}$ 在$|v\rangle := \sum_s \alpha_s |s\rangle$上被查询，结果为 $\mathcal{O}|v\rangle = \sum_s \alpha_i (\mathcal{O}|s\rangle)$。我们使用 $|g\rangle$、$|g'\rangle$等（当上下文明确时）表示任意的子单位向量，它们代表垃圾态（计算中未使用的状态）。在 a和 b 个量子比特上的状态 $|u\rangle$ 与 $|v\rangle$ 的张量积记为 $|u\rangle|v\rangle$，是一个 $(a+b)$量子比特态。量子电路的运行时间是其最大深度（以 w 位字上的算术门计）。

访问模型。 在全文中，我们假设通过标准量子预言机访问 $\mathbf{A}$（回忆一下 $\|\mathbf{A}\|_{\max} \le 1$）。具体而言，我们所说的 $\mathbf{A}$ 的量子预言机，是指这样一个预言机：当以 $|i\rangle|j\rangle|s\rangle$ for $i \in [m], j \in [n], s \in \{0,1\}^w$ 查询时，它会在 O 时间内将 $\mathbf{A}_{ij}$（以二进制表示）可逆地写入第三个寄存器，即 $\mathcal{O}_{\mathbf{A}}|i\rangle|j\rangle|s\rangle = |i\rangle|j\rangle|s \oplus \mathbf{A}_{ij}\rangle$，其中 $\oplus$ 是按位模 2 加法。

给定一个用于 $\mathbf{A}$ 的量子预言机，只需查询两次，利用标准构造即可构造出一个预言机，将该值置于状态的振幅中，而非寄存器本身。更多

更形式化地，可以构造[4] 一个 $\mathcal{O}'_{\mathbf{A}}$，其运作方式如下：

$$\mathcal{O}'_{\mathbf{A}}|0\rangle|i\rangle|j\rangle = \sqrt{\mathbf{A}_{ij}}|0\rangle|i\rangle|j\rangle + \sqrt{1-|\mathbf{A}_{ij}|}|1\rangle|g\rangle, \text{ for } (i,j) \in [m]\times[n].$$

文献中通常会（使用辅助量子比特存储输出寄存器，其中$\mathbf{A}^{ij}$ 被写入）构造这样的 $\mathcal{O}'_{\mathbf{A}}$，使其 $\mathcal{O}_{\mathbf{A}}$ 符合我们的经典计算模型，参见例如[GR02]。为简单起见，本文余下部分不再讨论辅助量子比特，并假设可以直接访问$\mathcal{O}'_{\mathbf{A}}$。我们还注意到，$\mathcal{O}'_{\mathbf{A}}$ 的实现存在歧义，因为平方根并不唯一，而且我们可以控制该实现中采用的符号。本文稍后将充分利用这一灵活性，具体见推论6。

3 方法概述

本节概述我们为证明主要结果所采用的方法：用于求解零和博弈的改进量子运行时间（定理4），以及用于动态吉布斯采样的改进量子数据结构（定理3）。本节安排如下。

在第3.1节中，我们给出算法1，即用于求解零和博弈的优化方法框架。该框架是 [GK95]所提出经典算法的推广。我们在命题1中陈述其保证，并将证明推迟到附录A。算法1 假设可以访问一个近似吉布斯预言机（定义1），用于从问题1所述的动态分布中采样。我们的主要工作是获得此类预言机的高效量子实现（定理3），并利用这一结果在第3.1节末证明定理4 。

在第 3.2 节中，我们概述本文的主要技术创新，即对问题 1 的改进解法。先前工作 [vAG19] 以每次迭代的摊销 $\approx \sqrt{m+n}\cdot\epsilon^{-1}$ 成本求解问题 1，而我们展示了如何以每次迭代的摊销 $\approx \sqrt{m+n}\cdot\epsilon^{-\frac{1}{2}}$ 成本求解该问题。需要指出的是，我们算法中唯一的量子组件（量子奇异值变换和振幅放大）已由命题 2 抽象处理，该命题在附录 B 中得到证明。

3.1 使用吉布斯采样预言机求解矩阵博弈

定理的证明4 使用了算法1中所述算法框架的高效实现，该框架基于随机镜像下降。在阐述算法1时，我们回顾此前的定义1，它描述了算法1执行所需的近似采样访问。

算法 1： MatrixGameSolver(δ, η, T)

输入： $\mathrm{A} \in \mathbb{R}^{m\times n}$，期望精度 $\epsilon \in (0,1)$，用于以下对象的 δ-近似吉布斯预言机（动态）向量 $-\mathrm{A}^\top x_t$ 和 $\mathrm{A}y_t$

参数： 吉布斯采样器参数 $\delta \in (0,1)$，步长 $\eta > 0$，迭代次数 T

初始化 $\hat{u} \leftarrow \mathbf{0}_m$、$\hat{v} \leftarrow \mathbf{0}_n$、$x_0 \leftarrow \mathbf{0}_m$ 和 $y_0 \leftarrow \mathbf{0}_n$

对于 $t = 0$ **到** $T-1$，**执行**

  使用 $\mathcal{O}^{\text{gibbs}}_{-}$ 独立地抽取 j_t、$j'_t \in [n]$ 样本$_{\mathbf{A}^\top x_t}$ 并使用 $\mathcal{O}^{\text{gibbs}}{}_{\mathbf{A}y_t}$ 抽取 i_t、$i'_t \in [m]$ 样本

  更新 $y_{t+1} \leftarrow y_t + \eta e_{j_t}$ 和 $x_{t+1} \leftarrow x_t + \eta e_{i_t}$ // 更新迭代。

  更新 $\hat{u} \leftarrow \hat{u} + \frac{1}{T}e_{i'_t}$ 和 $\hat{v} \leftarrow \hat{v} + \frac{1}{T}e_{j'_t}$ // 更新输出。

返回 $(\hat{u}, \hat{v})$

[4]例如，可以调用预言机获取 $\mathbf{A}^{ij}$ 的值（二进制表示，视为介于 0 和 1之间的有符号数），添加一个辅助量子比特，执行算术运算以计算该辅助量子比特所需的旋转角度，再使用该二进制表示的旋转角度，对辅助量子比特应用一系列受控旋转门，然后再次调用标准预言机，以反计算出 $\mathbf{A}^{ij}$的二进制值。详情请参见 [GR02] 。

算法1 （第 5–6 行）使用精确预言机时的主要框架与以下方法相同：[GK95]。不过，我们的框架在 [GK95] 的基础上，在以下三个方面进行了拓展。

1. 我们通过 δ-近似吉布斯预言机，在采样过程中容忍全变差误差。
2. 我们利用鞅论证，对对偶间隙给出高概率保证。
3. 我们对输出进行子采样，得到一个具有相当对偶间隙的稀疏解。

我们指出，其中一些改进此前已在随机梯度方法文献中明确或隐含地出现过。例如， [CJST20], 给出了一种容忍近似的随机梯度方法，而我们关于高概率保证的证明则基于[AL17和CDST19]中的论证。为完整起见，我们在附录1中给出算法A的以下保证的自包含证明。

命题1。设$\mathbf{A} \in \mathbb{R}^{m\times n}$满足 $\|\mathbf{A}\|_{\max} \leq 1$和 ϵ， $\alpha \in (0,\ 1)$。设 $\delta \leq \frac{\epsilon}{20}$， $\eta = \frac{\epsilon}{60}$，并且$T = \Theta(\epsilon^{-2}$对数$\frac{mn}{\alpha})$取适当的常数。以概率 $\geq 1-\alpha$，算法*1*输出一个ϵ-近似纳什均衡，对应于$\mathbf{A}$。

根据命题 1 ，要获得更快的零和博弈求解器，我们只需高效实现第 5 行中的吉布斯采样。正如第 1 节所述，问题 1 描述了一个足以完成此任务的动态近似吉布斯预言机采样问题。事实上，对问题 1 采用两种恰当的参数化形式求解，即可得到算法 1 所需的预言机。结合命题 1 与以下定理 3 （这是我们对问题 1 的解，将在第 3.2 节中详细讨论），我们证明主要结果——定理 4。

定理 3。 设 $\alpha \in (0,\ 1)$ 且 $\delta \leq \eta$。给定 $\mathbf{A} \in \mathbb{R}^{m\times n}$ （定义见第 *2* 节）的量子预言机，且 $\|\mathbf{A}\|_{\max} \leq 1$，我们可以以概率 $\geq 1-\alpha$ 求解问题 *1* 其中

$$\max(\mathcal{T}_{\text{samp}}, \mathcal{T}_{\text{update}}) = O\left(1 + \sqrt{n}\cdot T\eta \log^4\left(\frac{mn}{\delta}\right)\cdot\left(\sqrt{\eta\log\left(\frac{n\eta T}{\alpha}\right)} + \eta\log\left(\frac{n\eta T}{\alpha}\right)\right)\right),$$

并且初始化成本为

$$O\left(\eta^3 T^3 \log^4\left(\frac{n\eta T}{\delta}\right) + \log^7\left(\frac{n\eta T}{\delta}\right)\right).$$

定理 4。 设 $\mathbf{A} \in \mathbb{R}^{m\times n}$ 满足 $\|\mathbf{A}\|_{\max} \leq 1$，且 ϵ， $\alpha \in (0,\ 1)$。给定 $\mathbf{A}$（定义见第 *2* 节）的量子预言机，存在一种量子算法，能够以概率 $\geq 1-\alpha$ 在

$$O\left(\frac{\sqrt{m+n}}{\epsilon^{2.5}}\log^4\left(\frac{mn}{\epsilon}\right)\log^{2.5}\left(\frac{mn}{\alpha\epsilon}\right) + \frac{\sqrt{m+n}}{\epsilon^2}\log^4\left(\frac{mn}{\epsilon}\right)\log^3\left(\frac{mn}{\alpha\epsilon}\right) + \frac{1}{\epsilon^3}\log^7\left(\frac{mn}{\epsilon}\right)\right).$$

证明。 我们应用定理 3 的两个实例，以实现动态向量 δ 的近似吉布斯预言机，用于动态向量 $-\mathbf{A}^\top x_t$ 和 $\mathbf{A}y_t$，从而以摊销 1时间完成算法 $O(1+\mathcal{T}_{\text{samp}}+\mathcal{T}_{\text{update}})$ 的每次迭代。采用命题 T, η 中的参数设置 1 并令$\delta = \Theta(\epsilon)$，这足以满足算法 1 和定理 3，我们得到

$$\max(\mathcal{T}_{\text{samp}}, \mathcal{T}_{\text{update}}) = O\left(\frac{\sqrt{m+n}}{\epsilon}\log^4\left(\frac{mn}{\epsilon}\right)\log\left(\frac{mn}{\alpha\epsilon}\right)\left(\epsilon\log\left(\frac{mn}{\alpha\epsilon}\right) + \sqrt{\epsilon\log\left(\frac{mn}{\alpha\epsilon}\right)}\right)\right).$$

由观察可知，算法 1 的开销为 $O(T\cdot(1+\mathcal{T}_{\text{samp}}+\mathcal{T}_{\text{update}}))$，因此结论成立。正如引言中所述，运行时间中的加性项来自稳定实现一个量子电路的开销；在应用定理 3 来表示有限精度下的多项式变换时，需要用到该电路。我们将在附录 D 中更详细地讨论这一点。 □

3.2 通过动态提示维护实现动态采样维护

I本节概述定理 3 的证明，该证明分两步进行 s.

1. 我们将采样维护（问题 1）归约为一个我们称为提示维护的问题。后者是采样维护问题的一种特化形式，其中提供了适当的辅助信息，我们在下文中称之为提示。2. 我们在定理 3 中通过递归调用命题 2，并分阶段进行，从而维持适当质量的提示，以此展示如何解决命题 2 所需的提示维护问题。

将采样维护归约为提示维护。首先，我们介绍以下数据结构，用于维护问题 x 1中的变量；该结构在 [vAG19] 中对动态吉布斯采样起到了关键作用。这个数据结构支持对 x 坐标子集的高效查询，我们也在自己的吉布斯采样器中使用它。

引理 1 (采样器树)。设 $\eta \in \mathbb{R}_{\geq 0}$ 和 $m \in \mathbb{N}$。存在一种经典数据结构，SamplerTree，支持在 $O(m)$ 个节点上构建一棵树，其中 $[m]$ 对应于叶节点，并支持以下操作。

- 初始化$(m, \eta_{\text{固定}})$：初始化 $x \leftarrow \mathbf{0}_m$ 和 $\eta \leftarrow \eta_{\text{固定}}$
- 更新(i)：$x_i \leftarrow x_i + \eta$
- 子树和(v)：返回所有 x_i 的和，其中 i 位于 v 的子树中

T 次更新 调用的总运行时间为 $O(T$ 对数 $m)$，而子树和 调用的成本为 $O(1)$。

基于在更新时传播子树和的 SamplerTree 实现是一种标准的经典数据结构。为简洁起见，我们省略进一步的描述。接下来，我们陈述解决问题 1 的第一个构件；这一结果可视为带提示的量子采样。我们将其证明推迟到附录 B，因为该证明主要基于使用有界次数多项式近似推广动态块编码策略，而这一方法由 [GSLW19、vAG19] 首创。

命题 *2*。设 $x \in \mathbb{R}^m_{\geq 0}$ 对应于 *SamplerTree* 的一个实例，且 $\beta \geq \|x\|_1$。设 p 为与 $A^\top x$相关联的吉布斯分布，设 $Z := \sum_{j\in[n]} \exp([A^\top x]_j)$，并且 $\widetilde{Z} \in [Z, CZ]$ 对某个 $C \geq 1$成立。最后，设 $q \in \mathbb{R}^n$ 的条目可在 *O(1)* 时间内经典查询，逐元素满足 $q \geq p$，对所有 $j \in [n]$ 满足 $q_j \in [\frac{\delta}{n}, 1]$，且 $\|q\|_1 = \rho$。假设 $\widetilde{Z}$、C、ρ 和 β均为显式已知。给定 A 的量子预言机 $\in \mathbb{R}^{m\times n}$（定义见第 *2* 节），且 $\|A\|_{\max} \leq 1$，我们可以实现一个 δ-近似吉布斯预言机，其查询成本为 $O(\sqrt{\rho C} \cdot \beta$ 对数$^4 \left(\frac{Cmn}{\delta}\right))$。如果 x 经历了 T次保持 Z、C、ρ、β上不变量的更新调用，则产生的总额外成本~为 $O(T$对数 $m)$。

命题 2 使用了一个高估提示向量 q 和近似归一化~常数 Z，我们将它们统称为 提示。拒绝采样的接受概率由两个主要参数决定：$\rho = \|q\|_1$，它反映了高估程度（可视为提示质量）；以及 $C \geq 1$，它反映了当 $\frac{p_j}{q_j}$是隐式的情况下，我们无法以概率 p 接受的程度（可视为归一化质量）。特别是，命题 2 中使用的拒绝采样方案将改为以概率 $\frac{p_j}{Cq_j}$接受。[5]

这里我们简要阐述命题 2 的实现（更多详情请参见附录 4）。我们沿用命题 2的记号，并令 $w := \mathbf{A}^\top x$ 使得未归一化的

[5]精确计 算 Z 在标准实现中可能需要 $\Omega(n)$ 的时间，这会阻碍实现运行时间 $\propto \sqrt{n}$.

吉布斯分布为 $\exp(w)$，且 $p = \exp(w)/Z$。命题 2 是一个拒绝采样器，它首先将提示 q 加载到叠加态中，然后应用一个过滤器。总体而言，我们的方案形式如下

$$\text{sample } j \sim \frac{q}{\rho}, \text{ then accept with probability } \frac{\exp(w_j)}{CZ \cdot q_j} = \frac{p_j}{Cq_j}, \tag{1}$$

从而以概率 $\approx \frac{1}{\rho C}$ 获得一个被接受的样本，因此在应用量子振幅放大（Grover 搜索 [BHMT02] 的推广）后，需要进行 $\approx \sqrt{\rho C}$ 次试验才能成功。[6]后续的过滤步骤通过适当的块编码技术实现。

上述讨论表明，由 ρ 和 C 参数化的提示质量和归一化质量，对于控制我们方案的接受概率至关重要。更具体地说，在应用命题 2 时，$\beta = \eta T = \widetilde{O}(\frac{1}{\epsilon})$ 是在命题 1 的参数设置下，算法 1 中 x_t 和 y_t 次迭代的 ℓ_1 范数上界。总的来说，实现一个近似吉布斯预言机的代价为（忽略对数因子）$\sqrt{\rho C} \cdot \frac{1}{\epsilon}$。因此，命题 2 将问题 1 归约为维护由向量 $\sim q$ 和归一化估计值 Z 组成的提示这一问题。我们指出，命题 2 严格推广了 [vAG19]，中相应的一个构件；后者只使用了设为全 1向量的 q。

问题 1 的解决方法。我们现在概述如何通过高效运用命题 2 来改进问题 1 的解决方案。为说明我们的方案，我们列出问题 1 的三种解法，它们在整体质量方面各有不同的权衡 ρC。第一种只使用经典信息，完全不使用命题 2；第二种使用命题 2，但在迭代之间不保留任何历史信息；第三种则在前两种的基础上构建，是我们提出的方法。

方案 1：[GK95]。求解问题 1 的一种标准方法是显式更新 $w = \mathrm{A}^\top x$ 和 $\widetilde{\exp}(w)$，并精确维护归一化常数 Z。这样便可以在 O 时间内从 p 中采样。由于在对 x 执行 1-稀疏更新操作时，w 会随 A 的一行发生变化，因此每次迭代都可以在 $O(n)$ 时间内完成。我们可以将其视为方案 (1) 的一个实例，其中 $q = p$、$C = 1$、$\widetilde{Z}$ 和 $\rho = 1$。由此，问题 1 得到的（不平衡）权衡为 $\mathcal{T}_{\text{samp}} = O(1)$ 和 $\mathcal{T}_{\text{update}} = O(n)$。

方案 2：[vAG19]。近期一项工作 [vAG19] 提出了该方案 (1) 的量子实现，并改进了平衡权衡。[vAG19] 方案首先进行均匀抽样；用 (1) 的语言来说，这意味着 $q = \mathbf{1}_n$ 和 $\rho = n$。随后，它应用量子最大值查找 [DH96]，以获取 w 的一个 $\widetilde{\ }$ 近似最大值项；他们证明，这需要时间 $O(\beta \cdot \sqrt{n})$。为简便起见，这里假设它能精确得到 $w_{\max} := \max_{j \in [n]} w_j$。最后，将接受概率 $\frac{p_j}{Cq_j}$ 设为 $\exp(w_j - w_{\max})$。对于 $q = \mathbf{1}_n$，这转化为

$$p_j \cdot \exp(w_{\max} - w_j) = \frac{\exp(w_{\max})}{Z} \leq 1,$$

这意味着 $C = 1$ 已足够。我们注意到，当 w 非常不均匀时，关于 C 的这个界可能是紧的。总体而言，[vAG19] 方案的更新时间需要进行最大值查找，而其抽样时间（根据命题 2）需要时间 $\widetilde{O}(\beta \cdot \sqrt{\rho C}) = \widetilde{O}(\beta \cdot \sqrt{n})$。对于算法 1 中的 $\beta = \widetilde{O}(\frac{1}{\epsilon})$，这给出平衡权衡 $\max(\mathcal{T}_{\text{samp}}, \mathcal{T}_{\text{update}}) = \widetilde{O}\left(\sqrt{n} \cdot \epsilon^{-1}\right)$。正如前文所述，我们的关键洞见是改进 [vAG19]，在隐式使用命题 2 时所选用的这一特定提示。

解决方案 *3*：本工作。我们通过分阶段运行算法来为命题 2 设计更好的提示，每个阶段对应一批 $\approx \frac{1}{\eta}$ 次迭代。在每个阶段开始时，我们使用吉布斯访问

[6]定理 β 在 Pr 命题 2 来自将 $\exp(w_j)$ 通过次数为 $\approx \beta$ 的多项式加载到量子预言机中 .

命题 2 所提供的访问来生成合适的提示，以便高效地执行下一阶段。我们采用这一策略，其参数为整数 $k \in [n]$，并依赖以下观察结果。

1. 在 $\lceil \frac{1}{\eta} \rceil$ 次迭代 $t \in \{\tau + s\}_{s \in [\lceil \frac{1}{\eta} \rceil]}$（其中 τ 表示该阶段的开始）期间，动态吉布斯分布 p_t（其中 t 是迭代索引）会发生 $O(1)$ 的乘法变化，因为 w 逐元素发生 $O(1)$ 的加法变化。因此，提示向量的质量在该阶段内至多会劣化一个常数倍，所以只需在阶段开始时提供一个良好的提示 $q_\tau \geq p_\tau$。

2. 利用上一阶段末尾的命题 2，我们可以高效估计~的较大元素 p_τ。更准确地说，我们从 p_τ 中抽取 $O(k)$ 个样本，并将这些样本的经验分布记为 $\tilde{q}$。切尔诺夫界表明，任何较大的元素 $[p_\tau]_j = \Omega(\frac{1}{k})$都会在经验样本中得到准确反映。因此，我们将提示设为

$$q_j = \begin{cases} \tilde{q}_j \cdot O(1) & \tilde{q}_j = \Omega(\frac{1}{k}) \\ \frac{1}{k} \cdot O(1) & \tilde{q}_j = O(\frac{1}{k}) \end{cases},$$

对于适当的常数。这使提示质量提升至 $\rho \approx \frac{n}{k}$，因为提示中的大项之和至多为 $O(1)$（因为 $\tilde{q}_j \approx p_j$），而小项之和为 $O(\frac{n}{k})$。

3. 我们展示了一种类似的策略：将经验集中性与命题2的测试变体相结合，可以准确估计归一化因子 Z，从而得到 $C = O(1)$。

该策略得到 $\mathcal{T}_{\text{samp}} = \widetilde{O}(\beta \cdot \sqrt{n/k})$ 和 $\mathcal{T}_{\text{update}} = \widetilde{O}(\mathcal{T}_{\text{samp}} \cdot k\eta)$（因为我们将 $\mathcal{T}_{\text{update}}$分摊到 $\approx \frac{1}{\eta}$ 次迭代中）。对于算法1的参数设置，优化 k 可得

$$\max(\mathcal{T}_{\text{samp}}, \mathcal{T}_{\text{update}}) = \widetilde{O}\left(\sqrt{n} \cdot \epsilon^{-\frac{1}{2}}\right).$$

我们在第4节证明定理3，给出问题1的改进解法。忽略对数因子并假设 $\eta \ll 1$（与我们的设定相同），定理3 表明，我们可以维护$\max(\mathcal{T}_{\text{samp}}, \mathcal{T}_{\text{update}})$ = $\widetilde{O}\left(\sqrt{n} \cdot T\eta^{1.5}\right.$ $T = \widetilde{O}\ \epsilon^{-2}$ $\eta = \Theta\ \epsilon$ 1, ()。对于参数设置()、()，如命题中所述，这确实等价于$\max(\mathcal{T}_{\text{samp}}, \mathcal{T}_{\text{update}}) = \widetilde{O}(\sqrt{n} \cdot \epsilon^{-\frac{1}{2}})$。

4 吉布斯采样预言机的实现

在本节中，我们证明定理 3，该定理给出了问题 1 的解法。为此，我们遵循第 3.2 节给出的概要，分批次求解问题 1，每批次包含 $\lceil \frac{1}{\eta} \rceil$ 次迭代，我们将每批次称为一个“阶段”。在第 4.1 节和 4.2 节中，我们只讨论问题 1 的单个阶段，该阶段由迭代 $\tau + s$ 至 $s \in [\lceil \frac{1}{\eta} \rceil]$ 以及某个初始迭代 τ 组成，并假设该阶段开始时满足某些不变量（如下所述）。我们在第 4.3 节给出问题 1 的完整解法。

~ ~**不变量 1** (近似归一化访问)。明确地，我们有 Z_{prev}，其中 $Z_{\text{prev}} \in [Z_\tau, CZ_\tau]$ 对某个 $C = O(1)$。

不变量 2 (初始采样维护)。我们有 $\mathcal{O}_\tau$ 在迭代 τ中求解问题 1 .

本节其余内容安排如下。

- 第 4.1节：我们证明，假设不变量 1 和 2 在某个阶段开始时成立，就可以通过应用命题 $\sim Z$ 及向量 q，执行用于构造提示的预处理，其中包括估计归一化 2。由此可得问题 $\mathcal{T}$ 采样 中的成本 1。

- 第 4.2节：我们证明，在每个阶段结束时，都可以维持不变量 1 和 2，以供下一阶段使用。由此可得问题 $\mathcal{T}_{\text{更新}}$ 中的成本 1。
- 第 4.3节：我们递归调用第 4.1 节和 4.2 节中的子程序（该子程序针对所有满足 1 的迭代 $\tau+s$，其中 $s\in[\lceil\frac{1}{\eta}\rceil]$，对于某个 τ）$\approx \eta T$次，以证明定理 3。

4.1 预处理与近似吉布斯预言机实现

本节将说明如何在可访问 q 的情况下，构造“提示” q，该提示将在整个阶段中使用（阶段从迭代 τ开始），并在假设该阶段满足不变量 1 和 2 的条件下，给出 $\rho=\|q\|_1$的界限，该量用于衡量提示的质量。我们首先证明该阶段中相关吉布斯分布的乘法稳定性。

引理2。 对于所有 $s\in[\lceil\frac{1}{\eta}\rceil]$，我们有

$$Z_{\tau+s}\in\left[\frac{1}{3}Z_\tau,3Z_\tau\right],\ \textit{and}\ p_{\tau+s}\in\left[\frac{1}{9}p_\tau,9p_\tau\right]\ \textit{entrywise.}$$

证明。令 $\nu_t:=\exp(\mathbf{A}^\top x_t)$ 对所有 t 均成立，且满足 $p_t=\frac{\nu_t}{Z_t}$。对于任意 $j\in[n]$，我们有

$$\begin{aligned}\frac{[\nu_{\tau+s}]_j}{[\nu_\tau]_j}&=\exp\left(\left[\mathbf{A}^\top(x_{\tau+s}-x_\tau)\right]_j\right)\\&\in\left[\exp\left(-\|\mathbf{A}\|_{\max}\|x_{\tau+s}-x_\tau\|_1\right),\exp\left(\|\mathbf{A}\|_{\max}\|x_{\tau+s}-x_\tau\|_1\right)\right]\\&\in\left[\exp(-\eta s),\exp(\eta s)\right]\in\left[\frac{1}{3},3\right].\end{aligned}$$

同理，$Z_{\tau+s}\in[\frac{1}{3}Z_\tau,3Z_\tau]$，结合起来即可得出结论。 □

接下来，我们对过估向量 q 的计算由一个整数 $k\in[n]$参数化，该整数将在本节和第 4.2 节中固定不变。我们只需将 q 设为某个经验分布的放大版本，该经验分布由大约 k 个来自 $\mathcal{O}_\tau$ 的样本构成。

引理3。 设 $k\in[n]$，$\alpha\in(0,1)$，并假设 $\delta\le\frac{1}{16k}$。从$\mathcal{O}_\tau$ 中抽取 $N=\Theta(k\log\frac{n\eta T}{\alpha})$ 个样本，其中常数取充分大，并令 $\tilde{q}\in\Delta^n$ 为这 N个样本上的经验分布。定义 $\mathcal{B}:=\{i\in[n]\mid\tilde{q}_i\ge\frac{1}{2k}\}$。那么，对于

$$q_j=\begin{cases}18\tilde{q}_j & j\in\mathcal{B}\\ \frac{18}{k} & j\notin\mathcal{B}\end{cases},$$

以概率 $\ge 1-\frac{\alpha}{2\lceil\eta T\rceil}$，$\|q\|_1=O(\frac{n}{k})$且 $q\ge p_{\tau+s}$逐元素成立，对所有 $s\le\frac{1}{\eta}$均如此。

证明。第一个结论 $\|q\|_1=O\ \frac{n}{k}$ q $\|q\|_1\le 18\|\tilde{q}\|_1+(\ )$由 的定义可立即得出，因为 $\frac{18n}{k}$。根据引理 2（该引理确定性成立），要证明第二个结论，只需证明我们以所需的成功概率同时满足以下两点

$$2\tilde{q}_j\ge[p_\tau]_j\ \text{for all}\ j\in\mathcal{B}\tag{2}$$

and

$$\frac{2}{k}\ge[p_\tau]_j\ \text{for all}\ j\notin\mathcal{B}.\tag{3}$$

为方便记号，记 $\alpha':=\frac{\alpha}{2\lceil\eta T\rceil}$，并令 $\tilde{p}$ 表示从 $\mathcal{O}_\tau$ 中抽取样本的分布，回顾一下 $\|\tilde{p}-p_\tau\|_1\le\frac{1}{16k}$。由于我们从 $\tilde{p}$ 中抽取了 $\Theta(k\log\frac{n}{\alpha'})$ 个样本，根据标准切尔诺夫界，以至少 $1-\alpha'$ 的概率（对所有坐标应用并合界$j\in[n]$），以下两条均成立。

1. 对所有满足 $\tilde{p}_j \geq \frac{1}{4k}$ 的 $j \in [n]$， $\tilde{q}_j \geq \frac{2\tilde{p}_j}{3}$。
2. 对所有满足 $\tilde{p}_j \leq \frac{1}{4k}$ 的 $j \in [n]$， $\tilde{q}_j \leq \frac{1}{2k}$。

我们以这些事件为条件，在证明余下部分中；现在依次证明2）、（3）。

（2）的证明。为证明（2），上面的第二个事件意味着，若$\tilde{p}_j \leq \frac{1}{4k}$，则 $j \notin \mathcal{B}$。因此，对于所有 $j \in \mathcal{B}$，我们有 $\tilde{q}_j \geq \frac{2\tilde{p}_j}{3} \geq \frac{[p_\tau]_j}{2}$，因为 $\|\tilde{p} - p_\tau\|_\infty \leq \frac{1}{16k} \leq \frac{1}{4}\tilde{p}_j$对所有 $j \in \mathcal{B}$均成立。

（3）的证明。为证明（3），反设 $j \notin \mathcal{B}$且 $[p_\tau]_j > \frac{2}{k}$。这意味着$\tilde{p}_j > \frac{1}{k}$，因此根据上面的第一个事件， $\tilde{q}_j \geq \frac{1}{2k}$，这与 $j \notin \mathcal{B}$矛盾。 □

推论 1。假设不变量*1*、*2*在由以下迭代组成的阶段中成立： $\tau + s$， $s \in [\lceil \frac{1}{\eta} \rceil]$。我们可以以概率 $\geq 1 - \frac{\alpha}{2\lceil \eta T \rceil}$求解该阶段中的问题*1*，并且

$$\mathcal{T}_{\text{samp}} := O\left(\sqrt{\frac{n}{k}} \cdot T\eta \log^4\left(\frac{mn}{\delta}\right)\right).$$

证明。 我们将运行引理 3证明中描述的算法，并以算法成功为条件，从而得到失败概率。接下来只需应用命题 2 ，其中 q 在引理 3中定义。对于 q，我们在命题 2 中取 $C = O(1)$（见不变量 1）、 $\rho = O(\frac{n}{k})$（见引理 3）以及 $\beta = T\eta$。显然，命题 q 中关于 2 的各项下界均成立。 □

4.2 维护不变量

现在我们说明如何在迭代 τ'时维护不变量 1$= \tau + \lceil \frac{1}{\eta} \rceil$，以便用于下一阶段，并界定这样做的代价。注意，不变量 2可直接由推论 1中的构造推出。首先，结合引理 2与不变量 1，

$$Z_{\tau'} \in \left[\frac{\widetilde{Z}_{\text{prev}}}{3C}, 3\widetilde{Z}_{\text{prev}}\right]. \tag{4}$$

~ ~这表明我们可以在下一阶段使用 $3Z_{\text{prev}} = Z$ ；然而，这会导致乘法范围 C呈指数级膨胀。为避免这种情况，我们针对一个隐藏的~参数开发了一个检验器，该参数决定成功概率；检验器将用于给出更精细的估计 Z。我们需要命题 2的以下推论，其证明推迟至附录 B。

~**推论 2.** 沿用命题 *2*中的记号，令 $R := \frac{Z}{\widetilde{Z}}$。存在一个量子预言机 $\mathcal{O}_{\text{test}}$，可通过 T 次更新调用 x ，在 $O(T \log m)$ 时间内实现，其查询成本为

$$O\left(\sqrt{\rho C} \cdot \beta \log^4\left(\frac{Cmn}{\ell\delta}\right)\right).$$

此外，对于显式已知常数 C_ℓ 和 C_u， $\mathcal{O}_{\text{test}}$ 以 p 的概率返回“成功”，适用于

$$\frac{C_\ell}{\sqrt{R\rho}} \leq p \leq \frac{C_u}{\sqrt{R\rho}}.$$

推论 2 与命题 2 的不同之处在于，它返回的是布尔值答案（而非从近似吉布斯分布中抽取的样本），且其成功概率由明确的常数参数化。现在我们说明如何利用推论 2 来维持不变式 1。

引理 4。 假设不变式 1、2在由以下迭代构成的阶段中成立 $\tau + s$，$s \in [\lceil \frac{1}{\eta} \rceil]$，并假设 $C \geq \frac{4C_u^2}{C_\ell^2}$对于 $C = O(1)$成立，其中 C_u 和 C_ℓ 是推论 2中的常数。此外，假设我们已得到 q，且其满足引理 3 的结论（即引理中的算法已成功）。我们可以在时间 Z内确定 $Z \in [Z_{\tau'}, CZ_{\tau'}]$，且其成立的概率为 $\geq 1 - \frac{\alpha}{2\lceil \eta T \rceil}$。

$$O\left(\sqrt{\frac{n}{k}} \cdot T\eta \log^4\left(\frac{mn}{\delta}\right) \log\left(\frac{\eta T}{\alpha}\right)\right).$$

证明。 定义 $\widetilde{Z}_0 := 3\widetilde{Z}_{\text{prev}}$，$R_0 := \frac{Z_0}{Z_{\tau'}}$，并注意到 $\widetilde{Z}_0 \in [Z_{\tau'}, 9CZ_{\tau'}]$根据不变量 1和引理 2。接下来，假设引理 3成功，则根据推论 p 中 $\mathcal{O}_{\text{test}}$ 利用估计式得到的成功概率 Z_0满足（对于未知的 $R_0 \in [1, 9C]$，以及已知的 C_ℓ、C_u、ρ）

$$\frac{C_\ell}{\sqrt{R_0 \rho}} \leq p \leq \frac{C_u}{\sqrt{R_0 \rho}}.$$

对于 $N := 27$对数 $\frac{4\lceil \eta T \rceil}{\alpha} \cdot \frac{3\sqrt{C\rho}}{C_\ell}$，我们首先运行 $\mathcal{O}_{\text{test}}$ N次，并检查成功次数，记为 S；根据推论 2，这符合运行时间预算。根据切尔诺夫界，以概率 $\geq 1 - \frac{\alpha}{2\lceil \eta T \rceil}$，有

$$54 \log \frac{4\lceil \eta T \rceil}{\alpha} \cdot \sqrt{\frac{C}{R_0}} \leq \frac{2}{3} pN \leq S \leq \frac{4}{3} pN \leq 108 \log \frac{4\lceil \eta T \rceil}{\alpha} \cdot \frac{C_u}{C_\ell} \cdot \sqrt{\frac{C}{R_0}}.$$

因此，我们可以确定量 R_0，其精度达到乘法因子 $\frac{4C_u^2}{C_\ell^2} \leq C$，这也意味着 $Z_{\tau'}$具有相同的乘法近似因子，正如所需。 □

4.3 定理 3 的证明

定理 3。 设 $\alpha \in (0,1)$ 且 $\delta \leq \eta$。给定一个用于 $\mathbf{A} \in \mathbb{R}^{m \times n}$ （定义于第 2 节）的量子预言机 $\|\mathbf{A}\|_{\max} \leq 1$，我们可以以概率 $\geq 1 - \alpha$ 求解问题 1，其中

$$\max(\mathcal{T}_{\text{samp}}, \mathcal{T}_{\text{update}}) = O\left(1 + \sqrt{n} \cdot T\eta \log^4\left(\frac{mn}{\delta}\right) \cdot \left(\sqrt{\eta \log\left(\frac{n\eta T}{\alpha}\right)} + \eta \log\left(\frac{n\eta T}{\alpha}\right)\right)\right),$$

并且需要额外的初始化成本

$$O\left(\eta^3 T^3 \log^4\left(\frac{n\eta T}{\delta}\right) + \log^7\left(\frac{n\eta T}{\delta}\right)\right).$$

证明。 我们首先断言，对于任意 $k \in [n]$，我们可以以概率 $\geq 1 - \alpha$ 求解问题 1，且

$$\mathcal{T}_{\text{samp}} = O\left(\sqrt{\frac{n}{k}} \cdot T\eta \log^4\left(\frac{mn}{\delta}\right)\right),$$
$$\mathcal{T}_{\text{update}} = O\left(\left(\sqrt{\frac{n}{k}} \cdot T\eta \log^4\left(\frac{mn}{\delta}\right)\right) \cdot k\eta \log\left(\frac{n\eta T}{\alpha}\right)\right).$$

这由引理3（在 $\lceil \frac{1}{\eta} \rceil$ 次迭代中摊销）、推论 1 和引理 4 结合得出，并对至多 $\lceil \eta T \rceil$ 个阶段应用并合界。这里我们注意到，为支持引理 1、命题 2 和推论 2 中的更新所需的每次迭代 $\log m$ 的成本，x 并非主要成本。通过选取 $k = \Theta(\max(1, (\eta \log \frac{mn}{\alpha\epsilon})^{-1}))$，我们平衡了 $\mathcal{T}_{\text{samp}}$ 和 $\mathcal{T}_{\text{update}}$ 的成本，从而得到结论。最后我们注意到，通过在 k 的定义中选取适当的常数，我们有 $\delta \leq \eta \implies \delta \leq \frac{1}{16k}$，满足引理3的要求；引理3是唯一对 δ 的界限作出规定的部分。 □

致谢

我们感谢 András Gilyén 就先前工作 [vAG19] 提供交流。AB 的研究部分获得了美国能源部 QuantISED 资助 DE-SC0020360、美国空军科学研究办公室资助 FA9550-21- 1-0392，以及美国能源部科学办公室奖项编号 DE-SC0020266 的支持。YG 的研究部分获得了斯坦福大学管理科学与工程系 DE&I 研究计划的支持。YJ 的研究部分获得了斯坦福研究生奖学金和 Danzig-Lieberman 研究生奖学金的支持。AS 的研究部分获得了微软研究院教师奖学金、美国国家科学基金会 CAREER 奖 CCF1844855、美国国家科学基金会资助 CCF-1955039、PayPal 研究奖和斯隆研究奖学金的支持。KT 感谢 Ewin Tang 在量子线性代数方面提供的专业知识，并解答了我们的许多问题。

参考文献

[Aar15] Scott Aaronson。《仔细阅读细则》。《自然·物理》，11(4):291–293，2015年。

[AK07] Sanjeev Arora 和 Satyen Kale。半定规划的组合式原始-对偶规划。在第三十九届 *ACM* 年度计算理论研讨会论文集计算，第 227–236 页，2007 年。

[AL17] Zeyuan Allen-Zhu 和 Yuanzhi Li。 跟随压缩领导者：更快速的在线特征向量学习与更快的矩阵乘法权重更新。在 Doina Precup 和 Yee Whye Teh 编，编辑， 《第*34*届国际机器学习会议论文集》，*ICML 2017*，澳大利亚新南威尔士州悉尼，*2017*年*8*月*6*日至*11*日，第70卷，载于《机器学习研究论文集，第116–125页。PMLR，2017年。

[Alm21] Josh Alman。 矩阵乘法通用方法的界限。 理论计算机，17:1–30，2021。

[AW21] Josh Alman 和 Virginia Vassilevska Williams。改进的激光法以及更快的矩阵乘法。Dániel Marx，编辑，*2021*年*ACM-SIAM*会议论文集离散算法研讨会，*SODA 2021*，线上会议，*1*月*10*日*-13*日，*2021*年，第522–539页。SIAM，2021年。

[BHMT02] Gilles Brassard、Peter Høyer、Michele Mosca和Alain Tapp。量子振幅放大与估计。量子计算与量子信息，305:53–74 ，2002。

[BS17] Fernando GSL Brandao 和 Krysta M Svore。 用于求解的量子加速半定规划。在 *2017* 年 *IEEE* 第 *58* 届年度基础研讨会计算机科学（*FOCS*），第 415–426 页。IEEE，2017 年。

[Bub15] Sébastien Bubeck。凸优化：算法与复杂性。基础与机器学习趋势，8(3-4):231–357，2015 年。

[BWP+17] Jacob Biamonte、Peter Wittek、Nicola Pancotti、Patrick Rebentrost、Nathan Wiebe，和 Seth Lloyd。《量子机器学习》。《自然》，549(7671):195–202，2017 年。

[CCLW20] Shouvanik Chakrabarti、Andrew M Childs、Tongyang Li 和 Xiaodi Wu。量子算法与凸优化的下界。《*Quantum*》，4:221，2020 年。

[CDST19] Yair Carmon、John C. Duchi、Aaron Sidford 和 Kevin Tian。矩阵乘法权重的秩一草图。载于 Alina Beygelzimer 和 Daniel Hsu 编，《学习理论会议，COLT 2019，2019年6月25日至28日，美国亚利桑那州凤凰城》，《机器学习研究论文集》第99卷，第589–623页。PMLR，2019年。[CGL+20] Nai-Hui Chia、András Gilyén、Tongyang Li、Han-Hsuan Lin、Ewin Tang 和 Chun-hao Wang。用于量子机器学习去量子化的基于采样的次线性低秩矩阵运算框架。载于《第52届ACM SIGACT计算理论研讨会论文集》，第387–400页，2020年。[CJST19] Yair Carmon、Yujia Jin、Aaron Sidford 和 Kevin Tian。矩阵博弈的方差缩减。载于 Hanna M. Wallach、Hugo Larochelle、Alina Beygelzimer、Florence d'Alché-Buc、Emily B. Fox 和 Roman Garnett 编，《神经信息处理系统进展32：2019年神经信息处理系统年会（NeurIPS 2019），2019年12月8日至14日，加拿大不列颠哥伦比亚省温哥华》，第11377–11388页，2019年。[CJST20] Yair Carmon、Yujia Jin、Aaron Sidford 和 Kevin Tian。矩阵博弈的坐标方法。载于 Sandy Irani 编，《第61届IEEE计算机科学基础年会（FOCS 2020），2020年11月16日至19日，美国北卡罗来纳州达勒姆》，第283–293页。IEEE，2020年。[CLS21] Michael B Cohen、Yin Tat Lee 和 Zhao Song。以当前矩阵乘法时间求解线性规划。《ACM学报（JACM）》，68(1):1–39，2021年。[DH96] Christoph Dürr 和 Peter Høyer。一种寻找最小值的量子算法。《CoRR》，quant-ph/9607014，1996年。[DNV20] Daniel Dadush、Bento Natura 和 Làszlò A Vègh。重新审视线性规划的Tardos框架：利用近似求解器更快地获得精确解。载于 Sandy Irani 编，《第61届IEEE计算机科学基础年会（FOCS 2020），2020年11月16日至19日，美国北卡罗来纳州达勒姆》，第931–942页。IEEE，2020年。[GAW19] András Gilyén、Srinivasan Arunachalam 和 Nathan Wiebe。通过更快的量子梯度计算优化量子优化算法。载于《第三十届ACM-SIAM离散算法研讨会论文集》，第1425–1444页。SIAM，2019年。[GK95] Michael D. Grigoriadis 和 Leonid G. Khachiyan。一种用于矩阵博弈的次线性时间随机近似算法。《运筹学快报》，18(2):53–58，1995年。[GLG22] Sevag Gharibian 和 François Le Gall。量子奇异值变换的去量子化：关于量子化学和量子PCP猜想的难度与应用。载于《第54届ACM SIGACT计算理论研讨会论文集》，第19–32页，2022年。[GR02] Lov Grover 和 Terry Rudolph。创建与可高效积分的概率分布相对应的叠加态。《CoRR》，abs/quant-ph/0208112，2002年。

[GSLW19] András Gilyén、Yuan Su、Guang Hao Low 和 Nathan Wiebe。量子奇异值变换及其拓展：量子矩阵算术的指数级改进。载于 Moses Charikar 和 Edith Cohen 编，《第51届ACM SIGACT计算理论研讨会论文集，STOC 2019，2019年6月23日至26日，美国亚利桑那州凤凰城》，第193–204页。ACM，2019年。[Haa19] Jeongwan Haah。量子信号处理中周期函数的乘积分解。《Quantum》，3:190，2019年。[HHL09] Aram W Harrow、Avinatan Hassidim 和 Seth Lloyd。求解线性方程组的量子算法。《物理评论快报》，103(15):150502，2009年。[Jor05] Stephen P Jordan。用于数值梯度估计的快速量子算法。《物理评论快报》，95(5):050501，2005年。[JSWZ21] Shunhua Jiang、Zhao Song、Omri Weinstein 和 Hengjie Zhang。求解一般线性规划的更快算法。载于《第53届ACM SIGACT计算理论研讨会论文集，STOC 2021》，第823–832页，2021年。[Kar84] Narendra Karmarkar。一种新的线性规划多项式时间算法。载于《第十六届ACM计算理论研讨会年会论文集》，第302–311页，1984年。[KP16] Iordanis Kerenidis 和 Anupam Prakash。量子推荐系统。arXiv预印本 arXiv:1603.08675，2016年。[KP20] Iordanis Kerenidis 和 Anupam Prakash。用于线性规划和半定规划的量子内点法。《ACM量子计算汇刊》，1(1):1–32，2020年。[LCW19] Tongyang Li、Shouvanik Chakrabarti 和 Xiaodi Wu。用于训练线性分类器和基于核的分类器的次线性量子算法。载于《国际机器学习会议》，第3815–3824页。PMLR，2019年。[LMR14] Seth Lloyd、Masoud Mohseni 和 Patrick Rebentrost。量子主成分分析。《自然·物理》，10(9):631–633，2014年。[LS14] Yin Tat Lee 和 Aaron Sidford。线性规划的路径寻找方法：以 o (vrank) 次迭代求解线性规划，以及更快的最大流算法。载于《2014年IEEE第55届计算机科学基础年会》，第424–433页。IEEE，2014年。[LS19] Yin Tat Lee 和 Aaron Sidford。利用 sqrt (rank) 次线性方程组求解来求解线性规划。arXiv预印本 arXiv:1910.08033，2019年。[LWCW21] Tongyang Li、Chunhao Wang、Shouvanik Chakrabarti 和 Xiaodi Wu。用于一般矩阵博弈的次线性经典与量子算法。载于《AAAI人工智能会议论文集》，第35卷，第8465–8473页，2021年。[Nem04] Arkadi Nemirovski。具有收敛速率 $O(1/t)$ 的近端方法，适用于具有Lipschitz连续单调算子的变分不等式和光滑凸凹鞍点问题。《SIAM优化杂志》，15(1):229–251，2004年。

[Nes07] 尤里·涅斯捷罗夫。对偶外推及其在求解变分不等式和相关问题中的应用。《数学规划》，109(2-3)：319–344，2007年。[Neu28] 约翰·冯·诺伊曼。论博弈论。《数学年刊》，100：295–320，1928年。[NJLS09] Arkadi Nemirovski、阿纳托利·B·尤季茨基、蓝光辉和亚历山大·沙皮罗。随机规划的鲁棒随机逼近方法。《*SIAM*优化期刊》，19(4)：1574–1609，2009年。[Ren88] 詹姆斯·雷内加。一种基于牛顿法的线性规划多项式时间算法。《数学规划》，40(1)：59–93，1988年。[RML14] Patrick Rebentrost、Masoud Mohseni 和 Seth Lloyd。用于大数据分类的量子支持向量机。《物理评论快报》，113(13)：130503，2014年。[SV14] 苏尚特·萨赫德瓦和尼希特·K·维什诺伊。通过逼近理论实现更快的算法。计算理论与计算机科学前沿，9(2)：125–210，2014年。[Tan19] Ewin Tang。用于推荐系统的量子启发式经典算法。载于第*51*届*ACM SIGACT*计算理论研讨会论文集，第217–228页，2019年。[vAG19] 约兰·范阿佩尔多恩和András Gilyén。零和博弈的量子算法。$CoRR$，abs/1904.03180，2019年。[vAGGdW20a] 约兰·范阿佩尔多恩、András Gilyén、桑德·格里布林和罗纳德·德沃尔夫。使用量子预言机进行凸优化。《*Quantum*》，4：220，2020年。[VAGGdW20b] 约兰·范阿佩尔多恩、András Gilyén、桑德·格里布林和罗纳德·德沃尔夫。量子半定规划求解器：更好的上界和下界。《*Quantum*》，4：230，2020年。[vdB20] 扬·范登布兰德。一个在当前矩阵乘法时间内运行的确定性线性规划求解器。载于第*31*届*ACM-SIAM*离散算法研讨会论文集（*SODA 2020*），第259–278页，2020年。[vdBLL+21] 扬·范登布兰德、Yin Tat Lee、刘洋P.、塔查蓬·萨拉努拉克、Aaron Sidford、Zhao Song 和王迪。稠密实例中近线性时间求解最小费用流、马尔可夫决策过程和 ℓ_1-回归。载于第*53*届*ACM SIGACT*计算理论研讨会论文集（*STOC 2021*），第859–869页，2021年。[vdBLSS20] 扬·范登布兰德、Yin Tat Lee、Aaron Sidford 和 Zhao Song。近线性时间求解高瘦稠密线性规划。载于第*52*届*ACM SIGACT*计算理论研讨会论文集，第775–788页，2020年。

A 使用吉布斯采样预言机求解矩阵博弈

在本节中，我们证明命题1，该命题展示了如何使用近似吉布斯采样预言机求解零和矩阵博弈（通过算法1）。为简要说明我们所用算法及其保证的证明，我们回顾一下所考虑的问题具有如下形式

$$\min_{v\in\Delta^n}\max_{u\in\Delta^m} f(u,v) := u^\top \mathbf{A} v, \quad \text{where} \quad \|\mathbf{A}\|_{\max} \le 1, \tag{5}$$

并将相应的梯度算子定义为

$$g(u,v) = (-\mathbf{A}v, \mathbf{A}^\top u). \tag{6}$$

众所周知，对（5）中的梯度算子执行（随机）镜像下降步骤，可以得到矩阵博弈[Bub15]的一个近似纳什均衡。我们证明，对该策略进行近似实现，并结合适当的子采样，可以高效地得到一个近似纳什均衡。我们首先给出以下观察。

引理5。设 $u,\tilde{u}\in\Delta^m$ 满足 $\|u-\tilde{u}\|_1 \le \delta$。设 $\tilde{g} := \mathbf{A}_{i:}$，其中 $i\sim\tilde{u}$，且 $g := \mathbf{A}^\top u$。则，$\|g - \mathbb{E}\tilde{g}\|_\infty \le \delta$。

证明。注意到 $\mathbb{E}\tilde{g} = \mathrm{A}^\top\tilde{u}$，且 $\left\|\mathrm{A}^\top(u-\tilde{u})\right\|_\infty \le \|u-\tilde{u}\|_1 \le \delta$，因为 $\|\mathrm{A}\|_{\max} \le 1$。 □

接下来，我们给出经典镜像下降分析的一种变体，它界定了子采样前算法 1 各迭代点的期望近似质量。

命题3。设在算法 1 中，$\delta \le \frac{\epsilon}{20}$，$\eta = \frac{\epsilon}{15}$和 $T \ge \frac{6\log(mn)}{\eta\epsilon}$。设算法 1 的迭代点为 $\{x_t, y_t\}_{t=0}^{T-1}$，并记 $u_t := \exp(A y_t)/\|\exp(A y_t)\|_1$，$v_t := \exp(-A^\top x_t)/\|\exp(-\mathbf{A}^\top x_t)\|_1$，对所有 $0\le t<T$ 均成立。对于 $(\bar{u},\bar{v}) := \frac{1}{T}\sum_{t=0}^{T-1}(u_t, v_t)$，有

$$\mathbb{E}\left[\max_{u\in\Delta^m} u^\top \mathbf{A}\bar{v} - \min_{v\in\Delta^n}\bar{u}^\top\mathbf{A}v\right] \le \epsilon. \tag{7}$$

证明。根据更新的定义，在每次迭代 $0\le t\le T-1$，我们有 e

$$u_{t+1} = \mathrm{argmin}_{u\in\Delta^m}\left\{\eta\langle -\mathbf{A}_{:j_t}, u\rangle + \sum_{i\in[m]}[u]_i\log\frac{[u]_i}{[u_t]_i}\right\},$$

$$v_{t+1} = \mathrm{argmin}_{v\in\Delta^n}\left\{\eta\langle \mathbf{A}_{i_t:}, v\rangle + \sum_{j\in[n]}[v]_j\log\frac{[v]_j}{[v_t]_j}\right\}.$$

因此，根据 u_{t+1} 和 v_{t+1} 各自的最优性条件，对于任意 $u\in\Delta^m$、$v\in\Delta^n$，并令 $V_x(x') := \sum_k [x']_k \log\frac{[x']_k}{[x]_k}$ 表示适当维度的单纯形变量之间的 KL散度，

$$\begin{aligned}
\langle -\mathbf{A}_{:j}, u_t - u\rangle + \langle \mathbf{A}_{i:}, v_t - v\rangle &\le \frac{1}{\eta}\left(V_{u_t}(u) - V_{u_{t+1}}(u) + V_{v_t}(v) - V_{v_{t+1}}(v)\right) \\
&\quad + \left(\langle -\mathbf{A}_{:j}, u_t - u_{t+1}\rangle - \frac{1}{\eta}V_{u_t}(u_{t+1})\right) \\
&\quad + \left(\langle \mathbf{A}_{i:}, v_t - v_{t+1}\rangle - \frac{1}{\eta}V_{v_t}(v_{t+1})\right) \\
&\le \frac{1}{\eta}\left(V_{u_t}(u) - V_{u_{t+1}}(u) + V_{v_t}(v) - V_{v_{t+1}}(v)\right) \\
&\quad + \frac{\eta}{2}\|\mathbf{A}_{:j}\|_\infty^2 + \frac{\eta}{2}\|\mathbf{A}_{i:}\|_\infty^2,
\end{aligned} \tag{8}$$

其中，对于最后一个不等式，我们使用了霍尔德不等式，以及 V 在 ℓ_1 范数下是 1-强凸的这一事实（由平克赛不等式可得）。对上述结果关于 $0 \le t < T$ 取平均，并记 $w_t := (u_t, v_t)$ 和 $\tilde{g}_t := (-\mathbf{A}_{:j_t}, \mathbf{A}_{i_t:})$，则对于任意 $w = (u, v) \in \Delta^m \times \Delta^n$，

$$\frac{1}{T}\sum_{t=0}^{T-1}\langle \tilde{g}_t, w_t - w\rangle \le \frac{1}{\eta T}\left(V_{u_0}(u) + V_{v_0}(v)\right) + \eta. \tag{9}$$

在上述内容中，我们进一步回顾了界 $\|\mathbf{A}\|_{\max} \le 1$，这是由假设得到的。为了界定左侧与其期望之间的偏差，我们采用“幽灵迭代”论证，沿用[NJLS09、CJST19]中的方法。具体而言，我们定义迭代序列 $\tilde{u}_t$，$\tilde{v}_t$ 如下：令 $\tilde{u}_0 \leftarrow u_0$，$\tilde{v}_0 \leftarrow v_0$，然后对每个 $0 \le t < T$，定义

$$\tilde{u}_{t+1} := \mathrm{argmin}_{u\in\Delta^m}\left\{\eta\langle -\mathbf{A}v_t + \mathbf{A}_{:j_t}, \bar{u}\rangle + \sum_{i\in[m]}[u]_i \log\frac{[u]_i}{[\tilde{u}_t]_i}\right\},$$

$$\tilde{v}_{t+1} := \mathrm{argmin}_{v\in\Delta^n}\left\{\eta\langle \mathbf{A}^\top u_t - \mathbf{A}_{:i_t}, \bar{v}\rangle + \sum_{j\in[n]}[v]_j \log\frac{[v]_j}{[\tilde{v}_t]_j}\right\},$$

其中，上述 i, j 与定义 u_{t+1} 和 v_{t+1} 的更新时所用的坐标相同。由与（8）类似的界，并注意到 $\left\|\mathbf{A}_{:j_t} - \mathbf{A}^\top v_t\right\|_\infty, \|\mathbf{A}u_t - \mathbf{A}_{i_t:}\|_\infty \le 2$,

$$\left\langle -\mathbf{A}^\top v_t + \mathbf{A}_{:j_t}, \tilde{u}_t - u\right\rangle + \langle \mathbf{A}u_t - \mathbf{A}_{i_t:}, \tilde{v}_t - v\rangle \le \frac{1}{\eta}\left(V_{\tilde{u}_t}(u) - V_{\tilde{u}_{t+1}}(u) + V_{\tilde{v}_t}(v) - V_{\tilde{v}_{t+1}}(v)\right) + 4\eta.$$

对上述结果关于 $0 \le t < T$ 取平均，并记 $\tilde{w}_t := (\tilde{u}_t, \tilde{v}_t)$ 以及 $g_t := g(w_t)$（见（5））， 我们得到：对于任意 $w = (u, v) \in \Delta^m \times \Delta^n$,

$$\frac{1}{T}\sum_{t\in[T]-1}\langle g_t - \tilde{g}_t, \tilde{w}_t - w\rangle \le \frac{1}{\eta T}\left(V_{u_0}(u) + V_{v_0}(v)\right) + 4\eta. \tag{10}$$

求和 不等式（9）和（10），并对 $w = (u, v) \in \Delta^m \times \Delta^n$取最大值，可得

$$\begin{aligned}\max_{w\in\Delta^m\times\Delta^n}\frac{1}{T}\sum_{t=0}^{T-1}\langle g_t, w_t - w\rangle \le{}& \max_{u\in\Delta^n, v\in\Delta^m}\frac{2}{\eta T}\left(V_{u_0}(u) + V_{v_0}(v)\right)\\ &+ 5\eta + \frac{1}{T}\sum_{t=0}^{T-1}\langle g_t - \tilde{g}_t, w_t - \tilde{w}_t\rangle.\end{aligned} \tag{11}$$

对上述内容取期望，我们得到

$$\begin{aligned}\mathbb{E}\left[\max_{w\in\Delta^m\times\Delta^n}\frac{1}{T}\sum_{t=0}^{T-1}\langle g_t, w_t - w\rangle\right] &\le \max_{u\in\Delta^n, v\in\Delta^m}\frac{2}{\eta T}\left[V_{u_0}(u) + V_{v_0}(v)\right]\\ &\quad + 5\eta + \mathbb{E}\left[\frac{1}{T}\sum_{t=0}^{T-1}\langle g_t - \tilde{g}_t, w_t - \tilde{w}_t\rangle\right]\\ &\overset{(i)}{\le} \frac{2\log(mn)}{\eta T} + 5\eta + \frac{1}{T}\sum_{t\in[T]-1}\langle g_t - \mathbb{E}\tilde{g}_t, w_t - \bar{w}_t\rangle,\\ &\overset{(ii)}{\le} \frac{2\log(mn)}{\eta T} + 5\eta + 4\delta \overset{(iii)}{\le} \epsilon.\end{aligned}$$

在上述推导中，(*i*) 用到了 KL散度相对于均匀分布的直径界，即 $\max_{u\in\Delta^m} V_{u_0}(u) = \log m$（对 $V_{v_0}(v)$ 也有类似的界）。此外，(*ii*) 用到了 $\tilde{g}_t$ 在给定条件下与 w_t 和 $\tilde{w}_t$ 相互独立这一点，并用到了关于吉布斯采样器的假设 $\|g_t - \mathbb{E}\tilde{g}_t\|_\infty \le \delta$（通过引理5）、霍尔德不等式；而 (*iii*) 用到了我们对 T、η 和 δ 的选取。

最后，我们指出，所需结论可由线性性得出：对于任意 $w = (u, v)$，

$$\begin{aligned}\frac{1}{T}\sum_{t=0}^{T-1}\langle g_t, w_t - w\rangle &= \left\langle g\left(\frac{1}{T}\sum_{t=0}^{T-1} w_t\right), \frac{1}{T}\sum_{t=0}^{T-1} w_t - w\right\rangle \\ &= u^\top \mathbf{A}\bar{v} - \bar{u}^\top \mathbf{A} v.\end{aligned}$$

□

通过使用一个简单的鞅论证（其思路受 [AL17、CDST19]中的方法启发），对（11）中的误差项进行界定，我们证明命题 3 中的保证以高概率成立。

推论 3。 设 $\alpha \in (0,\ 1)$，并设 $\delta \le \frac{\epsilon}{20}$、$\eta = \frac{\epsilon}{20}$和 $T \ge {}^{8}\log(\ \frac{mn}{\eta\epsilon} + 2048)\log_{\epsilon^2}{}^{\frac{1}{\alpha}}$在算法 *1*中。则以至少 $1-\alpha$的概率，按照命题 *3*的记号，$(\bar{u},\ \bar{v})$ 是矩阵 ϵ的 -近似纳什均衡。$\mathbf{A}$。

证明。 考虑由以下对象给出的滤过 $\mathcal{F}_t = \sigma(u_0,\ v_0,\ \tilde{g}_0,\ \cdots,\ \tilde{g}_t,\ u_{t+1},\ v_{t+1})$。我们将对（$\sum_{t=0}^{T-1}\langle g_t - \tilde{g}_t,\ w_t - \bar{w}_t\rangle$）中的项进行界定。为此，我们定义如下形式的鞅差序列 D_t：$= \langle g_t - \tilde{g}_t,\ w_t - \bar{w}_t\rangle - \langle g_t - \mathbb{E}\left[\tilde{g}_t|\mathcal{F}_{t-1}\right],\ w_t - \bar{w}_t\rangle$，它适应于滤过 $\mathcal{F}_t$。我们首先注意到 $D_t \le \|g_{t-1} - \tilde{g}_{t-1}\|_\infty \|w_{t-1} - \bar{w}_{t-1}\|_1 \le 8$ 以概率 1成立。因此，应用阿祖马-霍夫丁不等式可得

$$\sum_{t=0}^{T-1} D_t \le \sqrt{128T\log\frac{1}{\alpha}} \text{ with probability } \ge 1-\alpha.$$

将其代回（11），并利用 KL 散度范围界引理 5，结合我们对 $\mathcal{O}^{\text{gibbs}}$ 的定义及参数选择，我们由此以概率 $1-\alpha$ 得到：

$$\max_{w\in\Delta^m\times\Delta^n}\frac{1}{T}\sum_{t=0}^{T-1}\langle g_t, w_t - w\rangle \le \frac{2\log mn}{\eta T} + 5\eta + 4\delta + \sqrt{\frac{128\log\frac{1}{\alpha}}{T}} \le \epsilon. \tag{12}$$

证明的其余部分与命题 3 的证明类似。 □

吉布斯采样预言机隐式地维护对 $u_t \propto \exp(\mathbf{A}y_t)$ 和 $v_t \propto \exp(-\mathbf{A}^\top x_t)$ 的访问，通过取平均可得到 $(\bar{u},\ \bar{v}) = \frac{1}{T}\sum_{t=0}^{T-1}(u_t,\ v_t)$，如推论 3 所保证的，这是一个近似均衡。为了将隐式维护的迭代序列转化为实际的经典输出，我们对这些迭代进行子采样。下面我们将正式证明：从接近 $\bar{u}$ 和 $\bar{v}$ 的分布中独立抽取样本并取其经验平均，也能以高概率得到一个近似均衡（近似因子相同，至多相差常数因子）。

引理 6. 假设 $\bar{u} = \frac{1}{T}\sum_{t=0}^{T-1} u_t$对于 $\{u_t\}_{t=0}^{T-1} \subset \Delta^m$ 以及 $\bar{v} = \frac{1}{T}\sum_{t=0}^{T-1} v_t$对于 $\{v_t\}_{t=0}^{T-1} \subset \Delta^n$ 是 $\mathbf{A}$ 的一个ϵ-近似纳什均衡。进一步假设存在某个 $\delta \in (0,1)$，使得 $\{\tilde{u}_t\}_{t=0}^{T-1} \subset \Delta^m$, $\{\tilde{v}_t\}_{t=0}^{T-1} \subset \Delta^n$，并且对于所有 $0 \le t < T-1$，都有 $\|\tilde{u}_t - u_t\|_1 \le \delta$ 和 $\|\tilde{v}_t - v_t\|_1 \le \delta$。令 $\hat{}u = \frac{1}{T}\sum_{t=0}^{T-1} e_{i_t}$，其中每个 $e_{i_t} \in \mathbb{R}^m$ 均根据 $\tilde{u}_t$独立抽取；类似地，令 $\hat{}v = \frac{1}{T}\sum_{t=0}^{T-1} e_{j_t}$，其中每个$e_{j_t} \in \mathbb{R}^n$ 均根据 $\tilde{v}_t$独立抽取。假设 $T \ge {}^{16}\log_{\epsilon^2}{}^{\frac{mn}{\alpha}}$。那么，以至少 $1-\alpha$ 的概率，$(\hat{}u, \hat{}v)$ 是 $\mathbf{A}$ 的一个 $(2\epsilon + 2\delta)$-近似纳什均衡。

证明。首先，令 $\tilde{u}_{\text{avg}} = \frac{1}{T}\sum_{t=0}^{T-1}\tilde{u}_t$和 $\tilde{v}_{\text{avg}} = \frac{1}{T}\sum_{t=0}^{T-1}\tilde{v}_t$。由范数的凸性可得$\|\tilde{u}_{\text{avg}} - \bar{u}\|_1 \le \delta$和 $\|\tilde{v}_{\text{avg}} - \bar{v}\|_1 \le \delta$，因此根据 $(\bar{u}, \bar{v})$ 的纳什均衡近似保证以及霍尔德不等式，

$$\max_{u\in\Delta^m} u^\top \mathbf{A}\tilde{v}_{\text{avg}} - \min_{v\in\Delta^m} \tilde{u}_{\text{avg}}^\top \mathbf{A} v \le \epsilon + 2\delta.$$

设 z 是 $[-1,1]^n$ 中的一个固定向量。根据霍夫丁不等式，由于每个随机变量 $\langle z, e_{j_t}\rangle$ 的取值范围为 $[-1,1]$ 和 $\hat{\mathbb{E}v} = \tilde{v}_{\text{avg}}$，我们有

$$\Pr\left[|\langle z, \hat{v} - \tilde{v}_{\text{avg}}\rangle| \ge \frac{\epsilon}{2}\right] \le 2\exp\left(-\frac{T\epsilon^2}{8}\right) \le \frac{\alpha}{m+n}. \tag{13}$$

接下来，注意到 $\max_{u\in\Delta^m} u^\top \mathbf{A}\tilde{v}_{\text{avg}}$ 可由一个基向量 $u = e_i$取得。因此，对所有 13个 $z = \mathbf{A}_{i:}$ 应用并合界可知，其概率至少为 $1 - \frac{\alpha m}{m+n}$，

$$\max_{u\in\Delta^m} u^\top \mathbf{A}\hat{v} \le \max_{u\in\Delta^m} u^\top \mathbf{A}\tilde{v}_{\text{avg}} + \frac{\epsilon}{2}.$$

由对称性可知，其概率至少为 $1 - \frac{\alpha n}{m+n}$，

$$\min_{v\in\Delta^n} \hat{u}^\top \mathbf{A} v \ge \min_{v\in\Delta^n} \tilde{u}_{\text{avg}}^\top \mathbf{A} v - \frac{\epsilon}{2}.$$

结论由并合界以及结合以上三个表达式即可得出。 □

最后，我们将这些部分组合起来，给出一个完整的保证。

命题1. 设 $\mathbf{A} \in \mathbb{R}^{m\times n}$满足 $\|\mathbf{A}\|_{\max} \le 1$且 ϵ， $\alpha \in (0,\ 1)$。设 $\delta \le \frac{\epsilon}{20}$， $\eta = \frac{\epsilon}{60}$，且 $T = \Theta(\epsilon^{-2}\log\frac{mn}{\alpha})$其中常数取适当值。以概率 $\ge 1-\alpha$，算法 *1*输出一个ϵ-近似纳什均衡，针对 $\mathbf{A}$。

证明。我们沿用命题 3的记号。应用推论 3（忽略常数因子），可知以至少 $1 - \frac{\alpha}{2}$ 的概率， $\bar{u} := \frac{1}{T}\sum_{t=0}^{T-1} u_t$和 $\bar{v} := \frac{1}{T}\sum_{t=0}^{T-1} v_t$满足

$$\max_{u\in\Delta^m} u^\top \mathbf{A}\bar{v} - \min_{v\in\Delta^n} \bar{u}^\top \mathbf{A} v \le \frac{\epsilon}{3}.$$

最后，引理 6（ 失败概率为$\frac{\alpha}{2}$），再应用并合界即可得到所需结论。 □

B 带提示的量子拒绝采样

本节证明命题 2，该命题给出一种动态量子拒绝采样子程序，并界定其实现成本。我们的结果扩展了 [vAG19], 中的类似研究，但表述得更为一般，以便在拒绝采样过程中使用适当的“提示”向量。我们将分几部分逐步介绍主要结果。

振幅放大。 首先，对于一个先应用酉算子 $\mathbf{U}$再进行测量、并以概率 α得到接受态的量子判定算法，量子放大 [BHMT02]表明，我们可以应用 $\mathbf{U}$ $\approx \alpha^{-\frac{1}{2}}$ 次，从而以高概率得到接受态。

命题 4 (定理 3, [BHMT02])。 设 $S \subseteq \{0,1\}^s$，设 $\mathbf{U}$ 是一个 s-量子比特量子预言机，并设 α 为对应用 $\mathbf{U}$ 的结果进行测量后得到接受态的概率。存在一种（量子）算法，使用 $O(\alpha^{-\frac{1}{2}}\log\frac{1}{\delta})$ 次对 $\mathbf{U}$ 的查询，并耗费 $O(\log s \log\frac{1}{\delta})$ 额外时间，以 s 为结果，且 $s \in S$ 的概率为 $\ge 1-\delta$。

从树中加载。 给定一个动态向量 $x \in \mathbb{R}^m_{\geq 0}$，它由适当高效的数据结构 SamplerTree (参见引理 1) 支持，且已知上界 $\beta \geq \|x\|_1$，我们回顾 [GR02] 的一个结果，该结果允许我们将 x （经过适当缩放后的）各项构造成叠加态。

引理 7. 令 $x \in \mathbb{R}^m_{\geq 0}$ 对应于一个SamplerTree实例，且 $\beta \geq \|x\|_1$。我们可以维护一个量子预言机 $\mathcal{O}_{\mathsf{SamplerTree}}$，其调用耗时为 $O(\log m)$，使得在执行 T 次更新 操作后，构建$\mathcal{O}_{\mathsf{SamplerTree}}$ 的总成本为 $O(T \log m)$，并且

$$\mathcal{O}_{\mathsf{SamplerTree}}|0\rangle^{\otimes(a+1)} = \sum_{i\in[m]} \sqrt{\frac{x_i}{\beta}}|0\rangle|i\rangle + \sqrt{1-\frac{\|x\|_1}{\beta}}|1\rangle|g\rangle.$$

证明。 这隐含于 [GR02]。我们首先应用一个 1量子比特量子门，根据是否从树中选取进行条件控制（概率为 $\frac{\|x\|_1}{\beta}$），然后在第一个量子比特为 $|0\rangle$时，应用 [GR02] 过程；该过程每次控制一个量子比特，同时传播子树和（由SamplerTree 通过 子树和提供）。构建电路的成本由此得出，因为执行一次更新时，我们需要修改对应于相关叶到根路径的量子门。

□

推论 4. 令 $x \in \mathbb{R}^m_{\geq 0}$ 对应于一个SamplerTree实例，且令 $\beta \geq \|x\|_1$，并假设$\mathbf{A} \in \mathbb{R}^{m\times n}$ 具有 $\|\mathbf{A}\|_{\max} \leq 1$。我们可以维护一个量子预言机 $\mathcal{O}_{\mathbf{A}^\top x}$，其调用耗时为 $O(\log m)$，在执行 T 次更新操作后的总构建成本为 $O(T \log m)$，使得对任意 $j \in [n]$,

$$\mathcal{O}_{\mathbf{A}^\top x}|0\rangle^{\otimes(a+2)}|j\rangle = |0\rangle\left(\sum_{i\in[m]}\sqrt{\frac{\mathbf{A}_{ij}x_i}{\beta}}|0\rangle|i\rangle + |1\rangle|g\rangle\right)|j\rangle.$$

证明。 我们将 $\mathcal{O}$ ′一个(见第 2节)应用于 $\mathcal{O}_{\mathsf{SamplerTree}}$的输出，并忽略额外的量子比特。 □

这里我们指出，推论 4 中的额外量子比特很快就会在构造 $\mathbf{diag}\left(\mathbf{A}^\top x\right)$的适当缩放版本的块编码时派上用场。

多项式近似。 为了为算法 1 所遇到的各类动态向量提供近似吉布斯采样器，我们还需要用到多项式逼近理论中的一些工具。我们首先陈述一个辅助结果，用于对指数函数进行有界近似；其变体也曾用于 [vAG19]。证明见附录 C。

引理 8 (引理 7, [vAG19])。 设 $\beta \geq 1, \xi \leq \frac{1}{10}$。存在一个多项式 $\mathcal{P}_{\beta,\xi}$，其次数为 $O(\beta \log \frac{1}{\xi})$，使得 $\max_{x\in[-1,1]} |\mathcal{P}_{\beta,\xi}(x)| \leq 3$ 且 $\max_{x\in[-1,0]} |\mathcal{P}_{\beta,\xi}(x) - \exp(\beta x)| \leq \xi$。

接下来，我们陈述引理 8 的另一个推论，以供我们的拒绝采样器使用。

推论 5。 令 $B, \delta \geq 0$，并假设 $v \in \mathbb{R}^n$ 满足 $\|v\|_\infty \leq B$。此外，假设对于某个 $c \geq 0$，$-c \leq \max_{j\in[n]} v_j \leq 0$。令 $q \in \mathbb{R}^n_{\geq 0}$ 满足 $q_j \in [\ell, 1]$ （逐元素）。最后，定义 $u_j := \frac{v_j}{2B}$ （逐元素）。存在一个次数为 Δ 的多项式 $\mathcal{P}$，对于 $\Delta = O(B \cdot (c + \log\frac{n}{\ell\delta}))$，使得对于 $w_j := \mathcal{P}(u_j)^2 q_j$，且 $z_j := \exp(2Bu_j)q_j$ （逐元素），

$$\left\| \frac{w}{\|w\|_1} - \frac{z}{\|z\|_1} \right\|_1 \leq \delta. \tag{14}$$

此外，$\max_{x\in[-1,1]} |\mathcal{P}(x)| \leq \frac{1}{2}$，且 $\|w\|_1 \geq \frac{1-\delta}{36}\|z\|_1$。

证明。 假设 $\delta \le 2$否则该命题显然成立。首先， $u_j \in [-\frac{1}{2}, 0]$根据给定假设逐元素成立（因为 $v_j \in [-B, 0]$ 逐元素）。令 $\mathcal{P}_{\beta,\ \xi}(\cdot)$ 为引理 8 给出的多项式，ξ-逼近 $\exp(\beta\cdot)$于 $[-\frac{1}{2}, 0]$上。我们定义

$$\mathcal{P}(u) := \frac{1}{6}\mathcal{P}_{B,\xi}(u)\,, \text{ for } \xi := \frac{\delta\ell}{6n\exp(c)}.$$

根据引理 8，立即可得该多项式的次数界和绝对值界，因此还需证明距离界。引理 8 的保证进而意味着，对所有 $j \in [n]$,

$$|6\mathcal{P}(u_j) - \exp(Bu_j)| \le \xi. \tag{15}$$

我们还得到 $u_j \le 0$，因此 $\exp(Bu_j) \le 1$。因此，我们还得到

$$|6\mathcal{P}(u_j) + \exp(Bu_j)| \le 2 + \xi \le 3.$$

综合可得，对所有 $j \in [n]$,

$$\left|36\mathcal{P}(u_j)^2 - \exp(2Bu_j)\right| \le 3\xi. \tag{16}$$

接下来，令 $y_j := 36w_j$ 对所有 $j \in [n]$，并注意到$\frac{y}{\|y\|_1} = \frac{w}{\|w\|_1}$。我们给出其上界

$$\begin{aligned}\left\|\frac{w}{\|w\|_1} - \frac{z}{\|z\|_1}\right\|_1 &= \sum_{j\in[n]}\left|\frac{y_j}{\|y\|_1} - \frac{z_j}{\|z\|_1}\right| \le \sum_{j\in[n]}\left|\frac{y_j}{\|y\|_1} - \frac{y_j}{\|z\|_1}\right| + \sum_{j\in[n]}\left|\frac{y_j}{\|z\|_1} - \frac{z_j}{\|z\|_1}\right| \\ &\le \left|1 - \frac{\|y\|_1}{\|z\|_1}\right| + \frac{\|y-z\|_1}{\|z\|_1} \le \frac{2\,\|y-z\|_1}{\|z\|_1}.\end{aligned} \tag{17}$$

利用 y、z 的定义以及（16），并结合 q 的假定取值范围，

$$\|y - z\|_1 \le 3n\xi,\ \|z\|_1 \ge \ell\exp(-c).$$

第二个不等式用到了根据假设，某个 $v_j = 2Bu_j$ 至少为 $-c$。结合上面的推导式、（17）以及 ξ 的定义，即可完成（14）的证明。最后，利用上文给出的$\|y-z\|_1$ 和 $\|z\|_1$ 的界可得

$$\|w\|_1 = \frac{1}{36}\|y\|_1 \ge \frac{1-\delta}{36}\|z\|_1.$$

□

块编码。 我们的近似吉布斯预言机采用了由[GSLW19] 首创的实现策略，称为“块编码”。具体而言，我们沿用 [GSLW19] 的说法，将 $\mathbf{U}$定义为一个 $(a+\ell)$- 量子比特量子门；若 ℓ-比特块编码的$\mathbf{M}$是 $2^a \times 2^a$ $\mathbf{U}$ 的左上角子矩阵$\mathbf{M}$。块编码矩阵支持高效的可组合操作，例如应用线性组合和有界多项式。我们在下文总结这些性质。

命题 5 （引理 52, [GSLW19]）。 设 $\mathbf{U}_1$ 和 $\mathbf{U}_2$ 是同尺寸矩阵$\mathbf{M}_1, \mathbf{M}_2$ 的 ℓ-比特块编码。存在一个 $O(\ell)$-比特块编码$_{1\,2}\mathbf{M}_1 + \frac{1}{2}\mathbf{M}_2$，其应用所需的渐近时间与应用$\mathbf{U}_1$ 和 $\mathbf{U}_2$相同。

命题 *6*（定理 56, [*GSLW19*]）。设 U 是 M 的一个 ℓ 位块编码，且 $\mathcal{P}: [-1,1] \to [-\frac{1}{2}, \frac{1}{2}]$ 是一个次数为 Δ 的多项式。存在一个 $O(\ell)$ 位块编码 $\mathcal{P}(M)$，可通过对 U 和 $U^\dagger$ 进行 $O(\Delta)$ 次调用并额外花费 $O(\ell\Delta)$ 时间来应用。

我们还证明，应用推论 4 可得到一个简单的块编码$\mathbf{diag}\left(\frac{\mathbf{A}^\top x}{\beta}\right)$。类似的构造此前已见于[vAG19]。

推论*6.* 令 $x \in \mathbb{R}^m_{\geq 0}$ 对应于 *SamplerTree* 的一个实例，并且 $\beta \geq \|x\|_1$。令 $M := \mathit{diag}\left(\frac{\mathbf{A}^\top x}{\beta}\right)$，$U := \mathcal{O}^* A^\top x (\mathit{SWAP}_{12} \otimes I) \mathcal{O}_{\mathbf{A}^\top x}$，其中 SWAP_{12} 交换前两个量子比特，且$\mathcal{O}_{\mathbf{A}^\top x}$ 来自推论 *4*。则 U 是 M 的块编码，其应用时间为 $O(\log m)$；在调用 *Update* T 次后，总构建成本为 $O(T \log m)$。

证明。 为方便起见，~~定义~~ $w_{ij} := \mathbf{A}_\beta^{ij x_i}$。根据 $\mathcal{O}_{\mathbf{A}^\top x}$ 的定义，我们有

$$(\mathrm{SWAP}_{12} \otimes \mathbf{I})\, \mathcal{O}_{\mathbf{A}^\top x} \left(|0\rangle^{\otimes(a+2)} |j\rangle \right) = \left(|00\rangle \sum_{i \in [m]} \sqrt{w_{ij}} |i\rangle + |10\rangle |g\rangle \right) |j\rangle.$$

因此，对于 $j, j' \in [n]$，我们计算 $\langle j' | \langle 0|^{\otimes(a+2)} \mathrm{U} |0\rangle^{\otimes(a+2)} |j\rangle$ 如下：

$$\langle j' | \left(|00\rangle \sum_{i \in [m]} \sqrt{w_{ij}} |i\rangle + |01\rangle |g\rangle \right)^* \left(|00\rangle \sum_{i \in [m]} \sqrt{w_{ij}} |i\rangle + |10\rangle |g\rangle \right) |j\rangle$$
$$= \begin{cases} \sum_{i \in [m]} w_{ij} = \frac{[\mathbf{A}^\top x]_j}{\beta} & j = j' \\ 0 & j \neq j' \end{cases}.$$

特别地， $|01\rangle$ 和 $|10\rangle$ 项消失，并且除非 $j = j'$，否则 $|j\rangle, |j'\rangle$ 彼此正交。上文要求 $\sqrt{w_{ij}}^* \sqrt{w_{ij}} = w_{ij}$，而这仅当 w_{ij} 非负时才成立。为绕过这个问题，我们将以略有不同的方式实现 $\mathcal{O}_{\mathbf{A}^\top x}$ 的两个副本，从而得到正确的符号。为使记号清晰，我们令 $\mathcal{O}^L$ 表示左侧经过共轭的预言机， $\mathcal{O}^R$表示右侧的预言机，使得 $\mathrm{U} = (\mathcal{O}^L)^*(\mathrm{SWAP}_{12} \otimes \mathrm{I})(\mathcal{O}^R)$。注意， x 逐元素非负且 $\beta > 0$，因此决定 w_{ij} 符号的唯一因子是 A_{ij}。当 $\mathrm{A}_{ij} \geq 0$时，我们将以一致的方式定义用于加载 $\sqrt{\mathrm{A}_{ij}}$ 的预言机 $\mathcal{O}'_{\mathbf{A}}$，分别对应 $\mathcal{O}^L$ 和 $\mathcal{O}^R$ （即使用符号相同的~~平~~方根），从而使得 $\sqrt{w_{ij}}^2 = w_{ij}$。当 $\mathrm{A}_{ij} < 0$ 时，我们将以不一致的方式定义它们，使得经过共轭操作后，$-\sqrt{w_{ij}}\sqrt{w_{ij}} = w_{ij}$。由此我们证明了 $\langle 0|^{\otimes(a+2)} \mathrm{U} |0\rangle^{\otimes(a+2)} = \mathrm{M}$，这就得出了第一个结论。要证明第二个结论，注意所有量子门都是可逆的（算术电路是可逆的，并且 $\mathcal{O}_{\mathbf{A}}$ 是其自身的逆），因此应用 $\mathcal{O}^*{}_{\mathbf{A}^\top x}$ 的复杂性与 $\mathcal{O}_{\mathbf{A}^\top x}$相同。 □

最后，我们将各部分组合起来，证明命题 2；本文将反复使用该命题来实现我们的吉布斯采样预言机。

命题 *2*。设 $x \in \mathbb{R}^m_{\geq 0}$ 对应于 *SamplerTree* 的一个实例，且 $\beta \geq \|x\|_1$。设 p 为与 $A^\top x$相关联的吉布斯分布，令 $Z := \sum_{j \in [n]} \mathit{exp}([A^\top x]_j)$，并且对于某个 $C \geq 1$，有 $\widetilde{Z} \in [Z, CZ]$。最后，设 $q \in \mathbb{R}^n$ 的各项可在 $O(1)$ 时间内经典查询，满足 $q \geq p$逐元素成立、对所有 $j \in [n]$均有 $q_j \in [\frac{\delta}{n}, 1]$，且 $\|q\|_1 = \rho$。假设 $\widetilde{Z}$、 C、 ρ和 β均已明确给定。给定 A 的量子预言机 $\in \mathbb{R}^{m \times n}$ （定义见第 *2* 节），其中 $\|A\|_{\max} \leq 1$，我们可以实现一个 δ-近似吉布斯预言机，其查询成本为 $O(\sqrt{\rho C} \cdot \beta \log^4(\frac{Cmn}{\delta}))$。如果 x 执行了 T 次更新调用，并且这些调用保持关于 Z、 C、 ρ、 β的不变量，则产生的总额外成本为 $\widetilde{O}(T \log m)$。

证明。 在整个证明过程中，令 $\delta \leftarrow \min(1_2, \delta)$以及 $B := 4(\beta + \log(\frac{Cn}{\delta}))$。另定义 $\ell := \frac{\delta}{n}$ (沿用推论 5中的记号）。首先注意到，由于 $\max_{j \in [n]} [\mathbf{A}^\top x]_j \leq \log Z \leq$

$\max_{j\in[n]}[\mathrm{A}^\top x]_j + \log n$,

$$-\log(Cn) \le \max_{j\in[n]}[\mathbf{A}^\top x]_j - \log\left(\widetilde{Z}q_j\right) \le 0.$$

此处使用的上界是：根据假设，对于所有 $j \in [n]$，$\exp([\mathrm{A}^\top x]_j - \widetilde{Z}q_j) = \frac{p_j}{q_j}\cdot\frac{Z}{\widetilde{Z}} \le 1$。因此，对于 $v := \mathrm{A}^\top x -$ 逐元素满足 $\log(\widetilde{Z}q)$，

$$-c \le \max_{j\in[n]} v_j \le 0 \text{ for } c := \log(Cn).$$

接下来注意，$\log(\widetilde{Z}q)$ 的逐元素绝对值有界于 $\frac{B}{2}$：

$$\log(\widetilde{Z}q_j) \le \log(CZ) \le \log\left(n\cdot\max_{j\in[n]}\exp([\mathbf{A}^\top x]_j)\right) + \log C \le \frac{B}{2},$$
$$\log(\widetilde{Z}q_j) \ge \log Z + \log\frac{\delta}{n} \ge \min_{j\in[n]}[\mathbf{A}^\top x]_j - \log\frac{n}{\delta} \ge -\frac{B}{2}.$$

定义 $\mathrm{M}_1 := \mathrm{diag}\left(\frac{\mathbf{A}^\top x}{2B}\right)$，以及 $\mathrm{M}_2 := \mathrm{diag}\left(-\frac{1}{2B}\log(\widetilde{Z}q)\right)$。根据上述计算，我们有$\|\mathrm{M}_2\|_{\mathrm{op}} \le \frac{1}{2}$；类似地，显然 $\|\mathrm{M}_1\|_{\mathrm{op}} \le \frac{1}{2}$，因为 $\left\|\mathrm{A}^\top x\right\|_\infty \le \beta$。此外，利用推论6并取 $\beta \leftarrow B$，我们得到 U_1，它是 M_1 的一个块编码，可在 $O(\log m)$ 时间内应用。~采用与推论6类似的构造，由于 q、B 和 Z 均可高效经典查询，我们得到 U_2，它是 M_2 的一个块编码，可在 $O(1)$ 时间内应用。因此，命题 5 给出 U，即一个块编码

$$\mathbf{M}_1 + \mathbf{M}_2 = \mathbf{diag}\left(\frac{v}{2B}\right),$$

它可以在 $O(\log mn)$ 时间内应用。接下来，令 $\mathcal{P}$ 为推论 5 中的次数为-$\Delta = O(B\log\frac{Cn}{\delta})$ 多项式，其参数为 B, v, c, q, ℓ，定义如前。推论 5 表明 $\mathcal{P}$:$[-1,1] \to [-\frac{1}{2},\frac{1}{2}]$。因此，命题 6 得出 U′，它是 $\mathrm{diag}\left(\mathcal{P}(\frac{v}{2B})\right)$ 的一个块编码，可以在 $O(\Delta\cdot\log mn)$ 时间内应用。此外，由于 q 和 ρ 均可高效地进行经典查询，我们可以定义量子门 $\mathcal{O}_q$，它可在 $O(1)$ 时间内应用，且其作用为

$$\mathcal{O}_q|0\rangle^{\otimes(b+1)} = |0\rangle\sum_{j\in[n]}\sqrt{\frac{q_j}{\rho}}|j\rangle + |1\rangle|g\rangle.$$

将 U′ 作用于 $\mathcal{O}_q$ 的输出，并使用适当的辅助量子比特，即可得到

$$|0\rangle^{\otimes O(1)}\sum_{j\in[n]}\sqrt{\frac{q_j\mathcal{P}(u_j)^2}{\rho}}|j\rangle|g_j\rangle + |g'\rangle, \text{ where } u_j := \frac{v_j}{2B} \text{ for all } j\in[n].$$

对第一寄存器进行后选择，使其处于全零态，并测量与 j 对应的寄存器，可知我们以正比于 $q_j\mathcal{P}(u_j)^2$ 的概率获得样本 $j \in [n]$。根据推论 5，在样本成功的条件下，所得分布与正比于 $q\circ\exp(v) \propto \exp(\mathrm{A}^\top x)$ 的分布之间的 δ-距离为 ℓ_1，因此结果是一个 δ-近似吉布斯预言机。最后，我们界定该预言机的查询成本。按照推论 5 中的定义，令 $w_j := \mathcal{P}(u_j)^2 q_j$，且 $z_j := \exp(v_j)q_j$~。根据 v、Z 的定义，

$$\|z\|_1 = \sum_{j\in[n]}\frac{\exp\left(\left[\mathbf{A}^\top x\right]_j\right)}{\widetilde{Z}} \in \left[C^{-1},1\right].$$

此外，推论 5 中的最后一个结论 $\|w\|_1 \geq \frac{1}{72}\|z\|_1 \geq (72C)^{-1}$。因此，

$$\sum_{j\in[n]} \frac{q_j \mathcal{P}(u_j)^2}{\rho} = \frac{\|w\|_1}{\rho} \geq \frac{1}{72C\rho}.$$

换言之，我们有一个预言机，其运行时间为 $O(\Delta \cdot \log mn)$，它以概率 $\alpha \geq \frac{1}{72C\rho}$正确返回一个样本。通过应用命题 4 来提高成功概率，我们可以得到所需结论，额外开销为 $O(\sqrt{C\rho}\log\frac{1}{\delta})$。

□

推论 2。沿用命题 2的记号，设 $R := \frac{Z}{Z}$。存在一个量子预言机 $\mathcal{O}_{\text{test}}$，可在 T 更新 次 x 调用下，于 $O(T\log m)$ 时间内实现，其查询成本为

$$O\left(\sqrt{\rho C}\cdot\beta\log^4\left(\frac{Cmn}{\ell\delta}\right)\right).$$

此外，对于显式已知常数 C_ℓ 和 C_u，$\mathcal{O}_{\text{test}}$ 以概率 p 返回“成功”，其中

$$\frac{C_\ell}{\sqrt{R\rho}} \leq p \leq \frac{C_u}{\sqrt{R\rho}}.$$

证明。我们的预言机 $\mathcal{O}_{\text{test}}$ 是命题 2中的预言机，只是我们会选取足够小的常数 δ。当样本经过振幅放大后被拒绝采样器接受时，它就返回“成功”。振幅放大前，命题 2给出的成功概率为 $\Theta(\frac{1}{R\rho})$，其中上下界中的常数都是显式的。此外，命题 4 中的常数也是显式的，因此，通过振幅放大可将成功概率提高至 $\Theta(\frac{1}{\sqrt{R\rho}})$，且其常数界已知，满足推论陈述的要求。

□

C 在 $[-1,1]$ 上对 exp 的有界逼近

此处，我们给出先前工作中用到的一个引理的证明（常数略有不同）[vAG19]。本节完全基于 [GSLW19] 中关于多项式近似的先前结果；为求完整起见，我们将其纳入本文，因为 [vAG19] 中并未给出证明。提醒一下，在附录 B 中构造拒绝采样器时，我们曾陈述并使用以下结果。

引理 8 (引理 7, [vAG19])。设 $\beta \geq 1$, $\xi \leq \frac{1}{10}$。存在一个次数为 $O(\beta\log\frac{1}{\xi})$ 的多项式 $\mathcal{P}_{\beta,\xi}$，使得 $\max_{x\in[-1,1]}|\mathcal{P}_{\beta,\xi}(x)| \leq 3$ 且 $\max_{x\in[-1,0]}|\mathcal{P}_{\beta,\xi}(x) - \exp(\beta x)| \leq \xi$。

为得到该引理，我们将利用 [GSLW19] 中的以下结果。

命题 7（推论 66, [GSLW19]）。设 $x_0 \in [-1,1]$, $r \in (0,2]$, $\delta \in (0,r]$。令 f: $[x_0 - r - \delta, x_0 + r + \delta] \to \mathbb{C}$ 满足：对所有 $x \in [-r-\delta, r+\delta]$，$f(x_0+x) = \sum_{\ell\geq 0} a_\ell x^\ell$。假设 $B > 0$ 满足 $\sum_{\ell\geq 0}(r+\delta)^\ell |a_\ell| \leq B$，并令 $\epsilon \in (0, \frac{1}{2B}]$。存在一个次数为 $O\left(\frac{1}{\delta}\log\frac{B}{\epsilon}\right)$ 的多项式 P（其数值稳定的实现见附录 D），使得

$$\max_{x\in[x_0-r,x_0+r]} |f(x) - P(x)| \leq \epsilon \text{ and } \max_{x\in[-1,1]} |P(x)| \leq \epsilon + B.$$

引理的证明 8. 我们应用命题 7，其中 $f(x) := \exp(\beta x)$ 它处处都有收敛的泰勒级数，并采用参数设置 $x_0 = -1$, $r = 1$, $\delta = \frac{1}{\beta}$, $B = e$. 我们有

$f(x_0+x) = \sum_{\ell\geq 0} \exp(-\beta)\frac{\beta^\ell \cdot x^\ell}{\ell!} = \sum_{\ell\geq 0} a_\ell x^\ell$ 其中 $a_\ell = \exp(-\beta)\frac{\beta^\ell}{\ell!}$ 对于任意整数 $\ell \geq 0$。我们还通过以下方式验证所选的 B 是有效的：

$$\sum_{\ell\geq 0}(r+\delta)^\ell |a_\ell| = \exp(-\beta)\sum_{\ell\geq 0}\left(1+\frac{1}{\beta}\right)^\ell \frac{\beta^\ell}{\ell!} = \exp(-\beta)\sum_{\ell\geq 0}\frac{(\beta+1)^\ell}{\ell!} = \exp(\beta+1-\beta) = e.$$

因此，根据命题7，对于任意$\xi \leq \frac{1}{2e}$，存在一个次数为 P的多项式 $O(\beta \log \frac{1}{\xi})$，使得$\max_{x\in[-2,0]} |\exp(\beta x) - P(x)| \leq \epsilon$，且$\max_{x\in[-1,1]} |\tilde{P}(x)| \leq e + \frac{1}{6} + \xi \leq 3$。 □

D 多项式近似的数值稳定实现

在本节中，令 $\Delta = O(\frac{1}{\epsilon}\log^2(\frac{mn}{\epsilon}))$为附录2 B 中命题2的证明中所用多项式的次数（具体而言，该多项式构造于命题2的证明中；在我们的应用中，有 $C = O(1)$ 和 $\delta = O(\epsilon)$）。我们使用的多项式是通过傅里叶基分解构造的（见引理57和 65, [GSLW19]）。在 [GSLW19], 的量子奇异值变换框架内，无法直接看出这种多项式变换能否通过有限精度算术稳定实现；该框架用于命题2的证明。不过， [Haa19] 指出，给定这样的傅里叶基分解，我们可以将所需的多项式变换构造成量子电路，并以数值稳定的方式实现，使加性误差不超过 ξ，且运行时间为

$$O\left(\Delta^3 \log\left(\frac{\Delta}{\xi}\right)\right).$$

在我们的设定中（在命题 2 的证明中），很容易验证 $\xi =$ 多项式$(m,\ n,\ \epsilon^{-1})$。这一构造产生了定理 4 中的加性项。