arXiv:2601.07074v1 [stat.ML] 11 Jan 2026

量化下的稳健均值估计

Pedro Abdalla* Junren Chen†

2026年1月13日

摘要

我们研究量化和对抗性污染下的均值估计问题。我们在两种不同的设置下构造了在对数因子范围内达到最优的多变量鲁棒估计量。第一种是单比特设置，其中每个比特仅取决于单个样本；第二种是部分量化设置，在该设置中，估计量可以使用一小部分未量化数据。

1 引言

量化条件下的参数估计是统计学 [12], 信号处理 [14], 和机器学习 [4]交叉领域中的一个基础问题。量化在这些领域至关重要，主要因为它能够降低内存和存储成本。

在分布式学习中，量化对于降低数据服务器之间的通信成本发挥着关键作用；中央服务器需要根据数据服务器发送的量化数据估计参数。正如 [17], 所指出的，量化也有助于推动近期兴起的数据隐私范式，因为量化样本能够保留敏感信息：估计量只能访问比特，从而降低了敏感信息泄露的可能性。

在这项工作中，我们考虑一个或许最基础的参数估计任务：根据 n 个随机向量 X的独立同分布副本 X_1，……， X_n，估计其 X的均值。我们的目标是利用 量化样本 X_1，…… X_n来估计均值，并尽可能使用最少的比特。按照 [17], 中的术语，我们将对文献中出现的不同设定作一个重要区分：

- 集中式：这些比特可以访问整个样本，即. X_1 (X_1、……、 X_n)……、 X_n(X_1、……、 X_n)。

*加州大学尔湾分校数学系。
†马里兰大学数学系，学院公园校区。

- 自适应：每个比特都是实际样本和先前比特的函数，即对于每个 $j \in [n]$， $X_j(X_j$， X_1，……， $X_{j-1})$。.
- 分布式：每一位 X_j 仅取决于样本 X_j，即 $\dot{X}_1(X_1) \ldots, \dot{X}_n(X_n)$ [1]。

需要指出的是，集中式设置的限制最少。事实上，在这种设置下，算法可以先处理未量化数据，然后再对均值估计器的输出进行量化。因此，与其他设置相比，这个问题要容易得多。另一方面，分布式设置的限制最多，因为样本会被直接量化，而无需了解其他样本的任何信息。我们的工作聚焦于分布式设置，但也可能与自适应和集中式设置相关。

我们的首要贡献是构造了在极小极大意义下针对量化数据的（近似）最优均值估计器。具体而言，我们证明，该估计器可以轻松扩展到高维设置，而目前文献中尚无这方面的结果。

秉承稳健统计这一活跃领域的研究思路 [1,10,22], ，我们还证明了我们的估计量能够抵御对抗噪声，这意味着即使少量数据遭到篡改，它仍能保持准确。据我们所知，我们的工作首次研究了量化条件下这一具有实际意义的稳健均值估计器问题。

我们的第二项主要贡献是提出一种（稍微）宽松一些的设置，允许算法使用少量未经量化的数据。这种设置称为“部分量化设置”，其主要优点是避免依赖均值位置，同时使用的比特数几乎相同。我们按照难度递增的顺序，在第 3 节和 4节报告结果；关于最完整形式（含对抗性污染的多变量情形）的正式陈述，请参阅定理 3.1和 4.5 。

相关工作

文献 [6,26,27] 研究了无偏估计量的确定性量化映射设计，重点关注其在费希尔信息和克拉美-罗下界意义下的最优性。然而，该文并未给出均值估计量的样本复杂度界。我们的方法则显著不同：量化映射是随机的，且只有（可忽略的）偏差，因此避免了克拉美-罗理论中的不可能性结果。截尾均值 [22] 或均值中位数 [20] 等估计量的偏差虽可忽略，但其收敛率往往快于最优无偏估计量。

[1]文献中一些关于集中式设置的研究，由于采用了分布式学习这一术语，将该问题称为分布式设置下的均值估计。

Cai 和 Wei [4,5] 为集中式设置构造了极小极大最优估计量。他们的构造也适用于多变量情形。另一方面，这些估计量仅适用于均值向量 μ的所有分量均有界于 1 的情形，且要求 X服从高斯分布。此外，他们的方法严重依赖于这样一个事实：在集中式设置中，可以先计算均值的估计量，再对该估计量的输出进行量化；这种方法既不适用于自适应设置，也不适用于分布式设置。值得指出的是，他们的方法对比特翻转非常敏感，也就是说，一旦有一个比特出错，整个过程就会彻底失效。

Kipnis 和 Duchi [17] 在数据为已知密度的对数凹分布这一假设下，证明了一维自适应设置中标准均方误差（MSE）的精确渐近结果。Kumar 和 Vat- edka [18]通过放宽对方差已知的要求，改进了 Kipnis 和 Duchi 针对自适应设置得出的结果。最近，在均值有界的条件下，Lau 和 Scarlett [19] 推导出了自适应设置下近乎最优的非渐近估计。由于对比特翻转敏感，这些方法似乎都不适用于处理对抗性污染。

Kipnis 和 Duchi 还在关于估计量构造的一些技术性假设下，给出了分布式设置中极小极大 MSE 的渐近下界。作者声称，分布式设置下任何均值估计器的收敛速率都必须取决于均值位置。Lau 和 Scarlett 最近给出的下界也得出了相同结论。我们给出一个简单的论证来证明这一事实。

Suresh、Sun、Ro 和 Yu [24]为分布式设置构造了一种量化方案，但该方案仅提供期望意义下的保证，且依赖于经验绝对偏差，而其控制方式尚不明确。他们的方法与我们的方法一样，依赖于随机量化，但其构造要求数据有界，且仅适用于一维设置。

以下结果与我们的目标有一定关联，但并不重合。Amiraz、Krauthgamer 和 Nadler [3]研究了在假设 μ为具有已知 K的 K-稀疏情形下，对 μ的支撑集进行估计的问题。Acharya、Canonne、Liu、Sun 和 Tyagi 研究了量化条件下的密度估计 [2]问题，但仅限于离散概率分布。

组织结构

本文其余部分安排如下。在第2节中，我们介绍稳健统计和抖动的相关背景知识，这些知识将用于构造我们的估计量。在第3节中，我们针对无噪声情形和存在对抗性污染的情形，推导分布式设置下的主要结果。在第4节中，我们描述部分量化设置，并推导主要

结果。在第5节中，我们通过数值实验验证我们的理论。

2 背景

本节将从数学角度描述量化约束下的均值估计问题及其必要背景。给定由 n 个独立同分布副本 X_1、……、X_n 组成的随机向量X样本，我们的目标是设计一种量化方案，将样本映射为比特 $\dot{X}_1(X_1)$……、$\dot{X}_n(X_n) \in \{0, 1\}^d$，并构造一个估计量 $\hat{\mu}(\dot{X}_1$、……、$\dot{X}_n)$ 来估计 X的均值，我们将其记为 $\mu := \mathbb{E}X$。

2.1 稳健统计与抖动背景

我们的核心思路是建立一种新颖的联系：将稳健统计文献中的截尾均值估计量[22] 与信号处理文献中的（随机）抖动技术 [13, 25, 29]联系起来。

我们首先介绍截尾均值估计量的基础知识。为简化起见，暂且假设 X 是一个均值为 μ、方差为 σ^2的一维随机变量。关于多变量情形的扩展将在下一节讨论。

简而言之，截尾均值估计量会剔除绝对值过大的样本，并对剩余样本取平均。也就是说，对于一些选取恰当的参数 α 和 β，我们定义

$$\phi_{\alpha,\beta}(x) := \begin{cases} \beta, & \text{if } x > \beta \\ x, & \text{if } x \in [\alpha, \beta] \\ \alpha, & \text{if } x < \alpha, \end{cases} \tag{2.1}$$

并计算

$$\frac{1}{n}\sum_{i=1}^{n} \phi_{\alpha,\beta}(X_i).$$

为了说明如何选取 α 和 β，我们需要回顾分位数的概念。为此，我们将 X 的第 p分位数定义为

$$Q_p(X) := \sup\{a \in \mathbb{R} : \mathbb{P}(X \geq a) \geq 1 - p\}. \tag{2.2}$$

理想情况下，我们希望针对某个足够小的 ε 选取 $\alpha = Q_\varepsilon(X)$ 和 $\beta = Q_{1-\varepsilon}(X)$，以确保

$$\mathbb{P}(X \notin [\alpha, \beta]) = O(\sigma n^{-1/2}),$$

其中，右侧是（未量化）均值估计问题的极小极大收敛速率。这意味着截断函数引入的偏差可以忽略不计。

显然，我们并不知道总体分位数。一种自然的做法是用经验对应量替代，也就是说，我们考虑数据 $X_1^* \leq \cdots \leq X_N^*$ 的非递减重排，并选择 $\alpha = X_\varepsilon^*$ 和 $\beta = X_{1-\varepsilon}^*$。直观而言，它们应分别接近 $Q_\varepsilon(X)$ 和 $Q_{1-\varepsilon}(X)$。关于这一选择精度的技术细节，我们留待下一节讨论。

抖动技术源自单比特估计问题中的信号处理文献（例如参见 [7,8,11–13,25]）。其基于以下思路：对于任意有界的（可能是确定性的） x $|x| \leq \lambda$，我们抽取一个在区间 τ 上均匀分布的随机变量 $[-1,1]$，即 $\tau \sim \mathscr{U}[-1,1]$。接下来，利用以下公式：

$$\mathbb{E}\big[\lambda \mathrm{sign}(x+\lambda\tau)\big] = x.$$

选择 τ 可确保 λsign$(x+\lambda\tau)$ 是 x 的无偏估计量。我们采用一种略有不同的策略。受稳健统计文献的启发，我们考虑抖动可能存在（可忽略的）偏差的情形。事实上，注意，对于任意 $x \in \mathbb{R}$ （不一定有界）以及 $\lambda > 0$，对于随机变量 $\tau \sim \mathscr{U}[-1,1]$，有

$$\begin{aligned}
&\mathbb{E}\Big[\lambda \mathrm{sign}(x+\lambda\tau)\Big] \\
&= \lambda \mathbb{1}(x > \lambda) - \lambda \mathbb{1}(x < -\lambda) + \mathbb{1}(|x| < \lambda)\Big[\lambda \mathbb{P}(\tau > -x) - \lambda \mathbb{P}(\tau < -x)\Big] \\
&= \begin{cases} \lambda, & \text{if } x > \lambda \\ x, & \text{if } |x| \leq \lambda \\ -\lambda, & \text{if } x < -\lambda, \end{cases}
\end{aligned}$$

其中右侧恰好是截尾函数，因此

$$\mathbb{E}\Big[\lambda \mathrm{sign}(x+\lambda\tau)\Big] = \phi_{-\lambda,\lambda}(x). \tag{2.3}$$

恒等式（2.3）实际上表明，有偏抖动方案可能有助于截除离群值。这种联系是我们证明中的一个基本组成部分。

最后，我们介绍可追溯至 Huber [16]研究工作的对抗噪声标准概念；如今，统计学和机器学习文献普遍采用这一概念，例如用于均值估计或协方差估计 [1,22]。对抗噪声背后的思想是将其作为定量基准，用于研究估计量应对不完美数据时的稳定性，这与实际应用密切相关。

数学描述相对简单：我们观察到数据在 ηn 个样本被任意篡改后的情况。本文将区分两种对抗噪声。

当对手将样本 $\widetilde{\quad}$ $\widetilde{\quad}$ 个 $X_1, \cdots X_n$ 修改为污染样本 $X_1, \cdots X_n$，且满足以下条件时，我们称之为量化前噪声：

$$\left|\{i \in [n] : \widetilde{X}_i \neq X_i\}\right| \leq \eta n. \tag{2.4}$$

噪声会影响我们应用量化过程之前收集的样本。类似地，当对抗性污染在应用量化映射之后影响样本时，我们称之为量化后噪声，$\sim$ $\sim$ $\dot{}$ $\dot{}$ 也就是说，量化映射输出 $X_1, \cdots X_n$，满足

$$\left|\{i \in [n] : \widetilde{\dot{X}}_i \neq \dot{X}_i\}\right| \leq \eta n. \tag{2.5}$$

3 分布式设置中的均值估计

本节将推导分布式设置下均值估计的主要结果。不过，我们认为这些结果对于集中式或自适应设置仍然具有参考意义，尤其是考虑到我们的估计量所具备的鲁棒性。

首先，我们对分布式设置作一项重要观察。除非对 X的分布作出额外假设，否则估计量 $\hat{\mu}$只是比特的函数，除此之外不依赖任何信息。因此，只有 2^n 种可能的输入来以任意高的精度近似任意实数值。基于此，我们需要对数据有一些额外了解，才能构造估计量。稍后我们将说明，这种假设在一定程度上不可避免。我们首先关注单变量情形。

3.1 一维情形

对于一维情形，我们假设已知分位数的一个（粗略）上界估计 λ。更准确地说，令 $X := X - \mathbb{E}X$，给定置信水平 $\delta > 0$，我们假设

$$\lambda \geq \max\left\{Q_{1-\varepsilon}(X), -Q_{\varepsilon}(X)\right\}, \tag{3.1}$$

其中 $\varepsilon \asymp \log(1/\delta)/n$。 [2] 显然， ε必须小于 1，因此在本文余下部分中，我们假设处于 $n = \Omega(\log(1/\delta))$这一范围内。这不失一般性；否则 $\log(1/\delta)/n$ 与零相距甚远，因此对于任意估计量 $|\hat{\mu} - \mu|$，误差界 $\hat{\mu}$也与零相距甚远。

对 λ 的上界要求可以理解为对 X 的大部分概率质量集中位置的粗略估计。事实上，落在区间 $[Q_{\varepsilon}(X)\ Q_{1-\varepsilon}(X)]$ 之外的数据与均值估计无关。

[2] 本文中，Landau（渐近）记号仅省略绝对常数。

与文献中先前的假设相比，这项对 λ 的较弱要求是一项重大优势；先前的假设要求均值有界$|\mu| \leq R$，其中某个已知的 R，且 X 的分布具有已知的对数凹密度。尤其是，我们的方法适用于离散分布，而且对 X性质的精确信息并不十分敏感。

接下来，我们描述我们的量化方案。给定 X_1、……、X_n 个均值为 μ、方差为 σ^2的独立同分布副本，我们计算量化样本

$$\dot{X}_i := \operatorname{sign}(X_i + \lambda\tau_i), \qquad 1 \leq i \leq n, \tag{3.2}$$

其中 τ_1、…… $\tau_n \sim \mathscr{U}[-1,1]$ 是独立随机变量。我们的估计量就是量化样本的经验均值，

$$\widehat{\mu}(\dot{X}_1, \cdots, \dot{X}_n) \coloneqq \frac{1}{n}\sum_{i=1}^{n} \lambda\dot{X}_i. \tag{3.3}$$

我们现在可以陈述所提出方案的第一个主要结果。

定理 3.1。存在一个绝对常数 $C > 0$，使得以下结论成立。由 $\widehat{\mu}$ 给出的估计量 (3.2) 和 (3.3) 以至少 $1-\delta$的概率满足，

$$|\widehat{\mu} - \mu| \leq C \max\{\sigma, \lambda\}\sqrt{\frac{\log(1/\delta)}{n}}.$$

此外，在存在量化前噪声 (2.4) 或量化后噪声 (2.5)的情况下，估计量以概率 $1-\delta$满足，

$$|\widehat{\mu} - \mu| \leq C \max\{\sigma, \lambda\}\sqrt{\frac{\log(1/\delta)}{n}} + 2\eta\lambda.$$

在继续证明之前，我们讨论一下结果在乘法绝对常数意义下的最优性。注意，项 $\sigma\sqrt{\log(1/\delta)/n}$即使在没有量化的情况下，也是均值估计的极小极大收敛速率 [20], ，因此该结果是最优的。在 [22], 中，作者证明了对于任何针对有界数据的均值估计过程，项 $\eta\|X\|_{L^\infty}$ 也是必需的。这表明项 $2\eta\lambda$ 在常数因子 2 的范围内是最优的。

接下来，我们讨论相对于 λ的最优性；这一点在标准均值估计问题中并不存在。注意，对于任意量化样本 $\lambda\dot{X} \in \{-\lambda, \lambda\}$，$\lambda\dot{X}$ 的方差为 $\lambda^2 - (\mathbb{E}\dot{X})^2$，只要 $\mathbb{E}\lambda X < \lambda/2$ （例如）便是 $\Omega(\lambda^2)$。因此，当 n 足够大时，如果估计量的偏差可以忽略不计，我们就必须有 $\dot{X}$ 的方差为 λ^2的量级。将标准的均值估计极小极大下界应用于独立同分布的量化样本，可知 $\lambda\sqrt{\log(1/\delta)/n}$同样是最优的。

有人可能会问，λ能有多小？不难看出，它不可能比 $Q_{1-\varepsilon}(X)$ 小太多。事实上，假设 X 的分布律已知

by

$$X \coloneqq \begin{cases} b, & \text{with prob } \varepsilon \\ a, & \text{with prob } (1-\varepsilon)/2 \\ -a, & \text{with prob } (1-\varepsilon)/2. \end{cases}$$

注意到 $Q_{1-\varepsilon}(X) = b$，因此，对于任意 $\lambda \ll b$，我们都可以得到偏差中任意大的间隔 $|\mathbb{E}\lambda X - \mu|$。因此，我们必须假设 λ 至少与 $Q_{1-\varepsilon}(X)$ 同阶。这表明，λ必须包含关于均值位置以及中心化分布的分位数的一些先验知识，因为 $Q_{1-\varepsilon}(X) = Q_{1-\varepsilon}(X) + \mu$。—

我们得出结论：在所有基于独立同分布比特的量化方案中，我们的量化方案是最优的。在不对 X 作任何先验知识假设的情况下，基于非独立同分布比特的量化方案不太可能改善这些结果。

现在我们开始证明定理3.1。

证明。回顾抖动与截尾估计量之间在（2.3）中的关系。接下来，由于 X_1、.....、X_n 相互独立且有界，伯恩斯坦不等式表明，以 $1-\delta$ 的概率，

$$\left| \frac{1}{n} \sum_{i=1}^{n} \lambda \dot{X}_i - \mathbb{E}\phi_{-\lambda,\lambda}(X) \right| \leq C\lambda \sqrt{\frac{\log(1/\delta)}{n}}. \tag{3.4}$$

剩下需要处理的只是偏差。为此，注意到

$$|\mathbb{E}\phi_{-\lambda,\lambda}(X) - \mu| \leq |\mathbb{E}(X-\lambda)\mathbb{1}_{X>\lambda}| + |\mathbb{E}(-\lambda - X)\mathbb{1}_{X<-\lambda}|.$$

我们处理右侧的第一项，第二项可以类似地处理。注意，根据柯西-施瓦茨不等式，

$$\begin{aligned} &|\mathbb{E}(X-\lambda)\mathbb{1}_{X>\lambda}| \leq |\mathbb{E}(X-\mathbb{E}X)\mathbb{1}_{X>\lambda}| + |\mathbb{E}X - \lambda|\mathbb{P}(X \geq \lambda) \\ &\leq \sigma\sqrt{\mathbb{P}(X \geq \lambda)} + |\mathbb{E}X - \lambda|\mathbb{P}(X \geq \lambda) \\ &= O\left(\sigma\sqrt{\frac{\log(1/\delta)}{n}} + |\lambda - \mu|\mathbb{P}(X - \mu \geq \lambda - \mu)\right). \end{aligned}$$

为了控制第二项 $|\lambda-\mu|\mathbb{P}(X-\mu \geq \lambda-\mu)$，我们应用切比雪夫不等式得到

$$\mathbb{P}(X - \mu \geq \lambda - \mu) \leq \frac{\sigma^2}{|\lambda-\mu|^2},$$

因此 $|\lambda-\mu| \leq \sigma/\sqrt{\mathbb{P}(X-\mu \geq \lambda-\mu)}$，或者等价地，

$$|\lambda-\mu|\mathbb{P}(X-\mu \geq \lambda-\mu) \leq \sigma\sqrt{\mathbb{P}(X-\mu \geq \lambda-\mu)}.$$

回顾 $Q_{1-\varepsilon}(X) = Q_{1-\varepsilon}(X) + \mu$，我们得到 $|\lambda - \mu| \geq Q_{1-\varepsilon}(X)$，根据（3.1），因此我们得出结论

$$|\lambda - \mu|\mathbb{P}(X - \mu \geq \lambda - \mu) \leq \sigma\sqrt{\varepsilon} = O\left(\sigma\sqrt{\frac{\log(1/\delta)}{n}}\right),$$

其中，在最后一步中我们使用了 $\varepsilon \asymp \log(1/\delta)/n$。现在我们证明鲁棒性。由于每个 X_i 仅依赖于 X_i，量化前噪声与量化后噪声等价。因此，对于任意序列 $X_1, \cdots X_n$ 满足 (2.5) 时，我们有

$$\left|\frac{1}{n}\sum_{i=1}^{n}\lambda\dot{X}_i - \frac{1}{n}\sum_{i=1}^{n}\lambda\widetilde{\dot{X}}_i\right| = \lambda\left|\frac{1}{n}\sum_{i=1}^{n}\dot{X}_i - \frac{1}{n}\sum_{i=1}^{n}\widetilde{\dot{X}}_i\right| \leq 2\eta\lambda,$$

这里我们用到了以下事实：对于任意 $i \in [n]$, $|X_i| \leq 1$。 □

3.2 多变量情形

本节中，我们将该过程扩展到多变量情形。现在，X 表示 $\mathbb{R}^d$ 中的一个随机向量，其均值为 μ，协方差矩阵为$\Sigma := \mathbb{E}(X - \mu)(X - \mu)^T$。为描述我们的量化映射 $X \to \dot{X}$，令$\Lambda := (\lambda_1, \cdots \lambda_d)$ 为一个向量，使得

$$\lambda_i \geq \max\left\{Q_{1-\varepsilon}(\langle X, e_i\rangle), -Q_{\varepsilon}(\langle X, e_i\rangle)\right\}, \quad i = 1, \cdots d. \tag{3.5}$$

这里我们也假设处于 $\varepsilon \asymp \log(1/\delta)/n$这一情形。接下来，通过（独立地）对 $\tau_i \sim \mathscr{U}[-1, 1]$ 进行采样，我们生成序列 $\tau_1, \cdots \tau_d$，并使用以下表达式对样本进行量化

$$\dot{X} := \begin{bmatrix} \operatorname{sign}\big(\langle X, e_1\rangle + \lambda_1\tau_1\big) \\ \operatorname{sign}\big(\langle X, e_2\rangle + \lambda_2\tau_2\big) \\ \vdots \\ \operatorname{sign}\big(\langle X, e_d\rangle + \lambda_d\tau_d\big) \end{bmatrix}.$$

为简化记号，我们记作

$$\dot{X} := \operatorname{sign}(X + \operatorname{Diag}(\Lambda)\tau), \tag{3.6}$$

其中，$\operatorname{Diag}(\Lambda)$ 是一个对角矩阵，其对角元素等于向量 Λ and $\tau := (\tau_1, \cdots \tau_d) \sim \mathscr{U}[-1, 1]^d$ 的各分量。这里，符号函数 $\operatorname{sign}(\cdot)$ 逐分量取值。

我们提出的第一个估计量是量化样本的经验均值 $\dot{X}_1, \cdots X_n$，即

$$\widehat{\mu}(\dot{X}_1, \cdots, \dot{X}_n) := \frac{1}{n}\sum_{i=1}^{n}\operatorname{Diag}(\Delta)\dot{X}_i. \tag{3.7}$$

定理 3.2 (无污染多元情形)。 存在一个绝对常数 $C > 0$ ，使得以下结论成立。由 $\widehat{\mu}$ 给出的估计量(3.6) 和 (3.7) 以至少 $1-\delta$ 的概率满足，

$$\|\widehat{\mu}-\mu\|_2 \le C\left(\max_{i\in[d]}\lambda_i\sqrt{\frac{\log(1/\delta)}{n}}+\sqrt{\frac{\sum_{i=1}^d\lambda_i^2}{n}}+\sqrt{\mathrm{Tr}(\Sigma)\frac{\log(1/\delta)}{n}}\right).$$

我们注意到，右侧的前两项在绝对常数意义下是最优的。首先，任何用于估计均值 μ 的多元均值估计量 $\widehat{\mu}$ 同时也是 μ， e_i 的估计量（对任意 $i\in[d]$ 而言），因此第一项是不可避免的。其次， X 的协方差矩阵的迹等于 $\sum_{i=1}^d\lambda_i^2$ ，与量化映射无关。因此，根据多元均值估计的标准极小极大速率 [20]，右侧的第二项在所有基于独立同分布比特的估计量中是极小极大最优的。最后，第三项是多元均值估计的标准极小极大速率 [20] ，但额外带有一个对数因子 $\log(1/\delta)$。

作为我们证明中的一个技术要点，我们需要回顾次高斯随机向量的概念。关于该主题的更全面介绍，请参阅 [28]。如果存在一个 $K>0$ ，使得随机变量 $Z\in\mathbb{R}$ 是 K-次高斯的，则称其为 K-次高斯。

$$\mathbb{P}\Big(|Z-\mathbb{E}Z|\ge(K\sigma_Z)t\Big)\le 2e^{-t^2/2},\quad \text{for all } t>0.$$

使该估计成立的最小 $K>0$ 记为 $\|Z\|_{\psi_2}$（ψ_2范数）。类似地，如果存在一个 $K>0$ ，使得下式成立，我们就称随机向量 X 是 K-次高斯：

$$\|\langle X,v\rangle\|_{\psi_2}\le K\sqrt{\langle\Sigma v,v\rangle},\quad \text{for every } v\in\mathbb{R}^d. \tag{3.8}$$

证明。 我们首先将误差估计分解为两部分：偏差项和集中项。根据三角不等式，

$$\|\widehat{\mu}-\mu\|_2\le\|\widehat{\mu}-\mathbb{E}\widehat{\mu}\|_2+\|\mu-\mathbb{E}\widehat{\mu}\|_2.$$

我们首先量化估计量与其期望值的接近程度（集中项）。为此，注意随机向量 $\mathrm{Diag}(\Delta)\,\dot{X}$ 的协方差矩阵 Σ 是一个对角矩阵，其对角元素为 λ_1^2、……、λ_d^2。此外，给定 X时， X 的各分量相互独立。因此，根据命题 2.7， 1]

$$\|\langle\dot{X},v\rangle\|_{\psi_2}^2\le\sum_{j=1}^d\|\langle\dot{X},e_j\rangle\|_{\psi_2}^2v_j^2\le c\sum_{j=1}^d\lambda_j^2v_j^2=c\langle\dot{\Sigma}v,v\rangle,$$

对于某个绝对常数 $c>0$。因此，经验均值的标准估计 $\widehat{\mu}$（例如参见 [21, 公式 1.5]）以如下概率满足

概率为 $1-\delta$,

$$\left\|\widehat{\mu}-\mathbb{E}\widehat{\mu}\right\|_2 = O\left(\sqrt{\frac{\sum_{i=1}^d \lambda_i^2}{n}} + \max_{i\in[d]}\lambda_i\sqrt{\frac{\log(1/\delta)}{n}}\right).$$

现在，只需控制偏差。为此，注意到

$$\mu-\mathbb{E}\widehat{\mu} = \mu-\mathbb{E}[\mathrm{Diag}(\Delta)\dot{X}] = \begin{bmatrix}\mathbb{E}(\langle X,e_1\rangle-\lambda_1)\mathbb{1}_{|\langle X,e_1\rangle|\geq\lambda_1}\\ \vdots \\ \mathbb{E}(\langle X,e_d\rangle-\lambda_d)\mathbb{1}_{|\langle X,e_d\rangle|\geq\lambda_d}\end{bmatrix},$$

这意味着我们需要控制以下量

$$\left|\langle\mu-\mathbb{E}\widehat{\mu},v\rangle\right| \leq \left|\sum_{j=1}^d \mathbb{E}\langle X,e_j\rangle-\lambda_j\mathbb{1}_{\langle X,e_j\rangle\geq\lambda_j}v_j\right| + \left|\sum_{j=1}^d \mathbb{E}\langle X,e_j\rangle+\lambda_j\mathbb{1}_{\langle X,e_j\rangle\leq-\lambda_j}v_j\right|.$$

我们关注右侧的第一项，第二项可以进行相同的分析。根据三角不等式和柯西-施瓦茨不等式，对于每个 $v\in S^{d-1}$，有

$$\begin{aligned}
&\left|\sum_{j=1}^d \mathbb{E}\langle X,e_j\rangle-\lambda_j\mathbb{1}_{\langle X,e_j\rangle\geq\lambda_j}v_j\right|\\
&\leq \left|\sum_{j=1}^d \mathbb{E}\overline{\langle X,e_j\rangle}\mathbb{1}_{\langle X,e_j\rangle\geq\lambda_j}v_j\right| + \left|\sum_{j=1}^d \mathbb{E}(\lambda_j-\langle\mu,e_j\rangle)\mathbb{1}_{\langle X,e_j\rangle\geq\lambda_j}v_j\right|\\
&\leq \sqrt{\sum_{j=1}^d(\mathbb{E}\overline{\langle X,e_j\rangle}\mathbb{1}_{\langle X,e_j\rangle\geq\lambda_j})^2} + \sqrt{\sum_{j=1}^d(\lambda_j-\langle\mu,e_j\rangle)^2\mathbb{P}\big(\langle X,e_j\rangle\geq\lambda_j\big)^2}\\
&\leq \sqrt{\sum_{j=1}^d\Sigma_{jj}\mathbb{P}(\langle X,e_j\rangle\geq\lambda_j)} + \sqrt{\sum_{j=1}^d(\lambda_j-\langle\mu,e_j\rangle)^2\mathbb{P}\big(\langle X,e_j\rangle\geq\lambda_j\big)^2}\\
&\leq \sqrt{\mathrm{Tr}(\Sigma)\frac{\log(1/\delta)}{n}} + \sqrt{\sum_{j=1}^d(\lambda_j-\langle\mu,e_j\rangle)^2\mathbb{P}\big(\overline{\langle X,e_j\rangle}\geq\lambda_j-\langle\mu,e_j\rangle\big)^2}\\
&= O\left(\sqrt{\mathrm{Tr}(\Sigma)\frac{\log(1/\delta)}{n}}\right),
\end{aligned}$$

其中在最后一步，我们利用以下事实估计了右侧的第二项:

$$(\lambda_j-\langle\mu,e_j\rangle)\mathbb{P}(\overline{\langle X,e_j\rangle}\geq\lambda_j-\langle\mu,e_j\rangle)\leq\sqrt{\Sigma_{jj}\log(1/\delta)/n}.$$

因此，我们在等式两边对所有 $v \in S^{d-1}$ 取上确界，从而得出：

$$\|\mu - \mathbb{E}\widehat{\mu}\|_2 = \sup_{v \in S^{d-1}} |\langle \mu - \mathbb{E}\widehat{\mu}, v \rangle| = O\left(\sqrt{\frac{\mathrm{Tr}(\Sigma)}{n}\log(1/\delta)}\right).$$

□

注释 3.3。鉴于公式（3.5），需要处理 d 调节参数 $\{\lambda_i\}_{i=1}^d$。对于每个 $i \in [d]$，可以将 $Q_{1-\varepsilon}(X, e_i) = Q_{1-\varepsilon}(X, e_i) + \mu, e_i$ 分解为中心化分位数的粗略估计与均值第 i 个坐标的位置之和。

当我们对均值向量 μ 的了解少于对中心化分布的了解，也就是说，没有关于 μ, e_i 的粗略界时，我们建议采用以下 Haar 随机化步骤：首先抽取一个 Haar 矩阵$O \sim$Haar(d) [3]，并将 $\{X_i\}_{i=1}^n$ 预处理为 $\{X_{i,O} := OX_i\}_{i=1}^n$，然后按照定理 3.2 中相同的（量化与估计）步骤，使用 $\{X_{i,O}\}_{i=1}^n$ 得到估计值 $\hat{}\mu$，最后将 $O^T\hat{}\mu$ 用作最终估计。由于现在只需对 $\|\mu\|_2$ 而非 $\{\mu, e_i\}_{i=1}^d$ 有一个粗略的（上界）估计，这或许能缓解调节问题：为说明这一点，注意到 $X_{i,O}$ 的均值为 $\mu_O := O\mu$，因而在 $\|\mu\|_2 S^{d-1}$ 上服从均匀分布。因此，标准的并集界论证表明

$$\max_{1 \le i \le d} |\langle O\mu, e_i \rangle| \le \|\mu\|_2 \sqrt{\frac{3\log d}{d}}$$

以高概率，因此我们可以设定

$$\lambda_i \ge \max\left\{Q_{1-\varepsilon}(\langle O\overline{X}, e_i\rangle) + \|\mu\|_2\sqrt{\frac{3\log d}{d}}, -Q_\varepsilon(\langle O\overline{X}, e_i\rangle) - \|\mu\|_2\sqrt{\frac{3\log d}{d}}\right\}$$

使用样本 $\{X_{i,O}\}_{i=1}^n$来估计均值 $O\mu$。这一论证对于分布式学习场景可能具有实际意义，因为 O 的生成和通信可以通过随机种子来处理，而且成本不高（例如参见 [23]），并且收敛速率仅受到一个额外的$O(\sqrt{\log d})$因子的影响。——

与一维情形不同，量化样本的经验均值似乎无法对抗对抗性噪声提供有力保证。沿用上述证明可以表明，由污染导致的附加项的量级为 $O\left(\eta\sqrt{\sum_{i=1}^d \lambda_i^2}\right)$；若不更换估计量，恐怕难以取得实质性改进。我们将在第 5 节给出一个数值示例，以佐证这一点。

[3]这意味着 O 在 $\mathbb{R}^{d\times d}$中所有正交归一矩阵构成的正交群上服从均匀分布。

基于这一事实，我们借鉴稳健统计学的文献，并回顾 Depersin 和 Lecu´e 在稳健均值估计方面的一项重要成果，下面将用我们的记号表述该结果。

命题 3.4 (Depersin 和 Lecu´e [9])。存在一个常数 $C > 0$，使得以下结论成立。假设处于 $\log(1/\delta) \geq 300\eta n$ 的情形。存在一个关于样本量 n 和维度 d的多项式时间算法，其输入为 n 随机向量的受污染样本 X，该随机向量的均值 μ 和协方差 Σ 满足 (2.4)，并输出一个向量 $\widehat{\mu}$，其以至少 $1-\delta$ 的概率满足

$$\|\widehat{\mu} - \mu\|_2 \leq C\left(\|\Sigma\|\sqrt{\frac{\log(1/\delta)}{n} + \eta} + \sqrt{\frac{\mathrm{Tr}(\Sigma)}{n}}\right).$$

接下来，我们采用一个更复杂的估计量来改进量化方案的鲁棒性保证。

定理 3.5 (多变量污染情形)。存在一个常数 $C>0$，使得以下结论成立。设 $\widehat{\mu}$ 为命题 *3.4* 中的估计量，输入为 ηn 由（*X 3.6*）给出的受污染样本，满足(2.4) 或 (2.5)。那么，以至少 $1-\delta$ 的概率，

$$\|\widehat{\mu} - \mu\|_2 \leq C\left(\max_{i\in[d]} \lambda_i \sqrt{\frac{\log(1/\delta)}{n} + \eta} + \sqrt{\frac{\sum_{i=1}^d \lambda_i^2}{n}} + \sqrt{\mathrm{Tr}(\Sigma)\frac{\log(1/\delta)}{n}}\right).$$

证明。我们应用之前相同的分解 $\|\widehat{\mu} - \mu\|_2 \leq \|\mu - \mathbb{E}\widehat{\mu}\|_2 + \|\widehat{\mu} - \mathbb{E}\widehat{\mu}\|_2$。偏差项 $\|\mu - \mathbb{E}X\|_2$ 的估计严格遵循定理3.2证明中的相同步骤。接下来，回顾一下，Diag(Δ)X 是一个随机向量，其协方差矩阵为对角协方差矩阵，等于 Diag(λ_1、 $\cdots$ λ_d)。因此，协方差矩阵的算子范数为 $\max_{i\in[d]} \lambda_i$，其迹等于 $\sum_{i=1}^d \lambda_i^2$。我们将命题 3.4 中的估计量应用于样本 Diag(Δ)X_1、$\cdots$、Diag(Δ)X_n，从而完成证明。 □

尽管当 X 只有两个有限阶矩时，因子 $\max_{i\in[d]} \lambda_i\sqrt{\eta}$ 是紧的，但在对 X的尾部作出更强假设的情况下，该因子可能得到改进。然而，我们不知道如何利用多项式时间算法实现这一点。

我们还要指出，或许可以利用 [22], 中的多变量截尾均值估计量的某个版本来改进这个额外的对数因子；然而，众所周知，此类估计量在计算上难以处理（运行时间随维度呈指数增长）。

4 部分量化下的均值估计

在第 3节中，我们推导出了分布式设置下满足量化约束的随机向量均值的（近似）最优估计量。如前所述，任何估计量都需要额外了解对均值位置敏感的数据。在实践中，对数据额外信息的依赖也会导致算法需要调节参数。我们或许可以问，是否能稍微放宽分布式设置，从而避免误差率对均值位置的依赖，并缓解调节问题。

尽管文献中广泛研究了完全量化通信模型，但在某些情形下，这些模型的限制可能过于严格。在实践中，人们可能希望放宽通信约束，使其不必一视同仁：由于带宽或能量限制，大多数观测值必须经过高度量化，但通常可以传输少量实值消息，用于协调或细化。事实上，实数被建模为定精度浮点数，例如采用32位的单精度格式。

本节旨在放宽严格的分布式设置，允许使用 $n_0 = o(n)$个未量化数据，然后再对其余 $n - n_0$ 样本进行量化。在此设置下使用的比特数为$32n_0 + (n - n_0) = (1 + o(1))n$，仅略多于分布式设置中使用的比特数。我们将其称为“部分量化”设置。

另一方面，正如我们将看到的，我们的估计量无需任何调参，而且收敛率不再取决于均值位置。

4.1 一维情形

我们先从无污染的单变量情形开始。下文中，我们将样本记为 $Y_1, Y_2, \ldots \ldots Y_{n_0}, X_{n_0+1}, \ldots\ldots X_n$，它们是随机变量 X 的独立同分布副本，其均值为 μ，方差为 σ^2。我们考虑未量化样本 $\mathcal{X}^{(\mathrm{f})} := \{Y_1, \ldots\ldots Y_{n_0}\} \quad X_n$，并对其余样本 $\{X_i\}_{i=n_0+1}^n$进行量化，量化时可能会利用样本 $\mathcal{X}^{(\mathrm{f})}$中的信息。

我们的目标是根据$\mathcal{X}^{(\mathrm{f})}$ 中的未量化样本以及量化后的样本$\{X_i\}_{i=n_0+1}^n$来估计均值 μ。请注意，我们寻求的均值估计器需要在 $n_0 = o(n)$ 的情形下保持准确；这使比特数从 $32n$ 降至 $(n - n_0) + 32n_0 = (1 + o(1))n$，仅略高于上一节所讨论的分布式设置中每个样本所用的一比特。

我们的估计过程也受到第 2 节所述截尾均值估计量的启发。在此情境下，我们的估计量使用来自$\mathcal{X}^{(\mathrm{f})}$ 的数据作为 X 的经验分位数，以剔除离群值。具体而言，对于某个

精心选择的参数 ε，我们建议计算 $\mathcal{X}^{(\mathrm{f})}$ 的经验 ε分位数和（$1-\varepsilon$）分位数

$$\alpha := Y^*_{\varepsilon n_0} \qquad \text{and} \qquad \beta := Y^*_{(1-\varepsilon)n_0}, \tag{4.1}$$

由此，我们进一步计算均值 μ的粗略估计 μ_1，以及未量化样本的近似范围

$$\mu_1 := \frac{\alpha+\beta}{2} \qquad \text{and} \qquad \Delta := \frac{\beta-\alpha}{2}. \tag{4.2}$$

接下来，为了量化样本 $\{X_i\}_{i=n_0+1}^n$，我们提出先将数据平移 μ_1，然后使用抖动级别为 Δ 的独立均匀抖动量 τ_i。也就是说，我们抽取一个独立同分布序列的随机变量 $\{\tau_i\}_{i=n_0+1}^n$，其分布为 $\mathscr{U}([-1,1])$，然后保留以下 $n-n_0$ 个比特

$$\dot{X}_i := \operatorname{sign}(X_i - \mu_1 + \Delta\tau_i), \qquad n_0+1 \le i \le n. \tag{4.3}$$

我们再次利用截尾估计量与抖动之间的关系（2.3）推导出

$$\mathbb{E}(\Delta\dot{X}|X) = \phi_{\alpha,\beta}(X) - \mu_1. \tag{4.4}$$

我们的估计量为

$$\hat{\mu} := \frac{\Delta}{n-n_0}\sum_{i=n_0+1}^{n}\dot{X}_i + \mu_1. \tag{4.5}$$

为准确陈述我们的结果，对于 $t \in (0,1)$，定义

$$\mathcal{E}(\overline{X};t) := \max\Big\{\mathbb{E}\Big[|\overline{X}|\mathbf{1}\{\overline{X}_i \le Q_t(\overline{X})\}\Big], \mathbb{E}\Big[|\overline{X}|\mathbf{1}\{\overline{X} \ge Q_{1-t}(\overline{X})\}\Big]\Big\}. \tag{4.6}$$

为简化起见，我们以某个指定的概率保证来陈述结果，而不再使用之前的一般置信水平 δ。这样可以简化表达式，并避免冗长复杂的表述。

为方便读者，我们回顾一下 X 的中心化版本的记号，即 $\overline{X} = X - \mathbb{E}X$。现在，我们陈述部分量化设置中最简单情形下的结果。

定理 4.1。存在绝对常数 C，c_1，$c_2 > 0$ 使得以下结论成立。考虑公式 (4.3) 中的量化映射以及公式 (4.5) 中的估计量，其参数为 $n_0 \le \frac{n}{2}$ 和 $\varepsilon > 0$。那么，以至少 $1 - 4\exp(-c_1 n_0\varepsilon) - \frac{2}{n}$ 的概率，有

$$\begin{aligned}|\hat{\mu}-\mu| &\le \mathcal{E}\Big(\overline{X};\frac{3\varepsilon}{2}\Big) + 3\varepsilon\big|\max\{-Q_{1-\varepsilon/2}(\overline{X}), Q_{3\varepsilon/2}(\overline{X})\}\big| \\ &\quad + \Big(Q_{1-\varepsilon/2}(\overline{X}) - Q_{\varepsilon/2}(\overline{X})\Big)\sqrt{\frac{\log n}{n}}.\end{aligned} \tag{4.7}$$

特别地，如果 X 是 K-次高斯的，那么在条件 $n_0 := \sqrt{n}\log n$ 且 $\varepsilon := c_2\sqrt{\log_n n}$ 下，以至少 $1-\frac{1}{n}$ 的概率，有

$$|\hat{\mu}-\mu| \le CK\frac{\log n}{\sqrt{n}}. \tag{4.8}$$

注意到，收敛速率取决于 X 的分位数，而非 X的分位数。因此，完全避免了对均值位置的依赖。此外，对于次高斯 X，除一个较小的对数因子 $\sqrt{\log n}$外，收敛速率是最优的，这表明我们的结果与极小极大最优速率相当接近。最后，我们指出，只需调整定理中的绝对常数，尾概率估计 n^{-1} 就可以替换为对任意常数 $c>1$ 都成立的更快衰减 n^c 。

证明。 回顾方程（2.2）中分位数的定义以及以下事实：$Q_\varepsilon(X) = Q_\varepsilon(X) + \mu$。注意，对于任意 $0<\delta<\varepsilon$,

$$|\{i\in[n_0] : Y_i \le Q_{\varepsilon-\delta}(X)\}| \sim \mathrm{Bin}(n_0, \varepsilon-\delta).$$

因此，根据Chernoff不等式

$$\mathbb{P}\left(|\{i\in[n_0] : Y_i \le Q_{\varepsilon-\delta}(X)\}| \le \left(\varepsilon-\frac{\delta}{2}\right)n_0\right) \ge 1-p_1, \tag{4.9}$$

其中 $p_1 := \exp\left(-n_0 \mathrm{D}_{\mathrm{KL}}\left(\varepsilon-\frac{\delta}{2}\|\varepsilon-\delta\right)\right)$。类似地，我们有

$$\mathbb{P}\left(|\{i\in[n_0] : Y_i \ge Q_{\varepsilon+\delta}(X)\}| \le \left(1-\varepsilon-\frac{\delta}{2}\right)n_0\right) \ge 1-p_2 \tag{4.10}$$

其中 $p_2 := \exp\left(-n_0 \mathrm{D}_{\mathrm{KL}}\left(\varepsilon+\frac{\delta}{2}\|\varepsilon+\delta\right)\right)$。特别地，令 $\delta := \varepsilon/2$，则存在一个绝对常数 $c_1>0$ ，使得

$$p_1+p_2 \le e^{-c_1 n_0 \varepsilon} + e^{-c_1 n_0 \varepsilon} = 2e^{-c_1 n_0 \varepsilon},$$

因此

$$\mathbb{P}\Big(Q_{\varepsilon/2}(X) \le \alpha \le Q_{3\varepsilon/2}(X)\Big) \ge 1-(p_1+p_2) \ge 1-2e^{-c_1 n_0 \varepsilon}. \tag{4.11}$$

类似地，我们有

$$\mathbb{P}\Big(Q_{1-\varepsilon/2}(X) \le \beta \le Q_{1-3\varepsilon/2}(X)\Big) \ge 1-2e^{-c_1 n_0 \varepsilon}. \tag{4.12}$$

在证明的其余部分，我们在（4.11）和（4.12）成立的事件条件下进行。接下来，我们结合（4.4）和（4.5），并对抖动取期望，得到

$$\mathbb{E}(\hat{\mu}) = \mathbb{E}[\phi_{\alpha,\beta}(X)]. \tag{4.13}$$

根据截断函数$\phi_{\alpha,\beta}(\cdot)$，（4.13）结合（4.11）和（4.12）可知

$$\begin{aligned}
\mathbb{E}(\hat{\mu}) &\le \mathbb{E}\Big[\phi_{Q_{3\varepsilon/2}(X),Q_{1-\varepsilon/2}(X)}(X)\Big] \\
&= \mu + \mathbb{E}\Big[\phi_{Q_{3\varepsilon/2}(X),Q_{1-\varepsilon/2}(X)}(X) - X\Big] \\
&\le \mu + \mathbb{E}\Big[(Q_{3\varepsilon/2}(X) - X)\mathbf{1}(X \le Q_{3\varepsilon/2}(X))\Big] \\
&= \mu + \mathbb{E}\Big[(Q_{3\varepsilon/2}(\overline{X}) - \overline{X})\mathbf{1}(\overline{X} \le Q_{3\varepsilon/2}(\overline{X}))\Big] \\
&\le \mu + \mathbb{E}\Big[|\overline{X}|\mathbf{1}(\overline{X} \le Q_{3\varepsilon/2}(\overline{X}))\Big] + Q_{3\varepsilon/2}(\overline{X})\frac{3\varepsilon}{2}.
\end{aligned} \tag{4.14}$$

同理，我们有

$$\mathbb{E}(\hat{\mu}) \ge \mu - \mathbb{E}\Big[|\overline{X}|\mathbf{1}(\overline{X} \ge Q_{1-\varepsilon/2}(\overline{X}))\Big] + Q_{1-\varepsilon/2}(\overline{X})\frac{3\varepsilon}{2}.$$

回顾方程（4.6）中的误差项，我们得出偏差项受以下内容控制

$$|\mathbb{E}(\hat{\mu}) - \mu| \le \mathcal{E}(\overline{X}; 3\varepsilon/2) + 3\varepsilon\big|\max\big\{-Q_{1-\varepsilon/2}(\overline{X}), Q_{3\varepsilon/2}(\overline{X})\big\}\big|, \tag{4.15}$$

这对应于方程（4.7）右侧的前两项。接下来需要控制集中项 $|\hat{\mu} - \mathbb{E}(\hat{\mu})|$。为此，我们写出

$$|\hat{\mu} - \mathbb{E}(\hat{\mu})| = \left|\frac{1}{n - n_0}\sum_{i=n_0+1}^{n}(\Delta\dot{X}_i - \mathbb{E}[\Delta\dot{X}_i])\right|, \tag{4.16}$$

并应用 Hoeffding 不等式，可得对任意 $t > 0$

$$\mathbb{P}\Big(|\hat{\mu} - \mathbb{E}(\hat{\mu})| \ge t\Big) \le 2\exp\Big(-\frac{(n - n_0)t^2}{2\Delta^2}\Big). \tag{4.17}$$

特别地，令 $t = \Delta\sqrt{2\log_{n-n_0} n}$，则以至少$1 - \frac{2}{n}$的概率，有

$$|\hat{\mu} - \mathbb{E}(\hat{\mu})| \le \Delta\sqrt{\frac{2\log n}{n - n_0}} \le 2\Delta\sqrt{\frac{\log n}{n}}. \tag{4.18}$$

在事件（4.11）和（4.12）发生时，我们有

$$\Delta = \frac{\beta - \alpha}{2} \le \frac{Q_{1-3\varepsilon/2}(\overline{X}) - Q_{\varepsilon/2}(\overline{X})}{2}. \tag{4.19}$$

因此，由公式（4.15）和公式（4.18）

$$|\widehat{\mu} - \mathbb{E}\widehat{\mu}| \le (Q_{1-3\varepsilon/2}(\overline{X}) - Q_{\varepsilon/2}(\overline{X}))\sqrt{\frac{\log n}{n}},$$

以至少 $1 - 4e^{-c_1 n_0 \varepsilon} - \frac{2}{n}$ 的概率，这就完成了第一部分的证明。对于命题的第二部分，我们应用次高斯分布的标准尾部估计，得到

$$\varepsilon\big|\max\{-Q_{1-\varepsilon/2}(\overline{X}), Q_{3\varepsilon/2}(\overline{X})\}\big| + \mathcal{E}\Big(\overline{X}; \frac{3\varepsilon}{2}\Big) \le c_2 K\varepsilon\sqrt{\log(1/\varepsilon)}, \quad (4.20)$$

$$Q_{1-\varepsilon/2}(\overline{X}) - Q_{\varepsilon/2}(\overline{X}) \le c_3 K\sqrt{\log(1/\varepsilon)}. \quad (4.21)$$

令 $n_0 = \sqrt{n}\log n$ 且 $\varepsilon = c_4\sqrt{\log_n n}$，其中常数 c_4足够大，即可得到所需结论。□

4.2 一维情形下的对抗噪声

现在我们来考察估计量在面对 η比例的对抗噪声时的鲁棒性。回顾公式（2.4）中的量化前噪声，以及公式（2.5）中的量化后噪声。它们分别刻画了过程不同阶段产生的污染（例如，参见 [13]）。在部分量化中，量化前噪声（2.4）更难处理，因为用于计算分位数 $\alpha = Y^*_{\varepsilon n_0}$ 和 $\beta = Y^*_{(1-\varepsilon)n_0}$ 的$\{X_i\}_{i=1}^n$ 个样本可能全部受到污染。为避免这种情况，我们将在$\{Y_i\}_{i=1}^{n_0}$的选取中引入随机性。另一方面，请注意，我们现在只使用比特 $\{X_i : n_0 + 1 \le i \le n\}$ 来构造估计量，因此量化后噪声应表述为

$$|\{n_0 + 1 \le i \le n : \widetilde{\dot{X}}_i = -\dot{X}_i\}| \le \eta n. \quad (4.22)$$

我们首先证明，我们的估计量 $\hat{}\mu$能够鲁棒地应对量化过程（4.22）中出现的量化后噪声。使用 $n - n_0$ 受损的比特 $\{X_i\}_{i=n_0+1}^n$，我们的估计量可表示为

$$\widetilde{\mu} := \frac{\Delta}{n - n_0}\sum_{i=n_0+1}^{n} \widetilde{\dot{X}}_i + \mu_1, \quad (4.23)$$

其中 μ_1 定义见公式（4.2）。

定理 4.2 (存在量化后噪声的单变量情形，见（4.22）)。 存在绝对常数 C, c_1, $c_2 > 0$ 使得下述结论成立。考虑估计量 $\widetilde{\mu}$ ，其定义见公式 (4.23)，其中 $\{X_i\}_{i=n_0+1}^n$ 满足 （*4.22*） ，其中

$\widetilde{\{X_i\}_{i=1}^{n_0}}$ 与定理 *4.1*中的相同。对于任意 $\eta \le 1/c_2$，则以至少 $1-\exp(-c_1 n_0 \varepsilon) - \frac{2}{n}$ 的概率，有

$$|\widetilde{\mu} - \mu| \le \mathcal{E}\Big(\overline{X}; \frac{3\varepsilon}{2}\Big) + 3\varepsilon \big|\max\{-Q_{1-\varepsilon/2}(\overline{X}), Q_{3\varepsilon/2}(\overline{X})\}\big| \tag{4.24}$$

$$+ (Q_{1-\varepsilon/2}(\overline{X}) - Q_{\varepsilon/2}(\overline{X}))\left(\sqrt{\frac{\log n}{n}} + 2\eta\right). \tag{4.25}$$

特别地，如果 X 是 K-次高斯的，那么在 $n_0 = \sqrt{n}\log n$ 且 $\varepsilon = c_2 \max\{\eta, \sqrt{\log n/n}\}$ 的条件下，以至少 $1-\frac{1}{n}$ 的概率，我们有

$$|\widetilde{\mu} - \mu| \le CK\left(\frac{\log n}{\sqrt{n}} + \eta\sqrt{\log(1/\eta)}\right). \tag{4.26}$$

我们注意到，附加误差项 $\eta\sqrt{\log(1/\eta)}$ 与对抗噪声下、具有次高斯 X 且来自 [22] 的均值估计的极小极大下界相匹配。

证明。令 $\hat{\mu}$ 为定理4.1中的估计量。我们只需估计由对抗性污染 $|\widetilde{\mu} - \hat{\mu}|$ 导致的附加误差项。为此，根据公式（4.22），有

$$|\widetilde{\mu} - \hat{\mu}| = \frac{\Delta}{n-n_0}\left|\sum_{i=n_0+1}^{n}(\widetilde{\dot{X}}_i - \dot{X}_i)\right| \le \frac{2\Delta\eta n}{n-n_0} \le 4\Delta\eta. \tag{4.27}$$

此外，根据定理 4.1的证明中的（4.19），以所承诺的概率，我们有

$$|\widetilde{\mu} - \hat{\mu}| \le 2\eta(Q_{1-\varepsilon/2}(\overline{X}) - Q_{\varepsilon/2}(\overline{X})). \tag{4.28}$$

结合（4.7）可得（4.24）。为了得到次高斯X的界，我们回顾公式（4.20）和公式（4.21）中的估计。注意，只要 $\eta \le \sqrt{n}/\log n$，这些估计就与定理 4.1中的相同。还需注意，$\log 1/\varepsilon = O(\log n)$。当 $\eta < \sqrt{n}/\log n$时，这显然成立。另一方面，当 $\eta \ge \sqrt{n}/\log n$ 时，有$\varepsilon = c_2\eta$，并且 $\log(1/\eta) \le \log(n)/2$。 □

接下来，我们考虑量化前噪声（2.4），它发生在我们的$\widetilde{\ }$过程之前，并会污染整个样本 $\{X_i\}_{i=1}^n$ 到 $\{X_i\}_{i=1}^n$。在这种情况下，我们先前的构造可能无法保持鲁棒。事实上，我们的目标是维持 $n_0 = o(n$ 这一范围，但这时集合 $\mathcal{X}^{(f)} = \{Y_1, \cdots Y_{n_0}\}$ 中的所有样本都有可能被污染，从而使我们的过程彻底失效。

为解决这一问题，我们建议从总共 n 个索引中进行无放回抽样，均匀随机地选择索引 $\{i_1, i_2, \cdots i_{n_0}\}$。接下来，$\widetilde{\ }$ $\widetilde{\ }$ $\widetilde{\ }$我们考虑集合 $\{X_{i_1}, X_{i_2}, \cdots X_{i_{n_0}}\}$，我们将其（稍微滥用一下记号）

记作 $\{Y_1, Y_2, \cdots \quad Y_{n_0}\}$。给定这组包含 n_0 个未量化样本的集合，我们计算分位数

$$\alpha := Y^*_{\varepsilon n_0} \quad \text{and} \quad \beta := Y^*_{(1-\varepsilon)n_0},$$

针对某个精心选择的 $\varepsilon > 0$。随后，我们对剩余的 $n - n_0$ 个样本采用与之前类似的量化方法。更准确地说，不失一般性，假设 $i_1 = 1$，$i_2 = 2$，$\ldots$，$i_{n_0} = n_0$，并考虑 $\tilde{}$ $\tilde{}$ 个样本 $\{X_{n_0+1}, \cdots \quad X_n\}$，我们计算

$$\mu_1 := \frac{\alpha + \beta}{2} \quad \text{and} \quad \Delta := \frac{\beta - \alpha}{2},$$

与之前一样，我们从 $\mathscr{U}([-1, 1])$ 中独立同分布地抽取 $\{\tau_i\}_{i=n_0+1}^n$，以应用量化映射

$$\dot{\tilde{X}}_i := \operatorname{sign}(\tilde{X}_i - \mu_1 + \Delta\tau_i), \qquad n_0 + 1 \le i \le n. \tag{4.29}$$

我们的估计量与之前的公式（4.23）形式相同：

$$\tilde{\mu} = \frac{\Delta}{n - n_0} \sum_{i=n_0+1}^{n} \dot{\tilde{X}}_i + \mu_1. \tag{4.30}$$

现在我们证明，采用我们的抽样策略，即使不限制对手可以影响哪些样本，也能获得与前一定理类似的保证。

定理4.3（公式（2.4）中的含污染的单变量情形）。存在绝对常数 C，c_1，$c_2 > 0$，使得以下结论成立。假设存在任意的 η-比例污染，如公式（2.4）所示，其中 $0 < \eta \le 1/8$。考虑基于公式（4.29）中的量化数据构造的公式（4.30）中的估计量。那么，对于任意 $\varepsilon \ge 8\eta$，以至少 $1 - 5\exp(-\frac{\varepsilon n_0}{24}) - \frac{2}{n}$ 的概率，我们有

$$\begin{aligned} |\tilde{\mu} - \mu| \le \mathcal{E}(\overline{X}; 2\varepsilon) + 4\varepsilon \Big| \max\{-Q_{1-\varepsilon/2}(\overline{X}), Q_{\varepsilon/2}(\overline{X})\} \Big| \\ + (Q_{1-\varepsilon/2}(\overline{X}) - Q_{\varepsilon/2}(\overline{X})) \left(\frac{3\eta}{2} + \sqrt{\frac{\log n}{n}} \right). \end{aligned}$$

具体而言，若 X 是 K-次高斯的，则对于 $\varepsilon =$ 最大值$\{8\eta, c_2\sqrt{\text{对数}}\, n/n\}$，且 $n_0 = \sqrt{n}$对数 n，以至少 $1 - \frac{1}{n}$ 的概率，我们有

$$|\tilde{\mu} - \mu| \le CK \left(\frac{\log n}{\sqrt{n}} + \eta\sqrt{\log(1/\eta)} \right). \tag{4.31}$$

证明。令 Z 表示集合 $\{Y_1, \cdots Y_{n_0}\}$ 中污染样本的数量。注意， Z 服从超几何分布：从大小为 n 的总体中抽取 n_0 个样本，其中 ηn 个是受污染样本。注意， Z 的均值为 ηn_0 ，它在随机序上被另一个超几何分布 Z' 所支配；该分布从大小为 n 的总体中抽取 n_0 个样本，其中 $(\varepsilon/6)n_0 > \eta n_0$ 个是受污染样本。因此，令 $p := \varepsilon/6$，根据超几何分布的标准尾部估计（例如参见 [15]），对于每个 $0 < t < p$，我们有

$$\mathbb{P}(Z \geq (p+t)n_0) \leq \mathbb{P}(Z' \geq (p+t)n_0) \leq e^{-D(p-t||p)}.$$

通过简单的泰勒级数展开，我们知道对于 p足够小的情况， $D(3p/2||p) \geq 0.1p$ 。特别地，令 $t = p/2$ ，即可确保

$$\mathbb{P}\left(Z \leq \frac{\varepsilon}{4}n_0\right) \geq 1 - e^{-0.1\varepsilon n_0}. \tag{4.32}$$

在证明的其余部分，我们假设上述事件成立。接下来，我们着手估计 α 和 β。为此，我们首先考虑 n_0 个未受污染的样本 $X_1, \cdots X_{n_0}$。根据Chernoff不等式，有

$$\mathbb{P}\left(|\{i \in [n_0] : X_i \geq Q_{1-2\varepsilon}(X)\}| \geq \frac{3}{2}\varepsilon n_0\right) \geq 1 - e^{-\varepsilon n_0/24},$$

并且

$$\mathbb{P}\left(|\{i \in [n_0] : X_i \leq Q_{1-\varepsilon/2}(X)\}| \geq (1 - \frac{3}{4}\varepsilon)n_0\right) \geq 1 - e^{-\varepsilon n_0/24}.$$

为考虑对抗噪声，注意到根据我们对 Z 的估计（见公式（4.32））， 我们得到其成立的概率至少为 $1 - 2e^{-\varepsilon n_0/24}$:

$$|\{i \in [n_0] : Y_i \geq Q_{1-2\varepsilon}(X)\}| \geq \left(\frac{3}{2}\varepsilon - \frac{\varepsilon}{4}\right)n_0 \geq \varepsilon n_0 \quad \text{and that} \tag{4.33}$$

$$|\{i \in [n_0] : Y_i \leq Q_{1-\varepsilon/2}(X)\}| \geq \left(1 - \frac{3}{4}\varepsilon - \frac{\varepsilon}{4}\right)n_0 = (1-\varepsilon)n_0. \tag{4.34}$$

在此事件中，我们可以保证

$$Q_{1-2\varepsilon}(X) \leq \beta \leq Q_{1-\varepsilon/2}(X). \tag{4.35}$$

类似地，以至少 $1 - 2e^{-\varepsilon n_0/24}$ 的概率，我们有

$$Q_{\varepsilon/2}(X) \leq \alpha \leq Q_{2\varepsilon}(X). \tag{4.36}$$

现在我们可以开始分析所提出的估计量。接下来，我们假设方程（4.32）、（4.35）和（4.36）中的事件均成立。

接下来的论证将重述定理 4.1和 4.2中的论证。首先，我们控制污染对$\{X_i\}_{i=n_0+1}^{n}$的影响。我们定义 $\dot{X}_i = \text{sign}(X_i - \mu_1 + \tau_i$，当 $n_0 + 1 \le i \le n$ 时，并考虑

$$\widehat{\mu} = \frac{\Delta}{n - n_0} \sum_{i=n_0+1}^{n} \dot{X}_i + \mu_1.$$

根据三角不等式，我们有

$$|\widetilde{\mu} - \mu| \le |\widetilde{\mu} - \widehat{\mu}| + |\mathbb{E}\widehat{\mu} - \mu| + |\widehat{\mu} - \mathbb{E}\widehat{\mu}|.$$

我们分别估计右侧的三个项。对于第一项，我们重复推导公式（2.4）和公式（4.22）时使用的论证，

$$\begin{aligned}
&|\widetilde{\mu} - \widehat{\mu}| \le \frac{2\Delta\eta n}{n - n_0} \le 3\eta\Delta \le \frac{3\eta}{2}(\beta - \alpha) \\
&\le \frac{3}{2}\eta(Q_{1-\varepsilon/2}(\overline{X}) - Q_{\varepsilon/2}(\overline{X})) \quad \text{(from Equations (4.35) and (4.36))}.
\end{aligned}$$

对于第二项，回想一下 $X = X - \mathbb{E}X$，并重复证明公式（4.15）时使用的相同论证，从而得到

$$|\mathbb{E}\widehat{\mu} - \mu| \le \mathcal{E}(\overline{X}; 2\varepsilon) + 4\varepsilon \max\left|\{Q_{1-\varepsilon/2}(\overline{X}), Q_{\varepsilon/2}(\overline{X})\}\right|.$$

接下来需要界定第三项 $|\widehat{\mu} - \mathbb{E}\widehat{\mu}|$。为此，我们对$\{\tau_i\}_{i=n_0+1}^{n}$ 的随机性应用 Hoeffding 不等式，得到

$$\mathbb{P}\left(|\widehat{\mu} - \mathbb{E}\widehat{\mu}| \le (\beta - \alpha)\sqrt{\frac{\log n}{n}}\right) = \mathbb{P}\left(|\widehat{\mu} - \mathbb{E}\widehat{\mu}| \le 2\Delta\sqrt{\frac{\log n}{n}}\right) \ge 1 - \frac{2}{n}.$$

结合公式（ α 和 β 中导出的估计式（4.36）和公式（4.35），即可完成第一部分的证明。

若要在 X 为次高斯时得到陈述的第二部分，回想式（4.20）和（4.21），对于足够小的 ε 和某些绝对常数 c_5， c_6，我们有

$$\begin{aligned}
\mathcal{E}(\overline{X}; 2\varepsilon) + 4\varepsilon\left|\max\left\{-Q_{1-\varepsilon/2}(\overline{X}), Q_{\varepsilon/2}(\overline{X})\right\}\right| &\le c_5 K\varepsilon\sqrt{\log(1/\varepsilon)}\,, \\
\eta|Q_{1-\varepsilon/2}(\overline{X}) - Q_{\varepsilon/2}(\overline{X})| \le \varepsilon|Q_{1-\varepsilon/2}(\overline{X}) - Q_{\varepsilon/2}(\overline{X})| &\le c_6 K\varepsilon\sqrt{\log(1/\varepsilon)}\,.
\end{aligned}$$

按照定理 4.2证明末尾的论证，我们得到所述的收敛速率。

□

4.3 多变量情形

现在我们说明如何将这些构造推广到多变量情形。首先，我们像之前一样将样本 $X_1, \cdots X_n$ 划分为集合 $\mathcal{X}^{(\mathrm{f})} = \{Y_1, \cdots Y_{n_0}\}$ 和 $\mathcal{X}^{(\mathrm{q})} = \{X_{n_0+1}, \cdots X_n\}$。我们将计算每个 $j \in [d]$ 的分位数，

$$\alpha_j = \langle Y, e_j \rangle^*_{\varepsilon n_0} \quad \text{and} \quad \beta_j = \langle Y, e_j \rangle^*_{(1-\varepsilon)n_0},$$

并计算向量 $\alpha = (\alpha_1, \cdots \alpha_d)^\top$ 和 $\beta = (\beta_1, \cdots \beta_d)^\top$。

与之前类似，我们计算 $\mu_1 := \frac{1}{2}(\alpha + \beta)$ 和 $\Delta := \frac{1}{2}(\beta - \alpha)$。接下来对样本进行量化，抽取 $\tau_{n_0+1}, \cdots \tau_n \overset{iid}{\sim} \mathscr{U}[-1,1]^d$，然后将 $\{X_i\}_{i=n_0+1}^n$ 量化为

$$\dot{X}_i = \mathrm{sign}(X_i - \mu_1 + \mathrm{Diag}(\Delta)\tau_i), \tag{4.37}$$

估计量定义为

$$\widehat{\mu} = \frac{1}{n - n_0} \sum_{i=n_0+1}^{n} \mathrm{Diag}(\Delta)\dot{X}_i + \mu_1, \tag{4.38}$$

这相当于对每个分量分别执行单变量过程。因此，我们的估计量将比特数从 $32nd$ 降低到 $32n_0 d + (n - n_0)d = (1 + o(1))nd$。与此同时，下一个定理表明，我们的估计量具有非渐近保证，其界限仅略大于基于未量化样本的估计量已有的估计结果（最多相差一个对数因子）。

定理 4.4 (无污染多元情形)。存在绝对常数 C、c_1、c_2、$c_3 > 0$，使得以下结论成立。考虑上述参数为 $n_0 \le \frac{n}{2}$ 和 $\varepsilon > 0$ 的量化与估计过程。以至少 $1 - 4d\exp(-c_1\varepsilon n_0) - \frac{2}{d}$ 的概率，我们有

$$\begin{aligned}\|\hat{\mu} - \mu\|_2 \le c_2 &\left(\sum_{j=1}^{d} \mathcal{E}(\overline{X}_j; 2\varepsilon)^2 + \varepsilon^2 \max\left\{ -Q_{1-\varepsilon/2}(\langle \overline{X}, e_j \rangle), Q_{3\varepsilon/2}(\langle \overline{X}, e_j \rangle) \right\}^2 \right)^{1/2} \\ &+ c_2 \sqrt{\frac{\sum_{j=1}^{d} [Q_{1-\varepsilon/2}(\langle X_i, e_j \rangle) - Q_{\varepsilon/2}(\langle X_i, e_j \rangle)]^2}{n}} \\ &+ c_2 \sqrt{\frac{\log d \max_{j \in [d]} [Q_{1-\varepsilon/2}(\langle X_i, e_j \rangle) - Q_{\varepsilon/2}(\langle X_i, e_j \rangle)]^2}{n}}.\end{aligned}$$

具体而言，对于 $n_0 = \sqrt{n \log d}$ 和 $\varepsilon = \frac{c_3}{\sqrt{n}}$，若 X 是 K-次高斯的，则其概率至少为 $1 - \frac{1}{d}$，

$$\|\hat{\mu} - \mu\|_2 \le CK \log(n) \sqrt{\frac{\mathrm{Tr}(\Sigma) + \|\Sigma\| \log(d)}{n}}. \tag{4.39}$$

可以看出，对于具有次高斯数据的未量化估计量，一旦我们将置信水平设为 $\delta \asymp d^{-1}$，所能期望的最佳结果是 $O(\sqrt{\mathrm{Tr}(\Sigma)/n + \|\Sigma\|\log\ d/n})$。因此，我们的估计在相差一个温和的 $\log(n)$ 因子的意义下是最优的。

证明。我们像之前一样，应用三角不等式，将误差估计分解为偏差项和集中项:

$$\|\hat{\mu} - \mu\|_2 \leq \|\mathbb{E}\hat{\mu} - \mu\|_2 + \|\hat{\mu} - \mathbb{E}\hat{\mu}\|_2. \tag{4.40}$$

为控制偏差，我们固定一个指标 $j \in [d]$ ，并应用切尔诺夫界，重新推导定理4.1证明中的论证。具体而言，我们得到

$$Q_{\varepsilon/2}(\langle X_i, e_j\rangle) \leq \alpha_j \leq Q_{3\varepsilon/2}(\langle X_i, e_j\rangle), \tag{4.41}$$
$$Q_{1-3\varepsilon/2}(\langle X_i, e_j\rangle) \leq \beta_j \leq Q_{1-\varepsilon/2}(\langle X_i, e_j\rangle) \tag{4.42}$$

其概率至少为 $1 - 4\exp(-c_1\varepsilon n_0)$。对所有指标 $j \in [d]$应用并集界，我们得出，方程（4.41）和（4.42）中的事件很可能发生，也就是说，概率至少为 $1 - 4d\exp(-c_1\varepsilon n_0$时，所有事件对所有指标同时成立。因此，我们有

$$\Delta_j \leq \frac{1}{2}[Q_{1-\varepsilon/2}(\langle X_i, e_j\rangle) - Q_{\varepsilon/2}(\langle X_i, e_j\rangle)]. \tag{4.43}$$

接下来，我们可以重新推导用于得到方程（4.15）的论证，从而得到对每个 $j \in [d]$,

$$|\mathbb{E}(\hat{\mu}_j) - \mu_j| \leq \mathcal{E}(\langle \overline{X}, e_j\rangle; 3\varepsilon/2) + 3\varepsilon \max\left|\{Q_{1-\varepsilon/2}(\langle \overline{X}, e_j\rangle), Q_{3\varepsilon/2}(\langle \overline{X}, e_j\rangle)\}\right|,$$

这意味着

$$\|\mathbb{E}\hat{\mu} - \mu\|_2 \leq \left(\sum_{j=1}^{d} 2\mathcal{E}(\overline{X}_j; 2\varepsilon)^2 + 18\varepsilon^2|\{Q_{1-\varepsilon/2}(\langle \overline{X}, e_j\rangle), Q_{3\varepsilon/2}(\langle \overline{X}, e_j\rangle)\}|^2\right)^{1/2}. \tag{4.44}$$

接下来需要控制集中项 $\|\hat{}\mu - \mathbb{E}\hat{}\mu\|_2$ ，它可以写成

$$\begin{aligned}\|\hat{\mu} - \mathbb{E}\hat{\mu}\|_2 &= \left\|\frac{1}{n-n_0}\sum_{i=n_0+1}^{n} \mathrm{Diag}(\Delta)[\dot{X}_i - \mathbb{E}\dot{X}_i]\right\|_2 \\ &= \sup_{v\in\mathbb{S}^{d-1}} \left\langle \mathrm{Diag}(\Delta)v, \frac{1}{n-n_0}\sum_{i=n_0+1}^{n}[\dot{X}_i - \mathbb{E}\dot{X}_i]\right\rangle \\ &= \sup_{v\in\mathrm{Diag}(\Delta)\mathbb{S}^{d-1}} \left\langle v, \frac{1}{n-n_0}\sum_{i=n_0+1}^{n}[\dot{X}_i - \mathbb{E}\dot{X}_i]\right\rangle.\end{aligned} \tag{4.45}$$

我们以$\{X_i\}_{i=n_0+1}^n, \alpha, \beta$为条件，并利用$\{\tau_i\}_{i=n_0+1}^n \overset{iid}{\sim} \mathscr{U}[-1,1]^d$的随机性，则$\dot{X}_i = \text{sign}(X_i - \mu_1 + \text{对角化}(\Delta)\tau_i)$的各个元素相互独立。因此，对于任意$v_1, v_2 \in \text{对角化}(\Delta)\mathbb{S}^{d-1}$，我们有

$$\begin{aligned}
&\left\| \left\langle v_1 - v_2, \frac{1}{n-n_0} \sum_{i=n_0+1}^n [\dot{X}_i - \mathbb{E}\dot{X}_i] \right\rangle \right\|_{\psi_2}^2 \\
&\leq \frac{c_2}{(n-n_0)^2} \sum_{i=n_0+1}^n \|\langle v_1 - v_2, \dot{X}_i - \mathbb{E}\dot{X}_i \rangle\|_{\psi_2}^2 \leq \frac{c_3 \|v_1 - v_2\|_2^2}{n-n_0}.
\end{aligned}$$

根据经验均值的标准估计，我们有

$$\|\hat{\mu} - \mathbb{E}\hat{\mu}\|_2 \leq c_5 \sqrt{\frac{\sum_{j=1}^d \Delta_j^2 + t^2 \max_{j\in[d]} \Delta_j^2}{n-n_0}} \tag{4.46}$$

$$\overset{(4.43)}{\leq} \sqrt{\frac{\sum_{j=1}^d [Q_{1-\varepsilon/2}(\langle X_i, e_j\rangle) - Q_{\varepsilon/2}(\langle X_i, e_j\rangle)]^2}{n}} \tag{4.47}$$

$$+ t \frac{\max_{j\in[d]} [Q_{1-\varepsilon/2}(\langle X_i, e_j\rangle) - Q_{\varepsilon/2}(\langle X_i, e_j\rangle)]}{\sqrt{n}}, \tag{4.48}$$

以至少$1 - 2\exp(-t^2)$的概率。我们令$t = \sqrt{\log d}$，从而得到

$$\|\hat{\mu} - \mathbb{E}\hat{\mu}\|_2 \tag{4.49}$$

$$\leq c_6 \sqrt{\frac{\sum_{j=1}^d [Q_{1-\varepsilon/2}(\langle X_i, e_j\rangle) - Q_{\varepsilon/2}(\langle X_i, e_j\rangle)]^2}{n}} \tag{4.50}$$

$$+ \max_{j\in[d]} [Q_{1-\varepsilon/2}(\langle X_i, e_j\rangle) - Q_{\varepsilon/2}(\langle X_i, e_j\rangle)] \sqrt{\frac{\log d}{n}} \tag{4.51}$$

以至少$1 - \frac{2}{d}$的概率成立。将 (4.44) 和 (4.49) 代入 (4.40) 即得结论。

次高斯情形与 (4.20)–(4.21) 有些类似。事实上，令Σ_{jj}为j协方差矩阵的第 -th 个对角元素，其中协方差矩阵对应于X，并注意到

$$\begin{aligned}
&\varepsilon \max \left| \{ -Q_{1-\varepsilon/2}(\langle \overline{X}, e_j\rangle), Q_{3\varepsilon/2}(\langle \overline{X}, e_j\rangle) \} \right| + \mathcal{E}(\langle \overline{X}, e_j\rangle; 2\varepsilon) \\
&\leq c_7 \varepsilon \sqrt{\Sigma_{jj} \log(1/\varepsilon)} \\
&\text{and that,} \\
&Q_{1-\varepsilon/2}(\overline{X}_j) - Q_{\varepsilon/2}(\overline{X}_j) \leq c_8 \sqrt{\Sigma_{jj} \log(1/\varepsilon)}.
\end{aligned}$$

将它们代入公式（4.46），可得

$$\|\hat{\mu} - \mu\|_2 \leq c_9 \left(\varepsilon \sqrt{\log(1/\varepsilon) \operatorname{Tr}(\Sigma)} + \sqrt{\frac{\log(1/\varepsilon) \operatorname{Tr}(\Sigma) + \log(d) \log(1/\varepsilon) \|\Sigma\|}{n}} \right)$$

其成立的概率至少为 $1-4d\exp(-c_1\varepsilon n_0)-\frac{2}{d}$。现在令 $n_0=\sqrt{n}\log d$ 和 $\varepsilon=\frac{c_{11}}{\sqrt{n}}$，其中 c_{11} 足够大，我们得到

$$\|\hat{\mu}-\mu\|_2 \le c_{12}\sqrt{\frac{\log(n)\,\mathrm{Tr}(\Sigma)+\|\Sigma\|\log(n)\log(d)}{n}} \tag{4.52}$$

以至少 $1-\frac{6}{d}$ 的概率成立。通过重新缩放 d 和绝对常数，我们完成证明。□

正如第 3 节末尾所指出的那样，当数据受到对抗噪声污染时，经验均值估计量似乎无法达到快速收敛速率。为了解决这一问题，我们将 Depersin 和 Lecue 提出的估计量与一维情形下的抽样策略相结合，以避免用于计算经验分位数的 n_0 个样本中出现过多受污染样本。

回想一下，我们从总共 n_0 个样本 $Y_1,\dots,Y_{n_0}$ 中无放回地均匀随机抽取 n 个样本 $X_1,\dots,X_n$。接下来，我们重复定理 4.3 中的相同步骤，

$$\alpha_j=\langle Y,e_j\rangle^*_{\varepsilon n_0} \quad \text{and} \quad \beta_j=\langle Y,e_j\rangle^*_{(1-\varepsilon)n_0},$$

并像之前一样计算量 $\alpha=(\alpha_1,\cdots\ \alpha_d)^\top$, $\beta=(\beta_1,\cdots\ \beta_d)^\top$, μ_1 和 Δ。量化方案也保持不变

$$\dot{X}_i=\mathrm{sign}(X_i-\mu_1+\mathrm{Diag}(\Delta)\tau_i), \tag{4.53}$$

然而，估计量会发生变化。令 $\widehat{\mu}_{DL}$ 为命题 3.4 中的估计量，将其应用于样本 $\mathrm{Diag}(\Delta)X_1$、$\cdots$ 和 $\mathrm{Diag}(\Delta)X_n$，并考虑如下估计量：

$$\widehat{\mu}=\widehat{\mu}_{DL}+\mu_1. \tag{4.54}$$

定理4.5 (多变量污染情形)。存在绝对常数 $C,c_1,c_2,c_3>0$，使得以下结论成立。假设样本中有 η 的比例受到污染，其中 $\eta<1/8$。考虑上述参数为 $n_0\le\frac{n}{2}$ 和 $\varepsilon>0$ 的量化与估计过程。那么，对于 $\varepsilon\ge 8\eta$，以至少 $1-d\exp(-c_1\varepsilon n_0)-\frac{1}{d}$ 的概率，有

$$\begin{aligned}\|\hat{\mu}-\mu\|_2 \le c_2&\left(\sum_{j=1}^d \mathcal{E}(\overline{X}_j;2\varepsilon)^2+\varepsilon^2\max\left\{-Q_{1-\varepsilon/2}(\langle\overline{X},e_j\rangle),Q_{3\varepsilon/2}(\langle\overline{X},e_j\rangle)\right\}^2\right)^{1/2}\\ &+c_2\sqrt{\frac{\sum_{j=1}^d[Q_{1-\varepsilon/2}(\langle X_i,e_j\rangle)-Q_{\varepsilon/2}(\langle X_i,e_j\rangle)]^2}{n}}\\ &+c_2\max_{j\in[d]}[Q_{1-\varepsilon/2}(\langle X_i,e_j\rangle)-Q_{\varepsilon/2}(\langle X_i,e_j\rangle)]\sqrt{\frac{\log d}{n}+\eta}.\end{aligned}$$

具体而言，对于 $n_0 = \sqrt{n}\log d$和 $\varepsilon = \max\{8\eta, \frac{c_3}{\sqrt{n}}\}$，如果 X是 K-次高斯的，那么以至少$1 - \frac{1}{d}$的概率，

$$\|\hat{\mu} - \mu\|_2 \leq CK\log(n)\sqrt{\frac{\mathrm{Tr}(\Sigma) + \|\Sigma\|\log(d)}{n} + \|\Sigma\|\eta}. \tag{4.55}$$

证明。 我们对 $X, e_1\rangle \ldots, \langle X, e_d\rangle$应用用于推导类似于（4.36）和（4.35）的估计的相同论证。因此，根据简单的并集界，我们得到以至少 $1 - 4de^{-\varepsilon n_0} - de^{-0.1\varepsilon n_0}$的概率，对每个$i \in [d]$,

$$\begin{aligned}
&Q_{1-2\varepsilon}(\langle X, e_i\rangle) \leq \beta_i \leq Q_{1-\varepsilon/2}(\langle X, e_i\rangle).\\
&Q_{\varepsilon/2}(\langle X, e_i\rangle) \leq \alpha_i \leq Q_{2\varepsilon}(\langle X, e_i\rangle)\\
&Q_{\varepsilon/2}(\langle X, e_i\rangle) \leq \Delta_i \leq Q_{1-\varepsilon/2}(\langle X, e_j\rangle).
\end{aligned}$$

在证明的其余部分，我们以此前估计成立这一事件为条件。根据三角不等式

$$\begin{aligned}
\|\widehat{\mu} - \mu\|_2 &\leq \|\widehat{\mu} - \mu_1 - \mathbb{E}\,\mathrm{Diag}(\Delta)\dot{X}\| + \|\mu - \mathbb{E}\,\mathrm{Diag}(\Delta)\dot{X} + \mu_1\|_2\\
&= \|\widehat{\mu}_{DL} - \mathbb{E}\,\mathrm{Diag}(\Delta)\dot{X}\| + \|\mu - (\mathbb{E}\,\mathrm{Diag}(\Delta)\dot{X} + \mu_1)\|_2,
\end{aligned}$$

其中，第二项可以使用定理 4.4 证明中的相同论证进行估计。为处理右侧的第一项，首先要注意，$\mathrm{Diag}(\Delta)X$ 是一个随机向量，其协方差矩阵为对角矩阵，对角元素为 $\Delta_1^2, \ldots, \Delta_d^2$。第二个观察是，均值估计器 $\widehat{\mu}_{DL}$ 的输入由 $n - n_0$ 个样本组成，其中至多有 ηn 被污染。因此，在 $n_0 = o(n)$ 的情形下，只要 $2\eta(n - n_0)$ 足够大，至多 n个样本会被破坏。因此，根据命题3.4 ，对于置信区间 $\delta \asymp d^{-1}$的选择，我们得到以概率 $1 - d^{-1}$

$$\|\widehat{\mu}_{DL} - \mathbb{E}\,\mathrm{Diag}(\Delta)\dot{X}\|_2 \leq C\left(\max_{j\in[d]}\Delta_j\sqrt{\frac{\log(d)}{n} + \eta} + \sqrt{\frac{\sum_{j=1}^d \Delta_j^2}{n}}\right),$$

对于某个绝对常数 $C > 0$。回想以下适用于所有指标的估计式 $Q_{\varepsilon/2}(\langle X, e_i\rangle) \leq \Delta_i \leq Q_{1-\varepsilon/2}(\langle X, e_j\rangle$，即可得到证明。第二部分只需应用定理4.4末尾使用的针对次高斯分布的相同估计式。

□

5 数值示例

本节展示数值实验，以支持我们的理论发现。我们重点关注第 4 节中针对部分量化情形提出的估计量，因为它们在实践中最为相关。唯一的

例外是，我们考虑图 5 中的分布式设置，其目标是给出一个否定性结论。结果中的每个数据点都是对 100次独立试验取平均得到的。用于复现模拟的代码可在此处获取：

https://github.com/junrenchen58/one-bit-mean

我们从定理 4.1 中的无噪声单变量设定开始。具体而言，我们针对 n 个独立同分布的 N (100, 1) 样本进行均值估计。在我们的估计量中，我们大致遵循定理中的参数来选择$n_0 = \lceil \sqrt{n} \rceil$ 和 $\varepsilon = \sqrt{2}/n$。没有量化时，我们将经验均值 $\bar{\mu} = \frac{1}{n}\sum_{i=1}^{n} X_i$ 作为衡量所提出估计量性能的基准。对于不同的样本量 $n \in \{50, 100, 200, 300, 400, 500\}$，我们在图1中绘出了使用公式（4.5）中的所提出（量化）估计量 $\hat{\mu}$以及使用最优估计量 $\bar{\mu}$时得到的误差。值得注意的是，在相同样本量下，使用量化（单比特）均值估计器 $\hat{\mu}$ 得到的误差，在经验上不超过使用最优（未量化）估计量 $\bar{\mu}$所得误差的两倍；也就是说，我们在经验上观察到 $|\hat{\mu} - \mu| \leq 2|\bar{\mu} - \mu|$。此外，我们注意到，当均值为 $\mu = 100$时，我们的估计量仍表现良好；这个值远大于方差 1，证实了第4节提出的方法不依赖于均值位置。

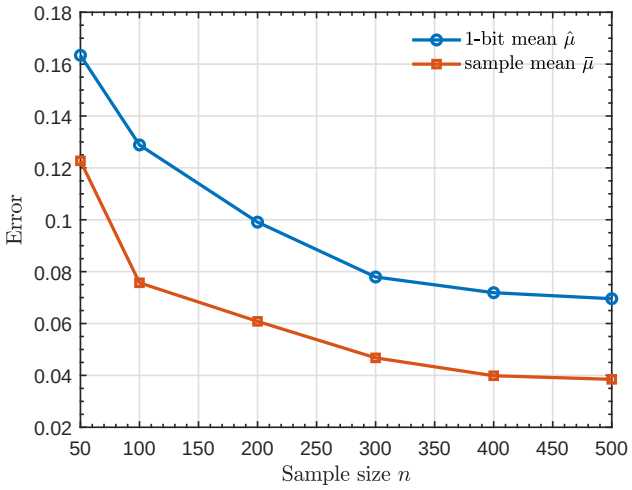

图1：无污染单变量均值估计。

接下来，我们讨论定理4.4中的无污染多变量设定。我们测试对独立同分布的 $\mathcal{N}(100 \cdot \mathbf{1}_d, \Sigma_{\text{Toe}})$ 个样本的均值进行估计，其中 Σ_{Toe}是一个托普利茨协方差矩阵，其第 (i, j) 个元素为 $\frac{1}{2^{|i-j|^{\circ}}}$ 我们测试 $d = 30$ 以及 $n \in \{1200, 1500, 1800, 2100, \text{——} 2400\}$。与此类似，我们比较了公式 (4.38) 中参数为 $n_0 = \lceil 2\sqrt{n} \rceil$的单比特估计器 $\hat{\mu}$ —

以及 $\varepsilon = \frac{3}{\sqrt{n}}$ 与经验均值 $\bar{\mu} = \frac{1}{n}\sum_{i=1}^{n} X_i$进行比较。结果如图 2所示。

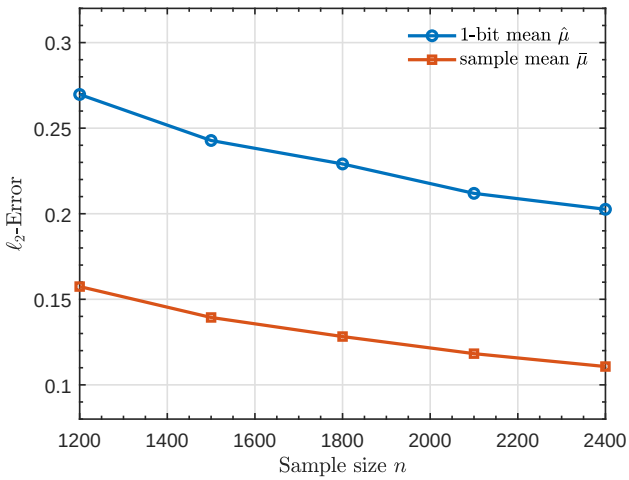

图 2：各向同性协方差下的无污染多元均值估计。

我们的结果所针对的一个更具挑战性的情形是高维情形：此时维度 d与样本量 n相当，但协方差矩阵 Σ 具有低秩特征，例如，其迹随维度缓慢增长。特别地，公式（4.39）中推导的收敛速率随协方差矩阵的迹 $\mathrm{Tr}(\Sigma)$变化，且对维度 d仅呈对数依赖。为刻画这一情形，我们在 $X \sim \mathrm{N}(100 \cdot \mathbf{1}_d, \Sigma_d)$（$d = n/10$）下检验均值估计问题，样本量为 $n \in \{200, 400, 600, 800, 1000\}$。环境维度 d 和样本量 n同时增加，且比值 $\frac{d}{n}$ 保持不变。对于给定的 d，我们通过从中采样生成协方差矩阵Σ_d

$$\Sigma_d = O^T \,\mathrm{Diag}([1^{-2}, 2^{-2}, 3^{-2}, \cdots, d^{-2}])O,$$

其中，O 取自正交变换群的哈尔测度。

因此，$\mathrm{Tr}(\Sigma_d) = \sum_{i=1}^{d} i^{-2}$ 会随 d 缓慢增加；在我们的设定中，$\mathrm{Tr}(\Sigma_{d=20}) = 1.5962$ 和 $\mathrm{Tr}(\Sigma_{d=100}) = 1.6350$ 非常接近。图3 所示结果展示了我们的单比特估计器所具有的（近似）无维数依赖行为，尤其是，误差会随着 n 而减小，尽管 d同时增大。值得注意的是，与前两次模拟一样，我们的单比特估计器的误差通常不会超过样本均值误差的两倍。

我们方法的另一个重要特点是能够抵御对抗性污染，这一点在此前关于量化下均值估计的研究中并未考虑。

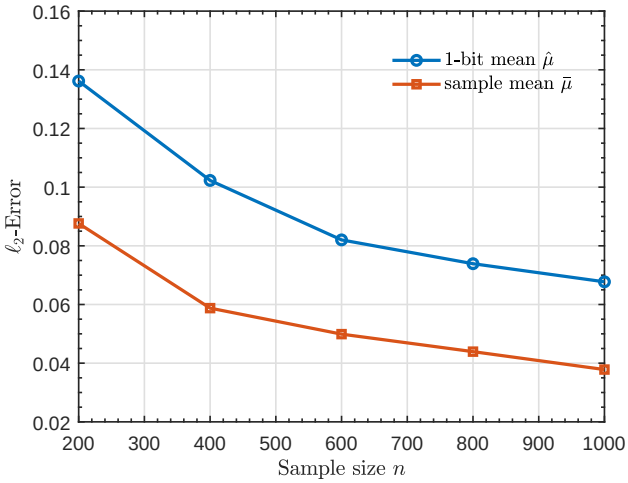

图 3：低迹 $\mathbf{Tr}(\Sigma)$ 下的多元均值估计。

为通过实证说明这一点，我们考虑定理4.3中更为微妙的情形，其中 $\lfloor \eta n \rfloor$ 对抗性污染发生在抽取 $\mathbf{X}^{(\mathrm{f})}$之前。我们模拟从 $\mathbf{N}(\mu = 100, 1)$ 分布中抽取 $n = 1000$ 个样本进行均值估计，并特别测试这样一种污染：将 $\{X_i\}_{i=1}^n$ 中最大的 ηn 个样本替换为相对于 μ 的对称值，即将 X_i 改为 $2\mu - X_i$。请注意，单变量均值估计中的样本量相对较大，因此公式（4.31）中误差率的噪声项$O(\eta\sqrt{\log(1/\eta)})$ 应占主导地位。在我们的估计量 $\hat{}\mu$ 中，我们令 $n_0 = \lceil \sqrt{n_0} \rceil$，并通过无放回抽样均匀抽取大小为 n_0 的 $\mathbf{X}^{(\mathrm{f})}$。我们还令 $\varepsilon = \eta + 1/\sqrt{n}$，并计算 $\mathbf{X}^{(\mathrm{f})}$ 的 ε 和 $1-\varepsilon$ 分位数。我们将把我们的估计量与（未量化的）截尾均值 [22] 进行比较；该方法计算 $\{X_i\}_{i=1}^{\xi n}$ 的 ε' 和 $1-\varepsilon'$ 分位数，分别记为 α' 和 β'，然后利用剩余的 $(1-\xi)n$ 个样本 $\{X_i\}_{i=\xi n+1}^n$ 来估计均值，具体如下：

$$\bar{\mu}_{\mathrm{trim}} = \frac{1}{(1-\xi)n} \sum_{i=\xi n+1}^{n} \phi_{\alpha'}^{\beta'}(X_i). \tag{5.1}$$

我们将 $\varepsilon' = \eta + 1/\sqrt{n}$ 设定为与单比特估计器中相同。在原论文 [22],中，作者将 $\xi = 1/2$设为此值，因此只使用一半的样本来构造估计量；但在实践中，这可能会过度影响收敛速率。在我们的实验中，我们使用 $\xi \in \{0.1, 0.2, 0.3, 0.4, 0.5\}$ 测试截尾均值，并记录每次独立试验中的最小误差。我们展示了 $\eta = 0.005$: $0.005 : 0.2$ 条件下的误差曲线，见图4。值得注意的是，我们的 $\hat{}\mu$的误差与 $\bar{\mu}_{\mathrm{trim}}$非常接近。

对抗性污染下的多变量情形要复杂得多。事实上，定理3.5 和4.5 依赖于所提出的估计量 [9]

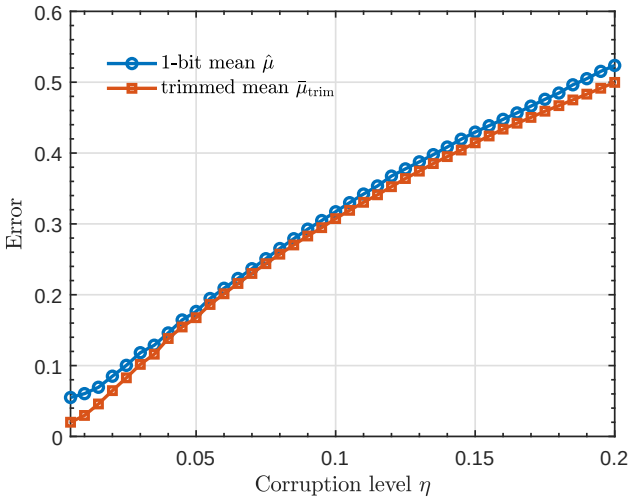

图4：鲁棒单变量均值估计。

以达到阶为 $O(\sqrt{\|\Sigma\|}\eta)$的收敛速率。尽管他们的工作中提出的算法具有多项式时间运行时间，但在实践中并没有高效的代码。定理中的常数可能过大，不适用于实际应用。我们将其留作一个重要的开放问题。

最后，我们通过实验说明，在对抗性污染下，直接取量化样本的经验均值这一自然选择并不能达到快速收敛速率。为简单起见，我们考虑定理 3.2 中的完全量化设置。我们从 $\mathrm{N}(0, I_d)$ 中生成 n 个独立同分布样本，并设置抖动级别为 $\lambda_1 = \cdots = \lambda_d = 2$。我们通过测试 $d = 10 : 10 : 100$，在 $n = 100 \cdot d$ 下固定比率 $\frac{d}{n} = \frac{1}{100}$。请注意，我们的结果中无污染情形下的误差速率按 $\tilde{O}(\sqrt{d/n})$ 缩放，因此在没有污染时，误差应大致保持不变。在存在污染的情况下，正如定理 3.2 后的说明所述，一个简单的论证可将误差增量控制在 $O(\eta\sqrt{d})$。在实验中，我们测试 $\eta = 0.05$ 和 0.10；污染模式为均匀随机选取 ηn 个样本，将其 X_i的改为 $X_i := X_i + \mathbf{1}_d$。图5中的“误差与维度”曲线证实，定理 3.2 中简单估计量的误差会随 d增大。

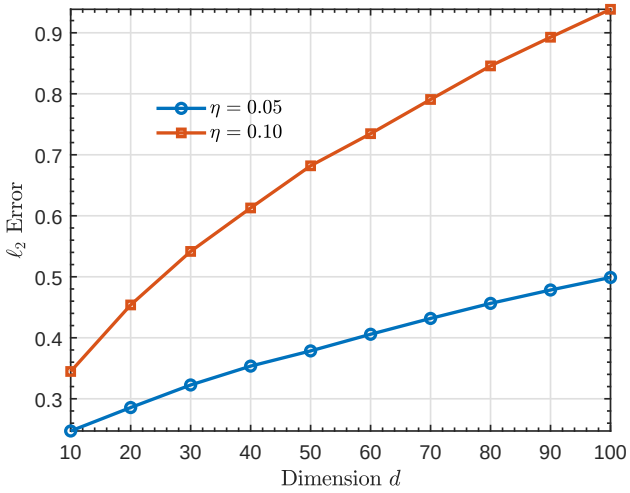

图5：经验均值不具备强鲁棒性。

致谢

P.A. 获得了美国国家科学基金会和西蒙斯深度学习理论基础合作项目的支持。J.C. 获得了马里兰大学数学系诺维科夫博士后奖学金的支持。本研究的部分工作是在 J.C. 任职于香港大学并访问加州大学尔湾分校期间完成的。J.C. 感谢 R. Vershynin 和 Y. He 的热情接待及富有启发性的讨论。

参考文献

[1] Pedro Abdalla 和 Nikita Zhivotovskiy。协方差估计：针对对抗性污染和重尾的最优无维度保证。《欧洲数学学会杂志》，2024 年。[2] Jayadev Acharya、Clement Canonne、Yuhan Liu、Ziteng Sun 和 Himanshu Tyagi。每个用户拥有多个样本时的分布式估计：精确速率与相变。神经信息处理系统进展，34：18920–18931，2021 年。[3] Chen Amiraz、Robert Krauthgamer 和 Boaz Nadler。采用次线性通信的分布式稀疏正态均值估计。*IMA*《信息与推断》，11(3)：1109–1142，2022 年。[4] T Tony Cai 和 Hongji Wei。未知方差下的分布式自适应高斯均值估计：交互式协议有助于实现自适应。《统计学年鉴》，50(4)：1992–2020，2022 年。

[5] T Tony Cai 和 Hongji Wei。通信约束下的分布式高斯均值估计：最优速率与高通信效率算法。机器学习研究杂志，25(37)：1–63，2024 年。[6] Hao Chen 和 Pramod K Varshney。采用相同一比特量化器的分布式估计系统的性能极限。*IEEE*《信号处理汇刊》，58(1)：466–471，2009 年。[7] Junren Chen 和 Michael K Ng。一种参数无关的二比特协方差估计器，具有更优的算子范数误差率。应用与计算调和分析，第 101774 页，2025 年。[8] Junren Chen、Cheng-Long Wang、Michael K Ng 和 Di Wang。均匀抖动一比特量化下的高维统计估计。*IEEE* 信息论汇刊，69(8)：5151–5187，2023 年。[9] Jules Depersin 和 Guillaume Lecu´e。近线性时间内对均值向量进行稳健次高斯估计。《统计学年鉴》，50(1)：511–536，2022 年。[10] Ilias Diakonikolas 和 Daniel M Kane。算法高维稳健统计。剑桥大学出版社，2023 年。[11] Sjoerd Dirksen 和 Johannes Maly。利用数据驱动抖动进行免调参的一比特协方差估计。*IEEE* 信息论汇刊，70(7)：5228–5247，2024 年。[12] Sjoerd Dirksen、Johannes Maly 和 Holger Rauhut。一比特量化下的协方差估计。《统计学年鉴》，50(6)：3538–3562，2022 年。[13] Sjoerd Dirksen 和 Shahar Mendelson。非高斯超平面镶嵌与稳健一比特压缩感知。《欧洲数学学会杂志》，23(9)：2913–2947，2021 年。[14] Sjoerd Dirksen、Shahar Mendelson 和 Alexander Stollenwerk。随机超平面镶嵌的精确估计。*SIAM*《数据科学数学杂志》，4(4)：1396–1419，2022 年。[15] Wassily Hoeffding。有界随机变量之和的概率不等式。美国统计学会杂志，58(301)：13–30，1963 年。[16] Peter J Huber。1972 年沃尔德讲座：稳健统计综述。数学统计年鉴，第 1041–1067 页，1972 年。

[17] Alon Kipnis 和 John C Duchi。基于单比特测量的均值估计。*IEEE* 信息论汇刊，68(9):6276–6296，2022。[18] Ritesh Kumar 和 Shashank Vatedka。未知方差下的单比特分布式均值估计。*arXiv* 预印本 *arXiv:2501.18502*，2025。[19]Ivan Lau 和 Jonathan Scarlett。具有近乎最优样本复杂度的序贯单比特均值估计。*arXiv* 预印本 *arXiv:2509.21940*，2025。[20] G´abor Lugosi。组合统计学讲义。第*47*届概率暑期学校，圣弗卢尔，第1–91页，2017。[21] G´abor Lugosi 和 Shahar Mendelson。关于一般范数的近乎最优均值估计量。概率论及相关领域，175(3):957–973，2019。[22] G´abor Lugosi 和 Shahar Mendelson。鲁棒多变量均值估计：截尾均值的最优性。《统计学年鉴》，49(1):393–410，2021。[23]Mayank Shrivastava、Berivan Isik、Qiaobo Li、Sanmi Koyejo 和 Arindam Banerjee。分布式深度学习的草图化：更精确的分析。《神经信息处理系统进展》，37:6417–6447，2024。[24] Ananda Theertha Suresh、Ziteng Sun、Jae Ro 和 Felix Yu。用于分布式均值估计与优化的相关量化。载于国际机器学习会议，第20856–20876页。PMLR，2022。[25]Christos Thrampoulidis 和 Ankit Singh Rawat。针对次高斯测量与抖动量化的广义套索。*IEEE* 信息论汇刊，66(4):2487–2500，2020。[26] Aditya Vempaty、Hao He、Biao Chen 和 Pramod K Varshney。传感器网络中分布式贝叶斯估计的量化器设计。*IEEE* 信号处理汇刊，62(20):5359–5369，2014。[27]Parvathinathan Venkitasubramaniam、Lang Tong 和 Ananthram Swami。分布式估计中的极大极小 ARE 量化。*IEEE* 信号处理汇刊，55(7):3596–3605，2007。[28] Roman Vershynin。高维概率：数据科学中的应用导论，第47卷。剑桥大学出版社，2018。

[29] Chunlei Xu 和 Laurent Jacques. 使用 RIP 矩阵的量化压缩感知：抖动的优势。*Information and Inference: AJournal of the IMA*，9(3):543–586，2020。