arXiv:2303.04288v2 [stat.ML] 7 Jun 2023

无界高斯混合模型的多项式时间与私有学习

Jamil Arbas* Hassan Ashtiani† Christopher Liaw‡

2023年6月9日

我们研究如何私密估计 d维高斯混合模型的参数（GMM），其中包含 k 个分量。为此，我们提出一种技术，将该问题归约为其非私有对应问题。这使我们能够以黑盒方式将现有的非隐私算法改造为私有算法，而样本复杂度和运行时间仅略有增加。作为我们框架的主要应用，我们基于 Moitra & Valiant 的非隐私算法 (ε, δ) 作为黑盒，开发了一种差分隐私算法，用于学习高斯混合模型 [MV10] 。因此，我们给出了首个样本复杂度上界，并提出了首个多项式时间算法，可在不对参数作任何有界性假设的情况下私密学习高斯混合模型。在分析过程中，我们还证明了高维高斯分布全变差距离的一个紧下界（相差至多一个常数因子），这一结果本身也可能具有独立的研究价值。

1 引言

学习高斯混合模型（GMM）参数是统计学中的一个基本问题，其研究可追溯到 Pearson 的早期工作 [Pea 94] 。具有 k 个分量、维度为 d 的 GMM 可表示为 $(w_i, \mu_i, \Sigma_i)_{i=1}^k$，其中 w_i 是混合权重（$w_i \geq 0$，且 $\sum_{i\in[k]} w_i = 1$），$\mu_i \in \mathbb{R}^d$ 是均值，而 $\Sigma_i \in \mathbb{R}^{d\times d}$ 是协方差矩阵（对应第 i 个高斯分量）。要从该 GMM 中随机抽取一个样本，首先以概率 w_i 抽取一个索引 $i \in [k]$，然后从高斯分布 $\mathcal{N}(\mu_i, \Sigma_i)$ 中随机抽取一个样本。本文研究大概近似正确（PAC）模型下的参数估计问题，其目标是仅凭来自未知 GMM 的独立样本，“近似恢复”[1] 其参数。

关于高斯混合模型参数学习的样本复杂度和计算复杂度，已有大量研究。这一研究方向的一项突破，是开发出针对高斯混合模型的多项式时间方法（关于 d），且只需满足最小分离要求 [MV10；BS10]。这些方法的运行时间和样本复杂度呈指数级增长 k，而这对于参数估计通常是必要的 [MV10]。

然而，上述方法可能无法保护参与估计的数据个体的隐私。为了解决这一问题，我们采用严格且广受认可的差分隐私（DP）概念 [DMNS06]。从高层次来看，差分隐私确保每个个体的贡献对估计器输出的影响都很小（不可区分）。然而，经典的 ε-DP（纯差分隐私）概念相当严格。例如，即使是估计无界单变量高斯随机变量的均值

*麦克马斯特大学，arbasj@mcmaster.ca。
†麦克马斯特大学，zokaeiam@mcmaster.ca。Hassan Ashtiani 也是 Vector 研究所的教职关联成员。
‡谷歌，cvliaw@google.com[1]精确的距离定义请参见1.4。

在此模型中也是不可能的。因此，遵循近期关于无界域私有估计的研究，我们考虑(ε, δ)-DP（即近似差分隐私 [DKMMN06]）模型。

对于更简单的多元高斯分布情形（参数不受任何有界性假设限制），已有研究证明，只需有限数量的样本，就能在(ε, δ)-差分隐私模型 [AAK21]下实现学习。近期，研究者针对同一任务设计了计算高效估计器 [AL22；KMSSU22；KMV22]。这就引出了一个关于高斯混合模型的相应问题。

> 是否存在一个（ε， δ）-差分隐私估计器，能够以有界的样本复杂度学习无界高斯混合模型？对于同一任务，是否存在一个关于 d 的多项式时间估计器？

请注意，如果对高斯混合模型额外作出有界性[2] 和强分离[3] 假设，那么 Kamath 等人 [KSSU19] 的工作为上述问题在 ε-差分隐私模型下给出了肯定答案。研究还表明，分量之间的分离条件可以显著放宽 [CKMST21；CCdEIST23]。不过，我们的目标是在最少分离假设下学习无界高斯混合模型。

为了解决这个问题，自然会问：是否存在一种通用归约，能将高斯混合模型的私有学习转化为其非私有对应问题？如果存在，我们就能轻松复用现有的高斯混合模型非私有学习结果。

> 是否存在一种从高斯混合模型的私有学习到非私有学习的归约，且只会带来多项式时间和多项式样本开销？

本文的主要结果是证明了这种归约的存在；严格表述见定理 6.2 。

定理 1.1 (**高斯混合模型的私有到非私有归约，非正式表述**)。 存在一种归约，能将 (ε, δ)-差分隐私模型下的高斯混合模型参数学习转化为其非私有对应问题。此外，该归约带来的时间和样本开销相对于 d 和 k而言都仅为多项式级别。

该归约结合 Moitra & Valiant 的非私有学习器 [MV10] ，给出了在 (ε, δ)-差分隐私模型下学习无界高斯混合模型参数的首个有限样本复杂度上界。此外，所得估计器基本继承了 Moitra & Valiant 的非私有估计器[MV10]的所有性质；对于固定的 d (k)，其运行时间为多项式级别，并且同样只要求对高斯混合模型的分量作出可证明的最小可分性假设。关于与 Cohen 等人 [CKMST21] 以及 Chen 等人 [CCdEIST23]的比较，请参阅相关工作一节。

1.1 相关工作

单个高斯分布的私有学习。Karwa 与 Vadhan [KV17] 在纯差分隐私和近似差分隐私设定下，均提出了用于学习一元高斯分布均值和方差的多项式时间且样本高效方法。具体而言，在(ε, δ)-差分隐私设定下，他们无需对参数作任何有界性假设，即可恢复该高斯分布的均值和方差。这一结果可推广至多元情形 [KLSU19；BDKU20], ，其中可找到在全变差距离意义下逼近底层高斯分布的高斯分布。然而，这些方法的样本复杂度依赖于协方差矩阵的条件数，并且需要参数范围的先验界。首个用于私有学习无界高斯分布的有限样本复杂度界出现在 [AAK21],中，且几乎匹配 [KMS22]的样本复杂度下界。 [AAK21] 的工作依赖于最小距离估计器的私有版本 [Yat85] ，并基于隐私假设选择的思想

[2]他们假设存在已知量 $R, \sigma_{max}, \sigma_{min}$， 使得 $\forall i \in [k], \|\mu_i\|_2 \leq R$ 且 $\sigma_{min}^2 \leq ||\Sigma_i|| \leq \sigma_{max}^2$。 [3]他们假设 $\forall i \neq j$, $||\mu_i - \mu_j||_2 \geq \tilde{\Omega}\left(\sqrt{k} + \sqrt{\frac{1}{w_i} + \frac{1}{w_j}}\right) \cdot \max\left\{||\Sigma_i^{1/2}||, ||\Sigma_j^{1/2}||\right\}$。

方法 [BSKW19]。然而，该方法并非计算高效。最近，若干论文提出了用于学习无界高斯分布的 (ε, δ)-差分隐私且计算高效算法 [AL22; KMSSU22; KMV22], ，其中 Ashtiani & Liaw 的工作 [AL22] 在该任务上实现了近乎最优的样本复杂度。Ashtiani & Liaw 的方法 [AL22] 的一部分是子采样与聚合方案，我们在本文中对其进行了修改并加以使用。FriendlyCore [TCKMS22] 是另一种可用于私有学习无界高斯分布的采样与聚合框架。值得注意的是， [AL22; KMV22] 的方法同样适用于鲁棒设定，尽管其样本复杂度并非最优。Alabi 等人近期的工作 [AKTVZ22] 提出了一种在维度方面具有近乎最优样本需求的鲁棒私有学习器。最后，Hopkins 等人 [HKMN23] 面面俱到，提出了一种样本复杂度近乎最优、鲁棒且高效的无界高斯分布学习器。

另一项相关成果是在 ε-差分隐私模型 [HKM22]下，提出了一种样本高效且计算高效的方法，用于学习有界高维高斯分布。另有研究探讨了关于马氏距离的隐私均值估计问题 [BGSUZ21；DHK23]。寻找隐私保护且具备鲁棒性的估计量 [LKKO21] ，以及鲁棒性与隐私之间的相互作用 [DL09；GH22；LKO22；HKMN23；AUZ23] ，是近期若干论文的研究主题。

具有 PAC 保证的高斯混合模型参数学习。给定来自高斯混合模型的独立同分布样本，我们能否近似恢复其参数？研究者已广泛探索如何开发样本高效且计算高效的方法来学习高斯混合模型的参数 [Das99; SK01; VW04; AM05; BV08; KMV10; FSO06; BS09; HP14; HK13; ABGRV14; RV17; KSS18; HL18; LL22]。值得注意的是，Moitra & Valiant [MV10] 和 Belkin & Sinha [BS10] 提出了首批多项式时间算法，能够在最小分离假设下学习具有无界分量的一般高斯混合模型。本文关注设计关于维度的多项式方法，因为对分量数量呈指数依赖是不可避免的 [MV10] （除非各分量之间分离良好）。近期，这些结果已扩展至鲁棒设定 [BDJKKV22; LM21; LM22]。

在隐私设定下，Nissim、Raskhodkarana 与 Smith 的早期工作 [NRS07] 提出了一种 (ε, δ)-差分隐私估计器，用于估计高斯混合模型的均值；该方法适用于各分量具有相同混合权重和相同（已知）协方差矩阵这一特殊情形。请注意，该结果也沿用了 Vempala & Wang [VW04]对高斯分量之间强分离（$\Omega(k^{1/4})$）的假设。Chen 等人 [CCdEIST23] 近期独立开展的工作表明，这一分离要求可以大幅放宽。不过，这些结果针对的是无界球形高斯混合分布的学习，与我们的工作不同，它们并不学习协方差矩阵。

与本文更相关的或许是 Kamath 等人 [KSSU19], 提出的方法，该方法提供了一种 (ε, δ)-差分隐私参数学习方法，可用于混合权重、均值和协方差矩阵均未知的高斯混合模型。事实上，他们的方法是对 Achlioptas 与 McSherry [AM05]方法的隐私化版本。然而，该方法仅在高斯分量的参数有界且均值充分分离（即分离程度为 $\Omega(\sqrt{k})$）时才有效。在一项相关工作中，Bie、Kamath 与 Singhal [BKS22] 展示了如何利用公开数据改进这一方法。

最后，Cohen 等人近期的工作 [CKMST21] 改进了 Kamath 等人 [KSSU19] 的结果，提供了更好的样本复杂度，并降低了对簇间分离程度的要求。他们证明，如果具备以下条件，就可以私有地学习高斯混合模型：（*i*）一个用于学习高斯分布的私有学习器；以及（*ii*）一种非私有聚类方法（即一种能够根据数据点所属的簇准确标记数据点的算法）。鉴于其归约方法具有普适性，可以接入一种对分量间分离程度要求更低的非私有聚类方法。除了聚类方法本身的分离要求外，他们的结果还要求均值之间的分离程度至少为$\Omega(\log n)$。其中， n 是样本数。鉴于 n 关于$1/\varepsilon$呈多项式增长， k 并且 d，他们的方法只要求适度的分离程度（即关于这些参数呈对数级增长）。

与 Kamath 等人 [KSSU19] 和 Cohen 等人 [CKMST21], 不同，我们的方法不需要预先给定高斯分布均值范围或协方差矩阵条件数的界限。它

或许可以将 Cohen 等人 [CKMST21] 的结果扩展到无界情形，例如使用 Ashtiani & Liaw [AL22]提出的私有高斯估计器；但当高斯分量的条件数较高时，聚类会面临一些微妙的挑战。另一个差异在于分离要求。Cohen 等人[CKMST21] 放宽了 Kamath 等人 [KSSU19],提出的分离要求，但仍要求分量之间具有（温和的）$\log(kd/\varepsilon)$ 分离。此外，非私有聚类方法要发挥作用，还必须满足额外的分离要求。对于球形高斯分布，这一要求相当宽松（即 $\sqrt{\log k}$ 分离 [LL22], ）；而据我们所知，目前没有适用于非球形高斯分布且只要求弱分离的方法（例如，要求与高斯分量的条件数无关）。相比之下，我们的方法采用非私有参数估计（而非聚类），只要求“最小分离”，且该要求与 ϵ, k, d 无关（参见定义 6.4）。

GMM 密度估计。 在高斯混合模型的密度估计问题中，目标是恢复一个与底层高斯混合模型接近（通常以全变差距离衡量）的分布。从统计角度来看，该问题的样本复杂度已得到解决，误差仅差对数因子 [DL01; ABM18 ; ABHLMP18 ; ABHLMP20]。与参数学习设定不同，样本复杂度关于维度和分量数实际上都是多项式级的。此外，已有用于学习一维高斯混合模型的计算高效算法[CDSS14; ADLS17; LLM22; WX18; LS17]。设计一种关于维度和分量数为多项式时间、且针对全变差距离学习高斯混合模型的算法，仍是一项重要的开放问题。解决这一问题颇具挑战，因为需要克服该问题已知的统计查询下界 [DKS17]。

在隐私设定中，可以使用 Bun 等人的私有假设选择框架 [BSKW19] 或私有最小距离估计器 [AAK21] ，来学习具有有限覆盖的类别。因此，参数有界的高斯混合模型具有 ε-差分隐私有限样本复杂度保证 [BSKW19]。已知在 (ε, δ)-差分隐私模型下，学习轴对齐高斯混合模型存在多项式样本复杂度上界，且 对参数没有任何有界性假设 [AAL21]。将这一结果推广到一般高斯混合模型仍是一个开放问题。此外，即使在一维设定下，为高斯混合模型设计兼具隐私性和计算效率的估计器仍是一个开放问题。另一个相关结果是关于学习协方差矩阵已知的高斯混合模型的样本复杂度下界 [ASZ21]。

1.2 预备知识

我们用 $\|v\|_2$ 表示向量 $v \in \mathbb{R}^d$ 的欧几里得范数，并用 $\|A\|_F$ （分别对应 $\|A\|$）表示矩阵 $A \in \mathbb{R}^{d\times d}$的 Frobenius 范数（分别对应谱范数）。
在本文中，我们用 $\mathcal{S}^d$ 表示 $\mathbb{R}^{d\times d}$中的正定锥。令 $\mathcal{G}(d) = \{\mathcal{N}(\mu, \Sigma) : \mu \in \mathbb{R}^d, \Sigma \in \mathcal{S}^d\}$ 为 d维高斯分布族。现在，我们可以如下定义高斯混合类 $\mathcal{G}(d, k)$。

定义 1.2 （高斯混合）。 $\mathbb{R}^d$ 中 k 个高斯分布的混合类定义为 $\mathcal{G}(d, k) :=$
$\left\{\sum_{i=1}^{k} w_i G_i \ : \ G_i \in \mathcal{G}(d), w_i \geq 0, \sum_{i=1}^{k} w_i = 1\right\}$.

我们用一组 k 元组 $(w_i, \mu_i, \Sigma_i)_{i=1}^k$表示高斯混合模型（GMM），其中每个元组分别表示一个分量的均值、协方差矩阵和混合权重。请注意，在我们的记法中，分量的顺序很重要，因为输出的顺序可能会影响隐私。

在下文的定义及本文其余部分中，我们可能会不严谨地使用术语，通过概率密度函数（p.d.f.）来指代一个分布。

定义 1.3（全变差距离）。给定定义在 $\mathbb{R}^d$ 上的两个绝对连续概率测度 $f(x)$ $g(x)$，f 与 g 之间的全变差（TV）距离定义为 $d_{\mathrm{TV}}(f(x)\ g(x)) = \frac{1}{2}\int_{\mathbb{R}^d} |f(x)\ -g(x)|\,\mathrm{d}x$。

一种标准的定义两个高斯混合模型之间距离的一种标准方式如下（[MV10], 定义 2）。

定义 1.4（两个高斯混合模型之间的距离）。两个高斯混合模型之间的距离定义为

$$\mathrm{dist}_{\mathrm{GMM}}\left((w_i,\mu_i,\Sigma_i)_{i=1}^k,(w_i',\mu_i',\Sigma_i')_{i=1}^k\right) = \min_{\pi}\max_{i\in[k]}\max\left\{|w_i - w'_{\pi(i)}|, d_{\mathrm{TV}}\left(\mathcal{N}(\mu_i,\Sigma_i),\mathcal{N}(\mu'_{\pi(i)},\Sigma'_{\pi(i)})\right)\right\}$$

其中，π 从 $[k]$上的所有排列构成的集合中选取。

如果 X（分别地，Y）是服从 f（分别地，g）分布的随机变量，我们记作 $d_{\mathrm{TV}}(X,Y) = d_{\mathrm{TV}}(f,g)$。当上下文已明确或隐含随机变量的概率密度函数时，我们省略对该概率密度函数的说明。

1.3 差分隐私基础

从高层次来看，如果给定两个仅在单个元素上存在差异的数据集时，算法的输出分布几乎相同[4]，则称该算法是差分隐私的。

定义 1.5（相邻数据集）。设 $\mathcal{X}$、$\mathcal{Y}$ 表示集合，且 $n\in\mathbb{N}$。若两个数据集 $D=(X_1,\ldots,X_n)$ $D'=(X_1,\ldots,X_n)$ $\in\mathcal{X}^n$ 的汉明距离满足 $d_H(D,D')\ \le 1$，则称它们是相邻的，其中 d_H 表示汉明距离，即 $d_H(D,D') = |\{i\in[n]: X_i\neq X_i'\}|$。

定义 1.6（(ε,δ)-不可区分）。设 D、D' 是定义在集合 $\mathcal{Y}$ 上的两个分布。若对于所有可测的 $S\subseteq\mathcal{Y}$、$\mathbb{P}_{Y\sim D}[Y\in S]\le e^{\varepsilon}\mathbb{P}_{Y\sim D'}[Y\in S]+\delta$ 和 $\mathbb{P}_{Y\sim D'}[Y\in S]\le e^{\varepsilon}\mathbb{P}_{Y\sim D}[Y\in S]+\delta$，$D$、$D'$ 均满足 (ε,δ)-不可区分，则称它们是 (ε,δ)-不可区分的。

定义 1.7（(ε,δ)-差分隐私 [DMNS06]）。若随机化机制 $\mathcal{M}$: $\mathcal{X}^n\to\mathcal{Y}$对于所有相邻数据集 $D,D'\in\mathcal{X}^n$，$\mathcal{M}(D)$ 和 $\mathcal{M}(D')$ 均为 (ε,δ)-不可区分，则称其满足 (ε,δ)-差分隐私。

1.4 技术

本文的技术受到 Ashtiani & Liaw [AL22] 的技术启发，这些技术基于提出-测试-发布框架 [DL09] 和子采样-聚合框架 [NRS07]。给定一个数据集 D，我们首先将 D 划分为 t 个子数据集，并在每个子数据集上运行一个非隐私算法 $\mathcal{A}$。接下来，我们以隐私方式检查 $\mathcal{A}$ 的大多数输出是否“良好聚类”（即彼此接近）。如果不是，则算法失败，因为这表明非隐私算法的输出不够稳定（可能是由于数据不足，也可能只是因为非隐私算法对其输入很敏感）。另一方面，如果大多数输出都良好聚类，那么我们就可以聚合这些聚类后的输出，并发布其加噪版本。不过，还需要解决多个额外的技术挑战。

一个核心难题是高斯分量的排序问题。也就是说，非私有高斯混合模型学习器可能会以不同的顺序输出高斯混合模型分量。因此，汇总这些非私有解（例如，按照 Ashtiani & Liaw [AL22] 的方式计算加权平均值）似乎不可能。因此，我们提出完全跳过汇总步骤，只需从

[4]为简化起见，我们假设数据集是有序的，因此邻接数据集是根据其汉明距离定义的。不过，很容易将针对有序情形证明的保证转换为无序情形；参见 [BGSUZ21]。

簇中任意选取一个解。因此，我们的私有众多估计器（PPE）简化并推广了 Ashtiani & Liaw [AL22], 提出的私有众多均值估计器（PPME）框架，使其适用于一般的半度量空间（因此也适用于高斯混合模型）。第 2.1小节将对该框架进行精确讨论。

另一个挑战是设计一种适当的机制，为高斯混合模型添加噪声。如上所述，我们的框架要求能够发布候选输出的含噪输出。更准确地说，给定两个相邻数据集 Y_1，Y_2，我们希望设计一种机制 $\mathcal{B}$，使得 $\mathcal{B}(Y_1)$，$\mathcal{B}(Y_2)$ 在 Y_1，Y_2 足够接近时不可区分。与 Ashtiani & Liaw [AL22], 一样，我们将这种机制称为“掩蔽机制”。在包含 k 个分量的混合分布中，候选输出对应一个 k元组，其中每个元素都包含单个分量的参数和混合权重。我们证明，如果能够为单个分量设计掩蔽机制，那么就可以将该掩蔽机制作为黑盒，以仅增加 k元组运行时间 $\mathrm{poly}(k)$ 的开销，为该 k元组设计掩蔽机制。一个重要步骤是随机打乱各分量，使输出不受分量顺序影响。

与分量顺序有关的另一个挑战是，根据定义 1.4 计算两个高斯混合模型之间的距离时，需要对所有排列取最小值。计算该距离的朴素方法可能需要指数时间，但我们证明，通过简单地归约为二分图匹配，可以在多项式时间内完成这项任务。

为展示上述框架的效用，我们说明，将该框架应用于高斯混合的隐私学习十分直接。我们设计了一种针对单个高斯分量的掩蔽机制，该机制对混合权重、均值和协方差矩阵进行掩蔽。掩蔽混合权重是相当标准的做法，而掩蔽均值和协方差矩阵则可以利用已知结果实现（例如，协方差矩阵可使用 [AL22], 引理 5.2，均值则可采用类似的技术）。

最后，我们指出，在一些关于高斯混合的文献中，结果通常声称，对于每个高斯分量 $\mathcal{N}(\mu, \Sigma)$，算法都会返回 $\hat{\mu}, \hat{\Sigma}$，使得 $\mathcal{N}(\mu, \Sigma)$ 和 $\mathcal{N}(\hat{\mu}, \hat{\Sigma})$ 的全变差距离较小（例如 [MV10]）。我们的框架要求，对于某个适当的范数，$\hat{\mu}$（分别为 $\hat{\Sigma}$）与 μ（分别为 Σ）接近。直观上，这应该成立，但此前尚无紧确刻画，除非这些高斯分布具有相同的均值（[DMR18], 定理 1.1）。本文证明了高斯分布与其参数之间的 TV 距离的以下紧确刻画。我们认为，这一结果本身可能也具有独立的研究价值。

定理 1.8。 设 $\mu_1, \mu_2 \in \mathbb{R}^d$ 和 Σ_1, Σ_2 是 $d \times d$ 正定矩阵。假设我们有 $d_{\mathrm{TV}}(\mathcal{N}(\mu_1, \Sigma_1)\ \mathcal{N}(\mu_2, \Sigma_2)) < \frac{1}{600}$。令

$$\Delta = \max\left\{\|\Sigma_1^{-1/2}\Sigma_2\Sigma_1^{-1/2} - I_d\|_F, \|\Sigma_1^{-1/2}(\mu_1 - \mu_2)\|_2\right\}.$$

Then

$$\frac{1}{200}\Delta \le d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1, \Sigma_1), \mathcal{N}(\mu_2, \Sigma_2)\right) \le \frac{1}{\sqrt{2}}\Delta.$$

注 1.9。 注意，$\mathcal{N}(\mu_1, \Sigma_1)$ 与 $\mathcal{N}(\mu_2, \Sigma_2)$ 之间的全变差距离是对称的（即交换 μ_1, Σ_1 和 μ_2, Σ_2 不会影响全变差距离），而 Δ 的定义则不是。因此，可以自动加强该定理，表明当通过交换Σ_1 和 Σ_2来定义 Δ 时，这些界仍然成立。

2 私有 populous 估计器

本节中，我们介绍称为“私有众多估计器”（PPE）的主要框架。在此之前，我们需要先给出几个定义。

半度量空间。 在我们的应用中，我们需要处理仅满足近似 三角不等式的距离函数，而且该不等式仅在点彼此足够接近时成立。为此，我们首先定义半度量空间的概念。

定义 2.1（半度量空间）。 如果对于每个 F、F_1、F_2、$F_3 \in \mathcal{F}$，以下条件均成立，则称 $(\mathcal{F}, \text{dist})$ 为半度量空间。

1. 非负性。$\textbf{dist}(F, F) = 0$；$\textbf{dist}(F_1, F_2) \geq 0$。**2. 对称性**。$\textbf{dist}(F_1, F_2) = \textbf{dist}(F_2, F_1)$。**3. z-近似 r-受限三角不等式**。令 $r > 0$ 和 $z \geq 1$。如果 $\textbf{dist}(F_1, F_2)$、$\textbf{dist}(F_2, F_3) \leq r$，则 $\textbf{dist}(F_1, F_3) \leq z \cdot (\textbf{dist}(F_1, F_2) + \textbf{dist}(F_2, F_3))$。

掩蔽机制。 直观地说，掩蔽机制 $\mathcal{B}$ 是一种随机函数，它返回输入的加噪版本，旨在使相近的输入不可区分。形式上，我们定义掩蔽机制如下。

定义 2.2（掩蔽机制（[AL22], 定义 3.3））。设（$\mathcal{F}$, dist）为一个半度量空间。若随机化函数 $\mathcal{B}\colon \mathcal{F} \to \mathcal{F}$满足：对于所有满足 $\text{dist}(F, F') \leq \gamma$ 的 $F, F' \in \mathcal{F}$， $\mathcal{B}(F)$ $\mathcal{B}(F')$ 均为（ε, δ）-不可区分，则称其为（$\gamma, \varepsilon, \delta$）-掩蔽机制，作用于（$\mathcal{F}$, dist）。此外，若对于所有 $F \in \mathcal{F}$, $\mathbb{P}[$, $\text{dist}(\mathcal{B}(F)$ $F) > \alpha] \leq \beta$，则称 $\mathcal{B}$ 为（α, β）-集中。

2.1 PrivatePopulous 估计器（PPE）

本节定义 PPE 框架，该框架使我们能够利用非隐私算法来设计私有算法。我们用 $\mathcal{A}\colon \mathcal{X}^* \to \mathcal{Y}$ 表示非隐私算法，该算法以数据集中的元素作为输入，并输出 $\mathcal{Y}$ 中的一个元素。PPE 需要两个假设。首先，我们假设（$\mathcal{Y}$, dist）是一个半度量空间。其次，我们假设可以使用一个作用于（$\mathcal{Y}$, dist）的高效掩蔽机制。

本节介绍的 PPE 框架可以看作是 Ashtiani & Liaw [AL22] 所用框架的一种广义版本，而且所需的假设更少。给定数据集 D 作为输入，我们将 D 划分为 t 个互不相交的子集。接下来，我们在每个子集上运行非隐私算法 $\mathcal{A}$，生成 t 个输出 Y_1、……、Y_t。随后，我们以隐私方式检查大多数 t 个输出是否彼此接近。如果不是，PPE 就会失败。否则，它会选出一个与超过 60% 的其他 Y_i个输出接近的 Y_j，并使用掩蔽机制 $\mathcal{B}$ 为其添加噪声，然后返回 Y_j的掩蔽版本。该算法的形式化细节见算法 1。

算法 1 私有众多估计器

输入： 数据集 $D = (X_1, \ldots, X_m)$，任意算法 $\mathcal{A}\colon \mathcal{X}^* \to \mathcal{Y}$，参数 $r, \varepsilon, \delta > 0, z \geq 1, t \in \mathbb{N}_{\geq 1}$。

1: 设 $s \leftarrow \lfloor m/t \rfloor$。
2: 对于 $i \in [t]$，令 $Y_i \leftarrow \mathcal{A}(\{X_\ell\}_{\ell=(i-\ 1)s+1}^{is})$.
3: 对于 $i \in [t]$，令 $q_i \leftarrow \frac{1}{t}|\{j \in [t] : \text{dist}(Y_i, Y_j) \leq r/2z\}|$。
4: 设 $Q \leftarrow \frac{1}{t}\sum_{i\in[t]} q_i$.
5: 令 $Z \sim$服从截断拉普拉斯机制$(2/t, \varepsilon, \delta)$。
6: 令 $\widetilde{Q} \leftarrow Q + Z$。
7: 如果 $\widetilde{Q} < 0.8 + \frac{2}{t\varepsilon}\ln(1 + \frac{e^\varepsilon - 1}{2\delta})$，则失败并返回 $\perp$。
8: $j =$ 分钟$\{i :\ q_i > 0.6\}$.
9: 返回 $\widetilde{Y} = \mathcal{B}(Y_j)$。

以下定理证明了算法 1 的隐私性和准确性。证明见附录 D.1。

定理 2.3。 假设 $(\mathcal{Y}, \mathrm{dist})$ 满足 z-近似 r-受限三角不等式。此外，假设 $\mathcal{B}$ 是一个 (r, ε, δ)-掩蔽机制。

- **隐私**。 对于 $t > 5$，算法 *1* 满足 $(2\varepsilon, 4e^{\varepsilon}\delta)$-差分隐私。
- **效用**。 假设 $\alpha \le r/2z$ 且 $t \ge (\frac{20}{\varepsilon}\ln(1 + \frac{e^{\varepsilon}-1}{2\delta})$。设 $\mathcal{B}$ 满足 $(\alpha/2z, \beta)$-集中条件。若存在 Y^*，使得对于所有 $i \in [t]$，$\mathrm{dist}(Y^*, Y_i) < \alpha/2z$，则 $\mathbb{P}\left[\mathrm{dist}(\widetilde{Y}, Y^*) > \alpha\right] \le \beta$。

效用保证表明，如果所有非隐私过程的结果彼此接近，那么 PPE 的输出也会接近这些非隐私结果。

注 *2.4*。设 $T_{\mathcal{A}}$ 为第 *2* 行算法 $\mathcal{A}$ 的运行时间，T_{dist} 为第 *3* 行计算任意 $Y_i, Y_j \in \mathcal{Y}$ 对应的 $\widetilde{\mathit{dist}}(Y_i, Y_j)$ 所需的时间，而 $T_{\mathcal{B}}$ 为第 *9* 行计算 Y 所需的时间。那么算法 *1* 的运行时间为 $O(t \cdot T_{\mathcal{A}} + t^2 \cdot T_{\mathrm{dist}} + T_{\mathcal{B}})$。我们将看到，对于高斯混合模型，$T_{\mathcal{A}}$、$T_{\mathcal{B}}$和 T_{dist} 都可以用多项式进行界定。

要应用算法 1 进行高斯混合模型的私有学习，我们需要为其引入一种掩蔽机制 .

为此，我们首先定义如何将针对分量的掩蔽机制转换为针对混合分布的掩蔽机制（第 3 节）。接着，我们定义针对单个高斯分量的掩蔽机制（见第 4 节）。最后，我们将其应用于高斯混合模型，提出一种掩蔽机制，如第 5 节所示。

3 混合分布的掩蔽

本节旨在说明如何将针对单个分量的掩蔽机制“提升”为针对混合分布的掩蔽机制。我们可以通过为每个分量添加噪声，并随机打乱输出分量的顺序来实现这一点。

形式化地，设 $\mathcal{F}$ 表示一个空间，并设 $\mathcal{F}^k = \mathcal{F} \times \ldots \times \mathcal{F}$（$k$ 次）。以下定义有助于定义两个混合分布之间的距离，因为它不受分量顺序的影响。

定义 3.1。 令 dist 表示 $\mathcal{F}$ 上的距离函数。我们定义 dist^k：$\mathcal{F}^k \times \mathcal{F}^k \to \mathbb{R}_{\ge 0}$ 为

$$\mathrm{dist}^k((F_1, \ldots, F_k), (F'_1, \ldots, F'_k)) \coloneqq \min_{\pi} \max_{i \in [k]} \mathrm{dist}(F_i, F'_{\pi(i)}),$$

其中，最小值是在所有排列 π 上取的。

注意，计算 dist^k 需要在所有排列 π上求最小值。直观上，人们可能会认为必须尝试所有排列，因此需要指数级时间。然而，事实证明，可以将计算 dist^k 的问题归约为判定带权二分图中是否存在完美匹配。该论证的详细内容见附录 E.1。

引理 3.2。 若 T_{dist} 是计算 dist 的运行时间，则 dist^k 可在 $O(k^2 T_{\mathrm{dist}} + k^3 \log k)$ 时间内计算。

以下定义有助于将针对一个分量的掩蔽机制扩展为针对混合的掩蔽机制。在该机制中，分量会被随机打乱，因此其结果独立于分量的原始顺序。

定义 3.3. 假设 $\mathcal{B}$ 是针对 $\mathcal{F}$ 的 $(\gamma, \varepsilon, \delta)$-掩蔽机制。我们将机制 $\mathcal{B}^k_\sigma$ 定义为 $\mathcal{B}^k_\sigma(F_1, \ldots, F_k) = (\mathcal{B}(F_{\sigma(1)}) \ldots, \mathcal{B}(F_{\sigma(k)}))$，其中 σ 是均匀随机排列。

我们还注意到，$\mathcal{B}^k_\sigma$ 只需多项式开销即可计算得到。证明见附录E.2。

引理 3. 4. 如果 $T_{\mathcal{B}}$ 是 $\mathcal{B}$ 的运行时间，那么 $\mathcal{B}_\sigma^k$ 可在时间 $O(k \cdot T_{\mathcal{B}} + k \log k)$ 内计算得到 .

下一个引理表明， $\mathcal{B}_\sigma^k$ 确实是关于 ($\mathcal{F}^k$,距离^k) 的掩蔽机制，并且当 $\mathcal{B}$ 准确时， $\mathcal{B}_\sigma^k$ 也是准确的。证明见附录 E.3。

引理 3.5. 若 $\mathcal{B}$ 是针对 (α, β)-集中 $(\gamma, \varepsilon, \delta)$-掩蔽机制，适用于 $(\mathcal{F}$,距离) 的机制，那么对于任意 $\delta' > 0$, $\mathcal{B}_\sigma^k$ α $k\beta$ γ ε' $k\delta + \delta'$ $\mathcal{F}^k$ ^{k} 都是针对 (,)-集中 (,,)-掩蔽机制，适用于 (,距离) 的机制，其中

$$\varepsilon' = \sqrt{2k \ln(1/\delta')}\varepsilon + k\varepsilon(e^\varepsilon - 1).$$

回顾一下，定理2.3 要求距离函数满足 r-受限的 z-近似性质。下一个引理表明，只要 距离 满足该性质，距离^k 也确实满足该性质。证明见附录 E.4。

引理 3.6. 若 距离 满足 r-受限的 z-近似三角不等式，则 距离^k 也满足该不等式。

4 掩蔽单个高斯分量

本节将为单个高斯分量构造一种掩蔽机制。为此，我们定义高斯分量之间的一种新距离度量。

令 $\mathcal{F}_{\text{Comp}} = \mathbb{R} \times \mathbb{R}^d \times \mathbb{R}^{d \times d}$ （分别对应权重 w、均值 μ 和协方差矩阵 Σ）。定义 $\text{dist}_{\text{Comp}}$: $\mathcal{F}_{\text{Comp}} \times \mathcal{F}_{\text{Comp}} \to \mathbb{R}_{\geq 0}$ 为

$$\text{dist}_{\text{Comp}}((w_1, \mu_1, \Sigma_1), (w_2, \mu_2, \Sigma_2)) = \text{最大值}\{|w_1 - w_2|, \text{dist}_{\text{Mean}}((\mu_1, \Sigma_1), (\mu_2, \Sigma_2)), \text{dist}_{\text{Cov}}(\Sigma_1, \Sigma_2)\},$$

其中

$$\text{dist}_{\text{Cov}}(\Sigma_1, \Sigma_2) = \max\{\|\Sigma_1^{1/2}\Sigma_2^{-1}\Sigma_1^{1/2} - I_d\|_F, \|\Sigma_2^{1/2}\Sigma_1^{-1}\Sigma_2^{1/2} - I_d\|_F\}$$

and

$$\text{dist}_{\text{Mean}}((\mu_1, \Sigma_1), (\mu_2, \Sigma_2)) = \max\{\|\mu_1 - \mu_2\|_{\Sigma_1}, \|\mu_1 - \mu_2\|_{\Sigma_2}\}.$$

首先，我们证明 $\text{dist}_{\text{Comp}}$ 满足近似三角不等式；这对于使用定理 2.3。

引理 4.1。 dist_{Comp} 满足 1-受限(3/2)-近似三角不等式 .

证明。 对于任意正定矩阵 Σ， $\|\cdot\|_\Sigma$ 是一个度量，因此，$\text{dist}_{\text{Mean}}$ 是一个度量（因而满足 1-受限 (3/2)-近似三角不等式）。接下来，dist_{Cov} 满足 1-受限 (3/2)-近似三角不等式（见引理 A.8）。通过直接计算可得，因此，$\text{dist}_{\text{Comp}}$ 也满足 1-受限 (3/2)-近似三角不等式。 □

以下引理给出了单个高斯机制的掩蔽机制。证明见附录 F。该机制基本上分别对混合权重、均值和协方差矩阵添加噪声。对混合权重添加噪声，可以使用高斯机制。对均值和协方差矩阵添加噪声时则必须谨慎。两种情况下，我们都使用经验协方差矩阵本身，对均值和协方差矩阵进行重新缩放。请注意，必须正确设置参数 γ （输入必须有多接近）以及 η_{W}， η_{Mean}， η_{Cov} （噪声幅度），才能确保隐私和准确性。粗略来说，对于大小为 d的向量，为确保准确性误差不超过 α，噪声应取为 η 约 $\alpha/\sqrt{d}$ 。因此 $\eta_{\text{W}} \sim \alpha$， $\eta_{\text{Mean}} \sim \alpha/\sqrt{d}$ 且 $\eta_{\text{Cov}} \sim \alpha/d$。为确保 ($\varepsilon$， δ)-差分隐私，我们必须确保输出足够接近（否则噪声不足以使输入不可区分）。瓶颈在于对协方差矩阵添加噪声，这要求 $\gamma \sim \varepsilon\eta_{\text{Cov}}/\sqrt{d} \sim \alpha\varepsilon/d^{3/2}$。关于参数选择的更多细节见附录 F。

引理 4.2。 对于 $\gamma \leq C_2\sqrt{d^2 \cdot d + \frac{\varepsilon\alpha}{(\ln(4/\beta))\cdot\ln(2/\delta)}}$，存在一个$(\gamma,\ 3\varepsilon,\ 3\delta)$-掩蔽机制 $\mathcal{B}_{\text{COMP}}$，其适用于$(\mathcal{F}_{\text{COMP}},\ \text{dist}_{\text{COMP}})$，且$(\alpha,\ 3\beta)$-集中，其中 C_2 是一个通用常数。

5 高斯混合模型的掩蔽机制

本节将展示如何对由 k 个高斯分布组成的混合进行掩蔽。令 $\mathcal{F}_{\text{GMM}} = \mathcal{F}_{\text{COMP}} \times \ldots \times \mathcal{F}_{\text{COMP}}$ (k 次)。注意，由于 k 在 $\mathcal{F}_{\text{GMM}}$ 中是固定的，且可从上下文推知，因此我们省略 k （以及下文相关的记号）。令$\text{dist}_{\text{COMP}}$ 为式（4）中定义的距离，并定义距离

$$\text{dist}_{\text{PARAM}}(\{(w_i,\mu_i,\Sigma_i)\}_{i\in[k]},\{(w_i',\mu_i',\Sigma_i')\}_{i\in[k]}) = \min_{\pi}\max_{i\in[k]}\text{dist}_{\text{COMP}}((w_{\pi(i)},\mu_{\pi(i)},\Sigma_{\pi(i)}),(w_i',\mu_i',\Sigma_i')),$$

其中 π i s 从 $[k]$上的所有排列构成的集合中选取。现在定义掩蔽机制

$$\mathcal{B}_{\text{GMM}}(\{(w_i,\mu_i,\Sigma_i)\}_{i\in[k]}) = \{\mathcal{B}_{\text{COMP}}(w_{\sigma(i)},\mu_{\sigma(i)},\Sigma_{\sigma(i)})\}_{i\in[k]},$$

其中 $\mathcal{B}_{\text{COMP}}$ 是引理 4.2 中的掩蔽机制，而 σ 是从 $[k]$上所有排列构成的集合中均匀随机选取的排列。换言之， $\mathcal{B}_{\text{GMM}}$ 先将第 $\mathcal{B}_{\text{COMP}}$节的掩蔽机制 4 分别应用于每个分量，然后对这些分量进行排列。为概述用于高斯混合模型的整个掩蔽机制，我们在算法 2中给出伪代码。

以下引理断言， $\mathcal{B}_{\text{GMM}}$ 确实是一种掩蔽机制。从高层次来看，这可由引理 4.2 和引理 3.5结合得出。详情见附录 G.1。

引理 5.1。 令 $\varepsilon < \ln(2)/3$。存在一个充分大的常数 C_2，使得对于 $\gamma \leq C_2\sqrt{k \quad 2/\delta}\sqrt{d^2 \cdot \frac{\varepsilon\alpha}{d + \ln()(\ln(12k/\beta))\cdot\ln(12k/\delta)}}$，$\mathcal{B}_{\text{GMM}}$ 是关于 $(\mathcal{F}_{\text{GMM}},\text{dist}_{\text{PARAM}})$ 的$(\gamma,\varepsilon,\delta)$-掩蔽机制。此外， $\mathcal{B}_{\text{GMM}}$ 是(α,β)-集中机制。

注意，$\text{dist}_{\text{PARAM}}$ 也满足1-受限的 $(3/2)$-近似三角不等式，因为 $\text{dist}_{\text{COMP}}$ 确实如此（证明见附录 G.2 ）。

引理 5.2。 $\text{dist}_{\text{PARAM}}$ 满足1-受限$(3/2)$-近似三角不等式。

6 私有学习高斯混合模型

至此，我们已经具备开发一种用于学习高斯混合模型参数的私有算法所需的一切条件。首先，我们更正式地定义这个问题。

定义 6.1 （高斯混合模型参数的 PAC 学习）。 令 $\mathcal{F} = \left\{\left(w_i^j,\mu_i^j,\Sigma_i^j\right)_{i=1}^k\right\}^j$ 为一个由 d 维、具有 k 个分量[5]的高斯混合模型构成的类。令 $\mathcal{A}$ 为一个函数，它接收一个由 S 个样本组成的序列，这些样本来自 $\mathbb{R}^d$，并输出一个混合分布 $\hat{F} = (\hat{w}_i, \hat{\mu}_i, \hat{\Sigma}_i)_{i=1}^k$。令 m: $(0,1)^2 \times \mathbb{N}^2 \to \mathbb{N}$。若对于每个 α、$\beta \in (0,1)$ 以及每个 $F \in \mathcal{F}$，当 S 是从 $\hat{F}$ 中抽取的大小为 $m(\alpha,\beta,k,d)$ 的独立同分布样本时，$\text{dist}_{\text{GMM}}(F,F) < \alpha$ 的概率至少为 $1-\beta$，则称 $\mathcal{A}$ 用 m 个样本学习了 $\mathcal{F}$ 的参数。

将第 5 节中提出的掩蔽机制（尤其是引理 5.1 和引理 5.2）代入 PPE（定理 2.3），即可得到高斯混合模型的私有到非私有归约。

[5]例如，通常选择 $\mathcal{F}$ 为可分离/可辨识的高斯混合模型。

算法 2GMM 掩蔽机制

输入： 由 $\{(w_i, \mu_i, \Sigma_i)\}_{i\in[k]}$ 给出的高斯混合模型，以及参数 $\eta_{\mathrm{W}}, \eta_{\mathrm{MEAN}}, \eta_{\mathrm{COV}} > 0$

函数 $\mathcal{R}_{\mathrm{W}}(w)$ ▷ 噪声混合权重
  返回 $\max(0, w + \eta_{\mathrm{W}} g)$，其中 $g \sim \mathcal{N}(0, 1)$。
函数结束
函数 $\mathcal{R}_{\mathrm{MEAN}}(\mu, \Sigma)$ ▷ 噪声均值
  返回 $\mu + \eta_{\mathrm{MEAN}} g$ 其中 $g \sim \mathcal{N}(0, \Sigma)$
结束函数
函数 $\mathcal{R}_{\mathrm{COV}}(\Sigma)$ ▷ 噪声协方差
  令 $G \in \mathbb{R}^{d\times d}$ 为元素独立服从 $(0, 1)$ 分布的矩阵。
  返回 $\Sigma^{1/2}(I_d + \eta_{\mathrm{COV}} G)(I_d + \eta_{\mathrm{COV}} G)^\top \Sigma^{1/2}$
结束函数
函数 $\mathcal{B}_{\mathrm{COMP}}(w, \mu, \Sigma)$ ▷ 掩码分量
  返回 $(\mathcal{R}_{\mathrm{W}}(w)\ \mathcal{R}_{\mathrm{MEAN}}(\mu, \Sigma)\ \mathcal{R}_{\mathrm{COV}}(\Sigma))$
结束函数
函数 $\mathcal{B}_{\mathrm{GMM}}(\{(w_i, \mu_i, \Sigma_i)\}_{i\in[k]})$ ▷ 掩码高斯混合模型
  令 σ 为均匀随机排列。
  $\{(\hat{w}_i, \hat{\mu}, \hat{\Sigma}_i)\} \leftarrow \{\mathcal{B}_{\mathrm{COMP}}(w_{\sigma(i)}, \mu_{\sigma(i)}, \Sigma_{\sigma(i)})\}$.
  归一化：$\hat{w}_i \leftarrow \hat{w}_i / \sum_{i\in[k]} \hat{w}_i$.
  返回 $\{(\hat{w}_i, \hat{\mu}, \hat{\Sigma}_i)\}_{i\in[k]}$。
结束函数

定理 6.2（从隐私到非隐私的归约）。设 $\mathcal{F}$ 是 $\mathbb{R}^d$ 中具有 k 个分量的高斯混合模型子类。设 $\mathcal{A}$ 是一个非隐私算法，它使用 $m_{\text{NON-PRIVATE}}(\alpha, \beta, k, d)$ 个样本，以 PAC 方式学习 $\mathcal{F}$ 相对于 dist_{GMM} 的参数。那么，对于每个 $\varepsilon < \ln(2)/3$、$\delta \in (0, 1)$、$\gamma \le C_2\sqrt{k\ln(2/\delta)}\sqrt{d^2\ d + (\ln(12k/\beta)) \cdot \ln(12k/\delta)}$

对于足够大的常数 C 和 $t = \text{最大值}\{5, \lceil \frac{20}{\varepsilon}\ln(1 + \frac{e^\varepsilon - 1}{2\delta})\rceil\}$，存在一个学习器 $\mathcal{A}_{PRIVATE}$，具有以下性质：

1. $\mathcal{A}_{PRIVATE}$ 是 $(2\varepsilon, 4e^\varepsilon\delta)$-差分隐私。 *2.* $\mathcal{A}_{PRIVATE}$ 使用 $O(m_{NON\text{-}PRIVATE}(\gamma, \beta/2t, k, d)\ \log(1/\delta)/\varepsilon)$ 个样本 PAC 学习 $\mathcal{F}$ 的参数。 *3.* $\mathcal{A}_{PRIVATE}$ 的运行时间为 $O((\log(1/\delta)/\varepsilon) \cdot T_{\mathcal{A}} + (\log(1/\delta)/\varepsilon)^2 \cdot (k^2 d^3 + k^3 \log k))$，其中 $T_{\mathcal{A}}$ 是非隐私算法的运行时间。

为证明 定理 6.2，我们需要以下引理，其证明见附录 H.

引理 *6.3.* 设 $F = (w_i, \mu_i, \Sigma_i)_{i=1}^k$ 和 $F' = (w'_i, \mu'_i, \Sigma'_i)_{i=1}^k$ 是两个 d 维高斯混合模型，其中 Σ_i 和 Σ'_i 是正定矩阵。假设 $dist_{GMM}(F, F') < \frac{1}{600}$。则 $1\ 200\ dist_{PARAM}(F, F') \le dist_{GMM}(F, F') \le \frac{1}{\sqrt{2}} dist_{PARAM}(F, F')$。

定理 *6.2*的证明。令 $z = 3/2$，$r = 1$，以及 $t \ge \frac{20}{\varepsilon}\ln\left(1 + \frac{e^\varepsilon - 1}{2\delta}\right) = O(\log(1/\delta)/\varepsilon)$。我们按如下方式运行算法 1。

- 对于非隐私算法 $\mathcal{A}$，我们使用定理 6.5 中的算法，其准确性参数为$\alpha/2z$，失败概率为 $\beta/2t$。
- 对于掩蔽机制，我们使用 (r, ε, δ)-掩蔽机制 $\mathcal{B}_{\text{高斯混合模型}}$，其定义见引理 5.1。此外，该机制是 $(\alpha/2z, \beta/2)$-集中。
- 最后，注意到距离函数 $\mathrm{dist}_{\mathrm{PARAM}}$ 满足 z-近似 r-受限三角不等式（引理 5.2）。

令 F^* 为真实的高斯混合模型。令 F_i 为由 $\mathcal{A}$ 在算法 2 的第 1 行计算得到的估计高斯混合模型。则上述第一项保证，对于所有 $i \in [t]$，以至少 $1 - \beta/2$ 的概率有$\mathrm{dist}_{\mathrm{PARAM}}(F^*, F_i) \le \alpha/2z$。

因此，我们得出结论：我们拥有一个用于学习高斯混合模型的私有算法，该算法满足 $(2\varepsilon, 4e^{\varepsilon}\delta)$-差分隐私，并且 $\tilde{}$ $\tilde{}$返回满足 F 的 $\mathrm{dist}_{\mathrm{PARAM}}(F, F^*) \le \alpha$，其概率为 $1-\beta$。根据引理 6.3，我们进一步得出 $\tilde{}\mathrm{dist}_{\mathrm{GMM}}(F, F^*) \le O(\alpha)$ 的概率为 $1-\beta$。

接下来需要检查我们算法的样本复杂度和计算复杂度。由于我们运行 t 个相互独立的非隐私算法 $\mathcal{A}$ 实例，因此需要 $t \cdot m_{\mathrm{PRIVATE}}(\alpha/2z, \beta/2t, k, d) = O(m_{\mathrm{PRIVATE}}(\alpha/2z, \beta/2t, k, d) \cdot \log(1/\delta)/\varepsilon)$ 个样本。最后，我们给出运行时间的上界。引理 3.4 表明，应用掩蔽机制的运行时间为 $O(k \cdot d^3 + k \log k)$；引理 3.2 表明，计算 dist 的运行时间为 $O(k^2 d^3 + k^3 \log k)$。由注 2.4 可得所述运行时间。 □

6.1 应用

作为一项具体应用，我们将定理 6.2 与 Moitra & Valiant 的算法 [MV10] 结合，从而得到首个用于学习高斯混合模型参数的私有算法，其样本复杂度和计算复杂度关于 d （对于固定的 k）均为多项式级，且只需满足最小分离假设。请注意，我们的算法对参数没有任何有界性假设。

定义 6.4（γ-统计可学习的 [MV10]）。如果一个高斯混合模型 $F = (w_i, \mu_i, \Sigma_i)_{i=1}^k$ 是 γ-统计可学习的，则称之为如此，当且仅当 (i) $\min_i w_i \ge \gamma$ 且 (ii) $\min_{i \ne j} d_{\mathrm{TV}}(\mathcal{N}(\mu_i, \Sigma_i)\ \mathcal{N}(\mu_j, \Sigma_j)) \ge \gamma$。

If a 高斯混合模型是 γ-统计可学习的，我们就能够准确地恢复其分量 .

定理 6.5 (高斯混合模型的非私有学习 [MV10])。存在一个算法 $\mathcal{A}$ 和一个函数 $m_{\mathcal{A}}(d, k, \alpha, \beta)$ 满足以下保证。固定 $\alpha, \beta \in (0, 1)$，$k, d \in \mathbb{N}$。

- 对于固定的 k，样本复杂度 $m_{\mathcal{A}}(d, k, \alpha, \beta)$ 关于 $d/\alpha\beta$ 是多项式的。
- 对于固定的 k，$\mathcal{A}$ 的运行时间为 $\mathrm{poly}(d/\alpha\beta)$。
- 设 $\mathcal{F}^*$ 是高斯混合模型的一个 α-统计可学习子类，其在 $\mathbb{R}^d$ 中有 k 个分量，并设 $F^* \in \mathcal{F}^*$。给定一个从 F^* 抽取的大小为 $m_{\mathcal{A}}$ 的独立同分布样本 $D(d, k, \alpha, \beta)$，以至少 $1-\beta$ 的概率，$\mathcal{A}$返回 ^^F，使得 $\mathrm{dist}_{GMM}(F, F^*) \le \alpha$。

将定理 6.5 代入定理 6.2即可立即得到以下推论 .

推论 6.6. 存在一个算法 $\mathcal{A}$和一个函数 $m_{\mathcal{A}}(d, k, \alpha, \beta, \varepsilon, \delta)$ 具有如下保证。固定 $\alpha, \beta, \varepsilon, \delta \in (0, 1)$，$k, d \in \mathbb{N}$。

- $\mathcal{A}$ 是(ε, δ)-差分隐私。
- 对于固定的 k，样本复杂度 $m_{\mathcal{A}}(d, k, \alpha, \beta, \varepsilon, \delta)$ 关于 $d\log(1/\delta)/\alpha\beta\varepsilon$是多项式的。
- 对于固定的 k，$\mathcal{A}$ 的运行时间为$\mathrm{poly}(d\log(1/\delta)/\alpha\beta\varepsilon)$。
- 设 $\mathcal{F}^*$ 是 *GMM* 的一个 α-统计可学习子类，在 $\mathbb{R}^d$ 中具有 k 个分量，并设 $F^* \in \mathcal{F}^*$。给定一个从 F^*中抽取的、大小为 $m_{\mathcal{A}}(d, k, \alpha, \beta, \varepsilon, \delta)$ 的独立同分布样本 D，以至少 $1-\beta$的概率，$\mathcal{A}$ ^^返回 F，使得$\mathrm{dist}_{GMM}(F, F^*) \le \alpha$。

致谢。作者感谢 Abbas Mehrabian 指出了早期版本中的定理 1.8 中的一处错误。作者还要感谢匿名审稿人提出的许多富有见地的意见。Hassan Ashtiani 得到了 NSERC Discovery 资助。

参考文献

[AAK21] Ishaq Aden-Ali、Hassan Ashtiani 和 Gautam Kamath《私密学习无界高维高斯分布的样本复杂度》。载于：（2021），第185–216页。

[AAL21] Ishaq Aden-Ali、Hassan Ashtiani 和 Christopher Liaw《私密学习轴对齐高斯混合分布》。载于：《神经信息处理系统进展》第34卷（2021），第3925–3938页。[ABGRV14] Joseph Anderson、Mikhail Belkin、Navin Goyal、Luis Rademacher 和 James Voss《越多越好：维度对学习大型高斯混合分布的益处》。载于：学习理论会议。PMLR，2014年，第1135–1164页。[ABHLMP18] Hassan Ashtiani、Shai Ben-David、Nicholas Harvey、Christopher Liaw、Abbas Mehrabian 和 Yaniv Plan《通过样本压缩方案学习高斯混合分布的近乎紧确样本复杂度界》。载于：《神经信息处理系统进展》第31卷（2018）。[ABHLMP20] Hassan Ashtiani、Shai Ben-David、Nicholas JA Harvey、Christopher Liaw、Abbas Mehrabian 和 Yaniv Plan《通过压缩方案鲁棒学习高斯混合分布的近乎最优样本复杂度界》。载于：《ACM学报》67.6（2020），第1–42页。[ABM18] Hassan Ashtiani、Shai Ben-David 和 Abbas Mehrabian《样本高效的混合分布学习》。载于：AAAI人工智能会议论文集，第32卷，2018年。[ADLS17] Jayadev Acharya、Ilias Diakonikolas、Jerry Li 和 Ludwig Schmidt《近线性时间内的样本最优密度估计》。载于：第二十八届ACM-SIAM离散算法年会论文集。SIAM，2017年，第1278–1289页。[AKTVZ22] Daniel Alabi、Pravesh K. Kothari、Pranay Tankala、Prayaag Venkat 和 Fred Zhang《高斯分布的私有估计：高效、鲁棒且最优》。载于：arXiv预印本 arXiv:2212.08018（2022）。[AL22] Hassan Ashtiani 和 Christopher Liaw《学习高斯分布及更广泛问题的私有多项式时间算法》。载于：学习理论会议。PMLR，2022年，第1075–1076页。[AM05] Dimitris Achlioptas 和 Frank McSherry《关于分布混合的谱学习》。载于：国际计算学习理论会议。施普林格，2005年，第458–469页。[ASZ21] Jayadev Acharya、Ziteng Sun 和 Huanyu Zhang《差分隐私版Assouad、Fano和Le Cam方法》。载于：算法学习理论。PMLR，2021年，第48–78页。[AUZ23] Hilal Asi、Jonathan Ullman 和 Lydia Zakynthinou《从鲁棒性到隐私，再回归》。载于：arXiv预印本 arXiv:2302.01855（2023）。[BDJKKV22] Ainesh Bakshi、Ilias Diakonikolas、He Jia、Daniel M Kane、Pravesh K Kothari 和 Santosh S Vempala《鲁棒学习k个任意高斯分布的混合》。载于：第54届 ACM SIGACT 计算理论年会论文集，2022年，第1234–1247页。[BDKU20] Sourav Biswas、Yihe Dong、Gautam Kamath 和 Jonathan Ullman《Coinpress：实用的私有均值与协方差估计》。载于：《神经信息处理系统进展》第33卷（2020），第14475–14485页。[BGSUZ21] Gavin Brown、Marco Gaboardi、Adam Smith、Jonathan Ullman 和 Lydia Zakynthinou《协方差

nce-

感知私有均值估计，无需私有协方差估计”。载于：神经信息处理系统进展34（2021），第 7950–7964 页。[BKS22] Alex Bie、Gautam Kamath 和 Vikrant Singhal，《使用公开数据的隐私估计》。载于：神经信息处理系统进展（2022）。[BS09] Mikhail Belkin 和 Kaushik Sinha，《任意分离条件下的高斯混合学习》。载于：*arXiv* 预印本 *arXiv:0907.1054*（2009）。[BS10] Mikhail Belkin 和 Kaushik Sinha，《分布族的多项式学习》。载于：*2010 IEEE* 第*51*届计算机科学基础年会。IEEE，2010，第 103–112 页。[BSKW19] Mark Bun、Thomas Steinke、Gautam Kamath 和 Zhiwei Steven Wu，《隐私假设选择》。载于：神经信息处理系统进展32（2019）。

[BV08] S Charles Brubaker 和 Santosh S Vempala，《各向同性主成分分析与仿射不变聚类》。载于《Building Bridges》。施普林格，2008，第 241–281 页。[CCdEIST23] Hongjie Chen、Vincent Cohen-Addad、Tommaso d'Orsi、Alessandro Epasto、Jacob Imola、David Steurer 和 Stefan Tiegel，《随机块模型与混合模型的私有估计算法》。载于：arXiv 预印本 arXiv:2301.04822（2023）。[CDSS14] Siu-On Chan、Ilias Diakonikolas、Rocco A Servedio 和 Xiaorui Sun，《通过分段多项式逼近实现高效密度估计》。载于《第四十六届 ACM 理论计算研讨会论文集》。2014，第 604–613 页。[CKMST21] Edith Cohen、Haim Kaplan、Yishay Mansour、Uri Stemmer 和 Eliad Tsfadia，《针对简单样本的差分隐私聚类》。载于《国际机器学习会议》。PMLR，2021，第 2049–2059 页。[Das99] Sanjoy Dasgupta，《高斯混合学习》。载于《第40届计算机科学基础年会（目录号 99CB37039）》。IEEE，1999，第 634–644 页。[DHK23] John Duchi、Saminul Haque 和 Rohith Kuditipudi，《自适应私有均值估计的快速算法》。载于：arXiv 预印本 arXiv:2301.07078（2023）。[DKMMN06] Cynthia Dwork、Krishnaram Kenthapadi、Frank McSherry、Ilya Mironov 和 Moni Naor，《我们的数据，我们自己：通过分布式噪声生成实现隐私保护》。载于《密码学技术与应用国际年会》。施普林格，2006，第 486–503 页。[DKS17] Ilias Diakonikolas 、 Daniel M Kane 和 Alistair Stewart，《高维高斯分布及高斯混合稳健估计的统计查询下界》。载于《2017 IEEE 第58届计算机科学基础年会（FOCS）》。IEEE，2017，第 73–84 页。[DL01] Luc Devroye 和 Gábor Lugosi，《密度估计的组合方法》。施普林格科学与商业媒体，2001。[DL09] Cynthia Dwork 和 Jing Lei，《差分隐私与稳健统计》。载于《第四十一届 ACM 理论计算研讨会论文集》。2009，第 371–380 页。[DMNS06] Cynthia Dwork、Frank McSherry、Kobbi Nissim 和 Adam Smith，《在私有数据分析中校准噪声以匹配敏感度》。载于《密码学理论：第三届密码学理论会议，TCC 2006，美国纽约，2006年3月4日至7日。论文集 3》。施普林格，2006，第 265–284 页。[DMR18] Luc Devroye、Abbas Mehrabian 和 Tommy Reddad，《高维高斯分布之间的全变差距离》。载于：arXiv 预印本 arXiv:1810.08693（2018）。[DR+14] Cynthia Dwork、Aaron Roth 等，《差分隐私的算法基础》。载于《理论计算机科学基础与趋势》9.3–4（2014），第 211–407 页。[DRV10] Cynthia Dwork、Guy N. Rothblum 和 Salil P. Vadhan，《增强与差分隐私》。载于《2010 IEEE 第51届计算机科学基础年会》（2010），第 51–60 页。[FSO06] Jon Feldman、Rocco A Servedio 和 Ryan O'Donnell，《无分离假设的轴对齐高斯混合 PAC 学习》。载于《国际计算学习理论会议》。施普林格，2006，第 20–34 页。[GDGK18] Quan Geng、Wei Ding、Ruiqi Guo 和 Sanjiv Kumar，《近似差分隐私的截断拉普拉斯机制》。载于：arXiv 预印本 arXiv:1810.00877（2018）。[GH22] Kristian Georgiev 和 Samuel B Hopkins，《隐私带来鲁棒性：信息—计算

n

间隙与稀疏均值估计"。载于：*arXiv*预印本 *arXiv:2211.00724* （2022年）。[HK13] Daniel Hsu 与 Sham M Kakade "球形高斯分布混合模型的学习：矩方法与谱分解"。载于：第*4*届理论计算机科学创新会议。2013年，第11–20页。

[HKM22] Samuel B Hopkins、Gautam Kamath 与 Mahbod Majid “通过平方和指数机制实现纯差分隐私下的高效均值估计”。载于：第54届 ACM SIGACT 计算理论年会论文集。2022年，第1406–1417页。[HKMN23] Samuel B Hopkins、Gautam Kamath、Mahbod Majid 与 Shyam Narayanan “统计估计中的鲁棒性意味着隐私”。载于：第55届 ACM SIGACT 计算理论年会论文集。2023年。[HL18] Samuel B Hopkins 与 Jerry Li “混合模型、鲁棒性与平方和证明”。载于：第50届 ACM SIGACT 计算理论年会论文集。2018年，第1021–1034页。[HP14] Moritz Hardt 与 Eric Price “学习两个高斯分布混合模型的紧致界”。载于：arXiv电子印本1404（2014年）。[KLSU19] Gautam Kamath、Jerry Li、Vikrant Singhal 与 Jonathan Ullman “私密学习高维分布”。载于：学习理论会议。PMLR。2019年，第1853–1902页。[KMS22] Gautam Kamath、Argyris Mouzakis 与 Vikrant Singhal “私密估计的新下界与广义指纹引理”。载于：arXiv预印本 arXiv:2205.08532（2022年）。[KMSSU22] Gautam Kamath、Argyris Mouzakis、Vikrant Singhal、Thomas Steinke 与 Jonathan Ullman “用于无界高斯分布的私密且计算高效的估计器”。载于：学习理论会议。PMLR。2022年，第544–572页。[KMV10] Adam Tauman Kalai、Ankur Moitra 与 Gregory Valiant “高效学习两个高斯分布的混合模型”。载于：第42届 ACM 计算理论研讨会论文集。2010年，第553–562页。[KMV22] Pravesh Kothari、Pasin Manurangsi 与 Ameya Velingker “通过稳定凸松弛实现私密鲁棒估计”。载于：学习理论会议。PMLR。2022年，第723–777页。[KSS18] Pravesh K Kothari、Jacob Steinhardt 与 David Steurer “鲁棒矩估计与通过平方和改进聚类”。载于：第50届 ACM SIGACT 计算理论年会论文集。2018年，第1035–1046页。[KSSU19] Gautam Kamath、Or Sheffet、Vikrant Singhal 与 Jonathan Ullman “用于学习分离高斯分布混合模型的差分隐私算法”。载于：神经信息处理系统进展第32卷（2019年）。[KV17] Vishesh Karwa 与 Salil Vadhan “有限样本差分隐私置信区间”。载于：arXiv预印本 arXiv:1711.03908（2017年）。[LKKO21] Xiyang Liu、Weihao Kong、Sham Kakade 与 Sewoong Oh “鲁棒且差分隐私的均值估计”。载于：神经信息处理系统进展第34卷（2021年），第3887–3901页。[LKO22] Xiyang Liu、Weihao Kong 与 Sewoong Oh “高维中的差分隐私与鲁棒统计”。载于：学习理论会议。PMLR。2022年，第1167–1246页。[LL22] Allen Liu 与 Jerry Li “在多项式时间内以近乎最优的分离度聚类混合模型”。载于：第54届 ACM SIGACT 计算理论年会论文集。2022年，第1248–1261页。[LLM22] Allen Liu、Jerry Li 与 Ankur Moitra “鲁棒模型选择与高斯混合模型的近乎适当学习”。载于：神经信息处理系统进展。2022年。[LM00] Beatrice Laurent 与 Pascal Massart “通过模型选择自适应估计二次泛函”。载于：《统计年鉴》（2000年），第1302–1338页。[LM21] Allen Liu 与 Ankur Moitra “确定高斯混合模型的鲁棒可学习性”。载于：第53届 ACM SIGACT 计算理论年会论文集。2021年，第518–531页。

[LM22] Allen Liu & Ankur Moitra《具有近乎最优鲁棒性保证的高斯混合模型学习》。载于：学习理论会议。PMLR。2022年，第2815–2895页。[LS17] Jerry Li & Ludwig Schmidt《通过多项式不等式系统对高斯混合进行鲁棒且适当的学习》。载于：学习理论会议。PMLR。2017年，第1302–1382页。[MV10] Ankur Moitra & Gregory Valiant《确定高斯混合的多项式可学习性》。载于：*2010 IEEE 第51届*计算机科学基础年会。IEEE。2010年，第93–102页。[NRS07] Kobbi Nissim、Sofya Raskhodnikova & Adam Smith《私有数据分析中的平滑敏感度与抽样》。载于：第三十九届 *ACM* 计算理论研讨会年会论文集。2007年，第75–84页。[Pea94] Karl Pearson《进化数学理论的贡献》。载于：伦敦皇家学会哲学汇刊 185 (1894)，第71–110页。[RV17] Oded Regev & Aravindan Vijayaraghavan《关于学习充分分离的高斯混合》。载于：*2017 IEEE 第58届*计算机科学基础年会（*FOCS*）。IEEE。2017年，第85–96页。[SK01] Arora Sanjeev & Ravi Kannan《学习任意高斯混合》。载于：第三十三届 *ACM* 计算理论研讨会年会论文集。2001年，第247–257页。[TCKMS22] Eliad Tsfadia、Edith Cohen、Haim Kaplan、Yishay Mansour & Uri Stemmer《Friendlycore：实用的差分隐私聚合》。载于：国际机器学习会议。PMLR。2022年，第21828–21863页。[VW04] Santosh Vempala & Grant Wang《一种学习混合模型的谱算法》。载于：计算机与系统科学杂志 68.4 (2004)，第841–860页。[WR06] Christopher KI Williams & Carl Edward Rasmussen用于机器学习的高斯过程。第2卷。麻省理工学院出版社，马萨诸塞州剑桥，2006年。[WX18] Xuan Wu & Changzhi Xie《高斯混合适当学习的改进算法》。载于：全国理论计算机科学会议。施普林格。2018年，第8–26页。[Yat85] Yannis G Yatracos《最小距离估计量的收敛速率与柯尔莫哥洛夫熵》。载于：统计年鉴 13.2 (1985)，第768–774页。

A 标准事实

事实 A.1。 设 X_1, X_2, Y_1, Y_2 为随机变量，且 X_1, X_2 （分别地， Y_1, Y_2）相互独立。那么$d_{\mathrm{TV}}((X_1, X_2), (Y_1, Y_2)) \leq d_{\mathrm{TV}}(X_1, Y_1) + d_{\mathrm{TV}}(X_2, Y_2)$。

事实 A.2。 设 X, Y 为随机变量。对于任意可测函数 f, $d_{\mathrm{TV}}(f(X)\ f(Y)) \leq d_{\mathrm{TV}}(X, Y)$.

以下事实中的等式是标准结果；例如，参见 Williams & Rasmussen 中的公式 2.3[WR06]。关于不等式，参见 Ashtiani 等人的引理 2.9 的证明 [ABHLMP20]。

事实 A.3。 设 $\mu_1, \mu_2 \in \mathbb{R}^d$和 $\Sigma_1, \Sigma_2 \succ 0$。那么

$$D_{\mathrm{KL}}(\mathcal{N}(\mu_1, \Sigma_1) \parallel \mathcal{N}(\mu_2, \Sigma_2)) = \frac{1}{2}\big[\operatorname{tr}(\Sigma_2^{-1}\Sigma_1 - I) + (\mu_2 - \mu_1)^\top \Sigma_2^{-1}(\mu_2 - \mu_1) - \ln\det(\Sigma_2^{-1}\Sigma_1)\big].$$

此外，假设 $\Sigma_2^{-1/2}\Sigma_1\Sigma_2^{-1/2}$ 的所有特征值都至少为 $1\ 2$。那么

$$D_{\mathrm{KL}}(\mathcal{N}(\mu_1, \Sigma_1) \parallel \mathcal{N}(\mu_2, \Sigma_2)) \leq \frac{1}{2}\big[\|\Sigma_2^{-1/2}\Sigma_1\Sigma_2^{-1/2} - I\|_F^2 + (\mu_2 - \mu_1)^\top \Sigma_2^{-1}(\mu_2 - \mu_1)\big].$$

引理 A.4 (Pinsker不等式)。 设 P 和 Q 是两个定义了 *KL*散度的分布。那么 $d_{\mathrm{TV}}(P, Q) \leq \sqrt{0.5 D_{\mathrm{KL}}(P \| Q)}$。

引理 A.5 ([LM00], 引理 1)。 令 $g_1, \ldots, g_k$ 为独立同分布的 $\mathcal{N}(0,1)$ 随机变量。那么

$$\mathbb{P}\left[\sum_{i=1}^{k} g_i^2 \geq k + 2\sqrt{kt} + 2t\right] \leq e^{-t}.$$

引理 A.6 ([AL22], 引理 D.2)。 令 $\mu_1, \mu_2 \in \mathbb{R}^d$ 并令 Σ_1, Σ_2 为满秩 $d \times d$ 半正定矩阵。令$Y \sim \mathcal{N}(\mu_1, \Sigma_1)$。那么

$$\begin{aligned}\mathcal{L}_{\mathcal{N}(\mu_1,\Sigma_1)\|\mathcal{N}(\mu_2,\Sigma_2)}(Y) \leq\ & D_{\mathrm{KL}}\left(\mathcal{N}(\mu_1,\Sigma_1) \,\|\, \mathcal{N}(\mu_2,\Sigma_2)\right) \\ & + 2\|\Sigma_1^{1/2}\Sigma_2^{-1}\Sigma_1^{1/2} - I_d\|_F \cdot \sqrt{\ln(2/\delta)} + 2\|\Sigma_1^{1/2}\Sigma_2^{-1}\Sigma_1^{1/2} - I_d\| \cdot \ln(2/\delta) \\ & + \|\Sigma_1^{1/2}\Sigma_2^{-1}\Sigma_1^{1/2}\| \cdot \|\Sigma_1^{-1/2} \cdot (\mu_2 - \mu_1)\|_2 \cdot \sqrt{2\ln(2/\delta)}\end{aligned} \tag{A.1}$$

以至少 $1-\delta$ 的概率。

事实 A.7。 对于 $x \in (0, \ln(2))$，有 $e^x \leq 1 + 2x$

证明。 考虑函数 $f(x) = 1 + 2x - e^x$。于是 $f''(x) = -e^x$，所以 f是凹函数。注意， $f(0) = 0$且 $f(\ln(2)) = 1 + 2\ln(2) - 2 > 0$，因此对于 $x \in [0, \ln(2)]$， $f(x) \geq 0$（由凹性可知）。 □

引理 A.8 ([AL22], 引理 3.2)。 设 $\mathcal{S}^d$ 为所有 $d \times d$ 正定矩阵的集合。对于 A， $B \in \mathcal{S}^d$定义 $\mathrm{dist}(A, B) = \max\{\|A^{-1/2}BA^{-1/2} - I\|, \|B^{-1/2}AB^{-1/2} - I\|\}$。则 $(\mathcal{S}^d, \mathrm{dist})$是一个半度量空间，满足 $(3/2)$-近似 1-受限三角不等式。

事实 A.9。 设 Σ_1, Σ_2 为 $d \times d$ 正定矩阵。则 $\Sigma_2^{-1/2}\Sigma_1\Sigma_2^{-1/2}$ 和 $\Sigma_1^{1/2}\Sigma_2^{-1}\Sigma_1^{1/2}$ 具有相同的谱。

证明。 假设 $x \in \mathbb{R}^d$ 是 $\Sigma_2^{-1/2}\Sigma_1\Sigma_2^{-1/2}$ 的特征向量，对应的特征值为 λ。令 $y = \Sigma_1^{1/2}\Sigma_2^{-1/2}x$。则

$$\Sigma_1^{1/2}\Sigma_2^{-1}\Sigma_1^{1/2}y = \Sigma_1^{1/2}\Sigma_2^{-1/2}\left(\Sigma_2^{-1/2}\Sigma_1\Sigma_2^{-1/2}\right)x = \lambda\Sigma_1^{1/2}\Sigma_2^{-1/2}x = \lambda y.$$

换句话说， y 是 $\Sigma_1^{1/2}\Sigma_2^{-1}\Sigma_1^{1/2}$ 的特征向量，其特征值为 λ。 □

B 高斯分布的全变差距离

本节中，我们证明以下定理。

定理 1.8。 设 μ_1， $\mu_2 \in \mathbb{R}^d$和 Σ_1， Σ_2是 $d \times d$正定矩阵。假设我们有$d_{\mathrm{TV}}(\mathcal{N}(\mu_1, \Sigma_1)\ \mathcal{N}(\mu_2, \Sigma_2)) < \frac{1}{600}$。令

$$\Delta = \max\left\{\|\Sigma_1^{-1/2}\Sigma_2\Sigma_1^{-1/2} - I_d\|_F, \|\Sigma_1^{-1/2}(\mu_1 - \mu_2)\|_2\right\}.$$

Then

$$\frac{1}{200}\Delta \leq d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1,\Sigma_1), \mathcal{N}(\mu_2,\Sigma_2)\right) \leq \frac{1}{\sqrt{2}}\Delta.$$

我们的证明使用了[DMR18]中的以下两个定理。

定理 B.1 ([DMR18], 定理 1.1)。 设 $\mu \in \mathbb{R}^d$, Σ_1, $\Sigma_2 \in \mathcal{S}^d$, 均值相同的高斯分布之间的全变差距离有界为

$$\frac{\min\left\{1, \|\Sigma_1^{-1/2}\Sigma_2\Sigma_1^{-1/2} - I_d\|_F\right\}}{100} \leq d_{\mathrm{TV}}\left(\mathcal{N}(\mu, \Sigma_1), \mathcal{N}(\mu, \Sigma_2)\right)$$

定理 B.2 ([DMR18], 定理1.3)。 一维高斯分布之间的全变差距离满足以下上界

$$\frac{1}{200}\min\left\{1, \max\left\{\frac{|\sigma_1^2 - \sigma_2^2|}{\sigma_1^2}, \frac{40|\mu_1 - \mu_2|}{\sigma_1}\right\}\right\} \leq d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1, \sigma_1^2), \mathcal{N}(\mu_2, \sigma_2^2)\right) \leq \frac{3|\sigma_1^2 - \sigma_2^2|}{2\sigma_1^2} + \frac{|\mu_1 - \mu_2|}{2\sigma_1}.$$

引理 B.3. $d_{\mathrm{TV}}\left(\mathcal{N}(0, \Sigma_1)\ \mathcal{N}(0, \Sigma_2)\right) \leq 2 \cdot d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1, \Sigma_1)\ \mathcal{N}(\mu_2, \Sigma_2)\right)$。

证明。 设 X_1, X_2, Y_1, Y_2 是独立随机变量, 其中 X_1, $X_2 \sim \mathcal{N}(\mu_1, \Sigma_1)$ 且 Y_1, $Y_2 \sim \mathcal{N}(\mu_2, \Sigma_2)$。应用事实 A.1 可得

$$\begin{aligned} d_{\mathrm{TV}}\left((X_1, X_2), (Y_1, Y_2)\right) &\leq d_{\mathrm{TV}}\left(X_1, Y_1\right) + d_{\mathrm{TV}}\left(X_2, Y_2\right) \\ &= d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1, \Sigma_1), \mathcal{N}(\mu_2, \Sigma_2)\right) + d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1, \Sigma_1), \mathcal{N}(\mu_2, \Sigma_2)\right) \\ &= 2 \cdot d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1, \Sigma_1), \mathcal{N}(\mu_2, \Sigma_2)\right). \end{aligned}$$

现在, 设 $X = (X_1, X_2)$ 和 $Y = (Y_1, Y_2)$, 并定义函数 $f(X) = f(X_1, X_2) = (X_1 - X_2)/\sqrt{2}$。然后应用事实 A.2 可得

$$d_{\mathrm{TV}}\left(f(X_1, X_2), f(Y_1, Y_2)\right) \leq d_{\mathrm{TV}}\left((X_1, X_2), (Y_1, Y_2)\right) \leq 2 \cdot d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1, \Sigma_1), \mathcal{N}(\mu_2, \Sigma_2)\right).$$

注意, 若 $X_1, X_2 \sim \mathcal{N}(\mu_1, \Sigma_1)$, 则 $f(X) \sim \mathcal{N}(0, \Sigma_1)$。因此我们有

$$d_{\mathrm{TV}}\left(\mathcal{N}(0, \Sigma_1), \mathcal{N}(0, \Sigma_2)\right) \leq 2 \cdot d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1, \Sigma_1), \mathcal{N}(\mu_2, \Sigma_2)\right),$$

如所需。 □

引理 B.4. 设 $\mu \in \mathbb{R}^d$。若 $d_{\mathrm{TV}}\left(\mathcal{N}(0, I_d)\ \mathcal{N}(\mu, I_d)\right) \leq 3\alpha < 1/200$ 则 $\|\mu\|_2 \leq 15\alpha$。

证明。 设 $g_1 \sim \mathcal{N}(0, I_d)$, $g_2 \sim \mathcal{N}(\mu, I_d)$ 且 $v = \mu/\|\mu\|_2$。注意, $v^\top g_1 \sim \mathcal{N}(0, 1)$ 且 $v^\top g_2 \sim \mathcal{N}(\|\mu\|_2, 1)$。应用事实 A.2 (其中 $f(x) = v^\top x$) 可得

$$d_{\mathrm{TV}}\left(\mathcal{N}(0, 1), \mathcal{N}(\|\mu\|_2, 1)\right) \leq d_{\mathrm{TV}}\left(\mathcal{N}(0, I_d), \mathcal{N}(\mu, I_d)\right) \leq 3\alpha < 1/200.$$

应用定理B.2 于左侧, 可得

$$\frac{1}{200}\min\left\{1, 40\|\mu\|_2\right\} \leq d_{\mathrm{TV}}\left(\mathcal{N}(0, 1), \mathcal{N}(\|\mu\|_2, 1)\right) \leq d_{\mathrm{TV}}\left(\mathcal{N}(0, I_d), \mathcal{N}(\mu, I_d)\right) \leq 3\alpha < 1/200.$$

注意, 这意味着 $\min\left\{1, 40\|\mu\|_2\right\} = 40\|\mu\|_2 < 1$。因此我们得出结论: $\|\mu\|_2 \leq 15\alpha$。 □

引理 B.5 . 设 $\mu_1, \mu_2 \in \mathbb{R}^d$ 和 Σ_1, Σ_2 是满秩 $d \times d$ 正定矩阵。假设 t *hat*

$$d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1, \Sigma_1), \mathcal{N}(\mu_2, \Sigma_2)\right) \leq \alpha < \frac{1}{600}.$$

那么 *(i)* $\|\Sigma_1^{-1/2}\Sigma_2\Sigma_1^{-1/2} - I_d\|_F \leq 200\alpha$ 和 *(ii)* $\|\Sigma_1^{-1/2}\left(\mu_1 - \mu_2\right)\|_2 \leq 15\alpha$。

证明。 (i) 从假设出发

$$d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1,\Sigma_1),\mathcal{N}(\mu_2,\Sigma_2)\right)\leq\alpha<\frac{1}{600},$$

我们应用引理B.3 得到

$$d_{\mathrm{TV}}\left(\mathcal{N}(0,\Sigma_1),\mathcal{N}(0,\Sigma_2)\right)\leq 2\alpha<\frac{1}{300}.$$

应用定理B.1 可得

$$\min\left\{1,\|\Sigma_1^{-1/2}\Sigma_2\Sigma_1^{-1/2}-I_d\|_F\right\}\leq 100\cdot d_{\mathrm{TV}}\left(\mathcal{N}(0,\Sigma_1),\mathcal{N}(0,\Sigma_2)\right)\leq 200\alpha<\frac{1}{3}.$$

注意，该不等式意味着 $\min\left\{1,\|\Sigma_1^{-1/2}\Sigma_2\Sigma_1^{-1/2}-I_d\|_F\right\}=\|\Sigma_1^{-1/2}\Sigma_2\Sigma_1^{-1/2}-I_d\|_F$。由此可得

$$\|\Sigma_1^{-1/2}\Sigma_2\Sigma_1^{-1/2}-I_d\|_F\leq 200\alpha.$$

这证明了第一个断言。

(ii) 根据三角不等式，我们有

$$\begin{aligned}d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1,\Sigma_1),\mathcal{N}(\mu_2,\Sigma_1)\right)&\leq d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1,\Sigma_1),\mathcal{N}(\mu_2,\Sigma_2)\right)+d_{\mathrm{TV}}\left(\mathcal{N}(\mu_2,\Sigma_1),\mathcal{N}(\mu_2,\Sigma_2)\right)\\&=d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1,\Sigma_1),\mathcal{N}(\mu_2,\Sigma_2)\right)+d_{\mathrm{TV}}\left(\mathcal{N}(0,\Sigma_1),\mathcal{N}(0,\Sigma_2)\right).\end{aligned}$$

我们的假设是

$$d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1,\Sigma_1),\mathcal{N}(\mu_2,\Sigma_2)\right)\leq\alpha<\frac{1}{600},$$

根据引理 B.3，可得

$$d_{\mathrm{TV}}\left(\mathcal{N}(0,\Sigma_1),\mathcal{N}(0,\Sigma_2)\right)\leq 2\alpha<\frac{1}{300}.$$

因此，我们有

$$d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1,\Sigma_1),\mathcal{N}(\mu_2,\Sigma_1)\right)\leq 3\alpha<\frac{1}{200}.$$

此外，由于双射保持全变差距离，我们有 e

$$\begin{aligned}d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1,\Sigma_1),\mathcal{N}(\mu_2,\Sigma_1)\right)&=d_{\mathrm{TV}}\left(\mathcal{N}(\Sigma_1^{-1/2}\mu_1,I_d),\mathcal{N}(\Sigma_1^{-1/2}\mu_2,I_d)\right)\\&=d_{\mathrm{TV}}\left(\mathcal{N}(0,I_d),\mathcal{N}(\Sigma_1^{-1/2}(\mu_1-\mu_2),I_d)\right).\end{aligned}$$

最后，应用引理 B.4 可得 $\|\Sigma_1^{-1/2}\left(\mu_1-\mu_2\right)\|_2\leq 15\alpha$。 □

定理 *1.8* 的证明。 下界由引理 B.5 得出。

上界是 Pinsker不等式 的标准应用，但为完整起见，我们给出证明。根据引理 B.5(i)， $\Sigma_2^{-1/2}\Sigma_1\Sigma_2^{-1/2}$ 的特征值都严格大于 $1/2$ （注意，在应用引理B.5 时我们交换了指标）。因此，根据事实 A.3 可知

$$D_{\mathrm{KL}}\left(\mathcal{N}(\mu_1,\Sigma_1)\parallel\mathcal{N}(\mu_2,\Sigma_2)\right)\leq\frac{1}{2}\left[\|\Sigma_2^{-1/2}\Sigma_1\Sigma_2^{-1/2}-I\|_F^2+(\mu_2-\mu_1)^\top\Sigma_2^{-1}(\mu_2-\mu_1)\right].$$

利用 Pinsker 不等式 （引理 A.4）以及已知事实 $\|\mu\|_\Sigma=\|\Sigma^{-1/2}\mu\|_2=\sqrt{\left(\mu^T\Sigma^{-1}\mu\right)}$，我们得到

$$d_{\mathrm{TV}}\left(\mathcal{N}(\mu_1,\Sigma_1),\mathcal{N}(\mu_2,\Sigma_2)\right)\leq\frac{1}{2}\sqrt{\left[\|\Sigma_2^{-1/2}\Sigma_1\Sigma_2^{-1/2}-I\|_F^2+(\mu_2-\mu_1)^\top\Sigma_2^{-1}(\mu_2-\mu_1)\right]}\leq\frac{\Delta}{\sqrt{2}}$$

至此，证明完毕。 □

C 差分隐私的标准事实

定义 C.1. 设 $\mathcal{D}_1$、$\mathcal{D}_2$ 是定义在 $\mathbb{R}^d$ 上的两个连续分布，f_1、f_2 分别是它们的密度函数。我们用 $\mathcal{L}_{\mathcal{D}_1\|\mathcal{D}_2}$: $\mathbb{R}^d \to \mathbb{R}$ 表示似然比的对数，即对于任意 $x \in \mathbb{R}^d$,

$$\mathcal{L}_{\mathcal{D}_1\|\mathcal{D}_2}(x) \coloneqq \ln \frac{f_1(x)}{f_2(x)}. \tag{C.1}$$

下述定义中，D、D' 仅在一个个体数据上有所不同，而函数 f 可以刻画最坏情况下变化的幅度。

定义 C.2 (L_1-敏感度（[DR+14]，定义 3.1）。函数 L_1-敏感度定义为：f：$\mathcal{X}^n \to \mathbb{R}^k$

$$\Delta(f) = \max_{D,D' \in \mathcal{X}^n : d_H(D,D') \le 1} ||f(D) - f(D')||_1$$

其中 d_H 是定义 1.5中定义的汉明距离

定义 C.3 (L_2-敏感度（[DR+14]，定义 3.8）。函数 L_2-敏感度定义为：f：$\mathcal{X}^n \to \mathbb{R}^k$

$$\Delta_2(f) = \max_{D,D' \in \mathcal{X}^n : d_H(D,D') \le 1} ||f(D) - f(D')||_2$$

其中 d_H 是定义 1.5中定义的汉明距离

参数为 σ 的高斯机制会对输出的 d 个分量分别添加经过缩放、服从 $\mathcal{N}(0,\sigma^2)$ 的噪声。

定理 C.4 (高斯机制 ([DR+14]，定理 3.22))。设 $\varepsilon \in (0,1)$ 为任意值。对于 $c^2 > 2ln(1.25/\delta)$，参数为 $\sigma \ge c\Delta_2 f/\varepsilon$ 的高斯机制是 (ε,δ)-差分隐私的。

对于给定函数，确保差分隐私所需的噪声量取决于该函数的敏感度。换言之，如果函数的敏感度有界，我们就可以通过添加加性噪声来保证隐私。函数的敏感度反映了其输入发生变化时，函数输出会变化多少。

定义 C.5 (截断拉普拉斯分布)。记作 TLap(Δ, ε, δ)，其概率密度函数为

$$f_{\mathrm{TLap}(\Delta,\varepsilon,\delta)}(x) \coloneqq \begin{cases} Be^{-|x|/\lambda} & x \in [-A,A] \\ 0 & x \notin [-A,A] \end{cases},$$

其中 $\lambda = \frac{\Delta}{\varepsilon}$, $A = \frac{\Delta}{\varepsilon}\ln\left(1 + \frac{e^\varepsilon - 1}{2\delta}\right)$, $B = 2\lambda \quad \frac{1}{(1-e^{-A/\lambda})}$。

定理 C.6 ([GDGK18], 定理 1)。假设 q：$\mathcal{X}^n \to \mathbb{R}$ 是一个具有 L_1-敏感度 Δ的函数。那么机制 $q(x) + Y$ 其中 $Y \sim$ 截断拉普拉斯机制$(\Delta,\varepsilon,\delta)$ 是 (ε,δ)-差分隐私。

定理 *C.7*（高级组合定理 [*DRV*10]）。设 $\mathcal{D}_1$、...、$\mathcal{D}_k$ 和 $\mathcal{D}'_1$、...、$\mathcal{D}'_k$ 是概率密度，且对于所有 $j \in [k]$，$\mathcal{D}_j$、$\mathcal{D}'_j$ 都是 *(ε, δ)*-不可区分的。令 $\mathcal{D} = (\mathcal{D}_1$、...、$\mathcal{D}_k)$ 和 $\mathcal{D}' = (\mathcal{D}'_1$、...、$\mathcal{D}'_k)$。那么对于每个 $\delta' > 0$，$\mathcal{D}$、$\mathcal{D}'$ 都是 *(ε′, kδ + δ′)*-不可区分的

$$\varepsilon' = \sqrt{2k\ln(1/\delta')}\varepsilon + k\varepsilon(e^\varepsilon - 1).$$

引理 C.8. 设 $\mathcal{D}_1,\ldots,\mathcal{D}_k$ 和 $\mathcal{D}'_1,\ldots,\mathcal{D}'_k$ 是空间 $\mathcal{X}$ 上的概率分布。假设对于所有 $j \in [k]$，$\mathcal{D}_j$ 和 $\mathcal{D}'_j$ 都是 (ε,δ)-不可区分的。设 $w = (w_1,..,w_k)$ 是一个概率向量，即对于 $j \in [k]$，$w_j \ge 0$，且 $\sum_{j\in[k]} w_j = 1$。那么概率分布 $\sum_{j\in[k]} w_j\mathcal{D}_j$ 和 $\sum_{j\in[k]} w_j\mathcal{D}'_j$ 是 (ε,δ)-不可区分的。

证明。 设 $\mathcal{D}=\sum_{j\in[k]} w_j\mathcal{D}_j$ 和 $\mathcal{D}'=\sum_{j\in[k]} w_j\mathcal{D}'_j$。固定一个集合 $S\subseteq\mathcal{X}$。则

$$\mathbb{P}_{x\sim\mathcal{D}}[x\in S]=\sum_{j=1}^{k} w_j\mathbb{P}_{x\sim\mathcal{D}_j}[x\in S]\le\sum_{j=1}^{k} w_j\left[e^{\varepsilon}\cdot\mathbb{P}_{x\in\mathcal{D}'_j}[x\in S]+\delta\right]=e^{\varepsilon}\cdot\mathbb{P}_{x\sim\mathcal{D}'}[x\in S]+\delta,$$

如所需。 □

引理 C.9 ([AL22], 引理 2.10)。 设 $\mathcal{D}_1,\mathcal{D}_2$ 是定义在 $\mathbb{R}^d$上的连续分布。如果

$$\mathbb{P}_{Y\sim\mathcal{D}_1}\left[\mathcal{L}_{\mathcal{D}_1\|\mathcal{D}_2}(Y)\ge\varepsilon\right]\le\delta\quad and\quad\mathbb{P}_{Y\sim\mathcal{D}_2}\left[\mathcal{L}_{\mathcal{D}_2\|\mathcal{D}_1}(Y)\ge\varepsilon\right]\le\delta$$

则 $\mathcal{D}_1,\mathcal{D}_2$ 是(ε,δ)-不可区分的。

D 第 2 节的缺失证明

D.1 定理 2.3 的证明

定理 *2.3* 的证明。 **隐私性证明**。 设 D 和 D' 是两个相邻数据集，并令 $\mathcal{A}$ 表示算法 1中指定的非隐私算法。注意， Q 在第 4 行计算得到，其敏感度小于 $\frac{2}{t}$。由于我们在第 7行使用截断拉普拉斯机制，因此（根据定理 C.6）

$$\mathbb{P}\left[\mathcal{A}(D)=\perp\right]\le e^{\varepsilon}\mathbb{P}\left[\mathcal{A}(D')=\perp\right]+\delta \tag{D.1}$$

现在证明，对于任意 $T\subseteq\mathcal{Y}$，我们有

$$\mathbb{P}\left[\mathcal{A}(D)\in T\right]\le e^{2\varepsilon}\mathbb{P}\left[\mathcal{A}(D')\in T\right]+3e^{\varepsilon}\delta\quad\text{and} \tag{D.2}$$

$$\mathbb{P}\left[\mathcal{A}(D)\in T\cup\{\perp\}\right]\le e^{2\varepsilon}\mathbb{P}\left[\mathcal{A}(D')\in T\cup\{\perp\}\right]+4e^{\varepsilon}\delta \tag{D.3}$$

这表明算法 1 是 (ε,δ)-差分隐私。为此，我们考虑两种不同的情况。

情况 1: $Q<0.8$。 在这种情况下， $\widetilde{Q}<0.8+\frac{2}{t\varepsilon}\ln\left(1+\frac{e^{\varepsilon}-1}{2\delta}\right)$ 以概率 1 因此 $\mathbb{P}\left[\mathcal{A}(D)=\perp\right]=1$。现在验证公式 (D.2) 和公式 (D.3) 成立。对于任意 $T\subseteq\mathcal{Y}$，我们有 $\mathbb{P}\left[\mathcal{A}(D)\in T\right]=0$，因此公式 (D.2) 显然成立。为验证公式 (D.3) 成立，我们应用公式 (D.1) 得到

$$\mathbb{P}\left[\mathcal{A}(D)\in T\cup\{\perp\}\right]=\mathbb{P}\left[\mathcal{A}(D)=\perp\right]\le e^{\varepsilon}\mathbb{P}\left[\mathcal{A}(D')=\perp\right]+\delta\le e^{\varepsilon}\mathbb{P}\left[\mathcal{A}(D')\in T\cup\{\perp\}\right]+\delta.$$

情况 2: $Q\ge0.8$。 设 $Y_1,\ldots,Y_t$和 $Y'_1,\ldots,Y'_t$分别为假设数据集为 D,D'时第 2 行的输出。设 j,j' 分别为假设数据集为 D,D'时第 8 行的输出。接下来，我们证明 $\mathrm{dist}(Y_j,Y'_j)\le r$。

令 $S=\{\ell\in[t]:\mathrm{dist}(Y_j,Y_\ell)\le r/2z\}$ 且 $S'=\{\ell\in[t]:\mathrm{dist}(Y'_j,Y'_\ell)\le r/2z\}$。根据定义， $|S|>0.6t$ 且 $|S'|>0.6t$（见第 8 行中的 j）。根据容斥原理，我们有 $|S\cap S'|=|S|+|S'|-|S\cup S'|>0.6t+0.6t-t=0.2t$。因此，若 $t\ge5$，则有 $|S\cap S'|>1$；又由于 $|S\cap S'|$ 是整数，我们必有 $|S\cap S'|\ge2$。由于 D和 D' 仅在一个数据点上不同，因此存在某个 $\ell\in S\cap S'$使得 $Y_\ell=Y'_\ell$。由此我们得出

$$\mathrm{dist}(Y_j,Y'_j)\le\mathrm{dist}(Y_j,Y_\ell)+\mathrm{dist}(Y_\ell,Y'_j)\le z\cdot(r/2z+r/2z)=r,$$

其中，在最后一个不等式中，我们用到了 dist 是一个 z-近似的 r受限三角不等式，且 $\mathrm{dist}(Y_j,Y_\ell)$、$\mathrm{dist}(Y_\ell,Y'_j)\le r$。

现在我们可以验证式（D.2）和式（D.3）成立。令 $\mathcal{M}$ 表示算法 1中描述的机制。任取 $T \subseteq \mathcal{Y}$。则有

$$\begin{aligned}\mathbb{P}\left[\mathcal{M}(D) \in T\right] &= \mathbb{P}\left[\mathcal{M}(D) \neq \perp\right] \mathbb{P}\left[\mathcal{B}(Y_j) \in T\right] \\ &\leq (e^{\varepsilon}\mathbb{P}\left[\mathcal{M}(D') \neq \perp\right] + \delta)(e^{\varepsilon}\mathbb{P}\left[\mathcal{B}(Y'_{j'}) \in T\right] + \delta) \\ &= (e^{2\varepsilon}\mathbb{P}\left[\mathcal{M}(D') \neq \perp\right] \mathbb{P}\left[\mathcal{B}(Y'_{j'}) \in T\right] + 2e^{\varepsilon}\delta + \delta^2 \\ &\leq e^{2\varepsilon}\mathbb{P}\left[\mathcal{M}(D) \in T\right] + 3e^{\varepsilon}\delta\end{aligned}$$

其中第一个不等式用到了以下事实： $\mathcal{B}$ 是一个$(r,\ \varepsilon,\ \delta)$-掩蔽机制，它满足公式 (D.2)。接下来，我们还有

$$\begin{aligned}\mathbb{P}\left[\mathcal{M}(D) \in \{\perp\} \cup T\right] &= \mathbb{P}\left[\mathcal{M}(D) = \perp\right] + \mathbb{P}\left[\mathcal{M}(D) \in T\right] \\ &\leq e^{\varepsilon}\mathbb{P}\left[\mathcal{M}(D') = \perp\right] + \delta + e^{2\varepsilon}\mathbb{P}\left[\mathcal{M}(D') \in T\right] + 3e^{\varepsilon}\delta \\ &\leq e^{2\varepsilon}\mathbb{P}\left[\mathcal{M}(D') \in \{\perp\} \cup T\right] + 4e^{\varepsilon}\delta.\end{aligned}$$

至此，隐私证明完成。

效用证明。我们将证明分为两部分。

1. 首先，我们证明 Y（含噪输出）集中在 Y^*附近。2. 其次，我们证明算法1 在第7行不会失败。

对于第一部分，我们知道 $\mathcal{B}$ 是 $(\frac{\alpha}{2z}, \beta)$ 集中的。此外，$\forall i \in [t], Y_i$ 满足 $\mathsf{dist}(Y^*, Y_i) < \frac{\alpha}{2z}$。我们有

$$\begin{aligned}\mathbb{P}[\mathrm{dist}(\widetilde{Y}, Y^*) > \frac{\alpha}{2} + \frac{\alpha}{2}] &\leq \mathbb{P}[z \cdot \mathrm{dist}(\widetilde{Y}, Y_j) + z \cdot \mathrm{dist}(Y_j, Y^*) > \frac{\alpha}{2} + \frac{\alpha}{2}] \\ &\leq \mathbb{P}[\mathrm{dist}(\widetilde{Y}, Y_j) + \mathrm{dist}(Y_j, F^*) > \frac{\alpha}{2z} + \frac{\alpha}{2z}] \\ &\leq \mathbb{P}[\mathrm{dist}(\widetilde{Y}, Y_j) > \frac{\alpha}{2z}] + \mathbb{P}[\mathrm{dist}(Y_j, Y^*) > \frac{\alpha}{2z}] \\ &\leq \beta + 0 \leq \beta,\end{aligned}$$

其中，第一个不等式由 r-受限的 z-近似三角不等式3 推出（因为根据假设 $\alpha/2z < r/4z^2$），最后一个不等式的第一部分由掩蔽机制的集中性推出。~我们得到 $\mathbb{P}[\mathrm{dist}(Y,\ Y_j) > \frac{\alpha}{2z}] = \beta$，因为 Y只是 Y_j的一个掩蔽版本。此外，$\mathbb{P}[\mathrm{dist}(Y_j,\ Y^*) > \frac{\alpha}{2z}] = 0$，因为 Y_j 是从 Y_i中选出的，并且根据我们的假设，它们中没有任何一个与 $\frac{\alpha}{2z}$ 的距离大于 Y^*。

对于第二部分，我们首先保证 Q 在第4 行中等于 1。为此，我们需要确保对所有 $i,\ j \in [t],\ \mathrm{dist}(Y_i,\ Y_j) \leq \frac{r}{2z}$。由三角不等式可知：

$$\mathrm{dist}(Y_i, Y_j) \leq z \cdot (\mathrm{dist}(Y_i, Y^*) + \mathrm{dist}(Y^*, Y_j))$$

因为 $\mathsf{dist}(Y_i, Y^*)$、$\mathsf{dist}(Y^*, Y_j) \leq \frac{r}{4z^2}$。所以我们得出 $Q = 1$。

~现在我们需要证明 $Q \leq 0.9$。根据第6行，$Q = Q + Z$。因此，只需证明 $|Z| \leq 0.1$。根据定义C.5 $|Z| \leq \frac{2}{t\varepsilon}\ln(1 + \frac{e^{\varepsilon}-1}{2\delta})$。根据 $t \geq \frac{20}{\varepsilon}\ln(1 + \frac{e^{\varepsilon}-1}{2\delta})$ we~这一假设，我们得出 $Q \leq 0.9$，因此算法1 不会在第7行失败。 □

E 第 3 节缺失证明

E.1 引理 3.2 的证明

引理3.2的证明。 我们的思路是将计算dist^k 的问题归约为二分搜索，并检查二分图是否存在完美匹配。

首先，对于每个 i、 $j \in [k]$，我们计算 $\mathrm{dist}(F_i, F_j)$。这需要时间 $k^2 T_{\mathrm{dist}}$。注意，

$$\mathrm{dist}^k((F_1, \ldots, F_k), (F'_1, \ldots, F'_k))$$

必须是这些 k^2 值之一。此外，注意我们可以确定是否

$$\mathrm{dist}^k((F_1, \ldots, F_k), (F'_1, \ldots, F'_k)) \leq x$$

对于任意数值 x，我们可以考虑以下二分图。两个互不相交的节点集为 $\{F_1, \ldots, F_k\}$ 和 $\{F'_1, \ldots, F'_k\}$，当且仅当 $\mathrm{dist}(F_i, F'_j) \leq x$ 时， F_i 和 F'_j 之间有一条边。然后，我们确定该图中是否存在完美二分图匹配，这至多需要 $O(k^3)$ 时间（例如，使用匈牙利算法）。因此，我们只需对由 $\{\mathrm{dist}(F_i, F'_j)\}_{i,j'}$ 给出的排序值进行二分搜索，即可计算 dist^k。 □

E.2 引理 3.4的证明

引理 3.4 的证明。计算 $\mathcal{B}^k_\sigma$ 只需要计算 $\mathcal{B}$ 总共 k 次并找到排列。前者耗时 $O(k \cdot T_{\mathcal{B}})$ 后者耗时 $O(k \log k)$（例如，通过对 k 个均匀随机数进行采样，然后排序）。 □

E.3 引理 3.5的证明

引理 3.5 的证明。首先，我们证明隐私性。设 $F = (F_1, \ldots, F_k) \in \mathcal{F}^k$ 和 $F' = (F'_1, \ldots, F'_k) \in \mathcal{F}_k$ 满足 $\mathrm{dist}^k(F, F') \leq \gamma$。换言之，存在一个排列 π，使得对所有 $i \in [k]$，都有 $\mathrm{dist}(F_i, F'_{\pi(i)}) \leq \gamma$。由于 $\mathcal{B}$ 是一个 $(\gamma, \varepsilon, \delta)$-掩蔽机制，我们知道 $\mathcal{B}(F_i)$ $\mathcal{B}(F'_{\pi(i)})$是 (ε, δ)-不可区分的。因此，根据高级组合定理（见定理 C.7），$(\mathcal{B}(F_1) \ldots, \mathcal{B}(F_k))$ 和 $(\mathcal{B}(F'_{\pi(1)}) \ldots, \mathcal{B}(F'_{\pi}(k)))$ 是 $(\varepsilon', k\delta + \delta')$-不可区分的，其中 ε' 如引理所述。由于 $\mathcal{B}^k_\sigma((F'_1, \ldots, F'_k))$ 与 $\mathcal{B}^k_\sigma((F'_{\pi(1)}, \ldots, F'_{\pi}(k)))$ 具有相同的分布，因此利用排列保持隐私性这一事实（见引理 C.8 ），我们得出 $\mathcal{B}^k_\sigma(F)$ 和 $\mathcal{B}^k_\sigma(F')$ 是 $(\varepsilon', k\delta + \delta')$-不可区分的。

最后，还需证明准确性（即 $\mathcal{B}^k_\sigma$ 是 $(\alpha, k\beta)$-集中）。事实上，给定 $F = (F_1, \ldots, F_k) \in \mathcal{F}^k$，我们知道 $\mathrm{dist}(\mathcal{B}(F_i)\ F_i) \leq \alpha$ 的概率至少为 $1-\beta$。因此，根据并集界，对于所有 $i \in [k]$，$\mathrm{dist}(\mathcal{B}(F_i)\ F_i) \leq \alpha$ 的概率至少为 $1 - k\beta$。由此可得，$\mathrm{dist}(\mathcal{B}(F)\ F) \leq \alpha$ 的概率至少为 $1 - k\beta$。 □

E.4 引理的证明 3.6

引理 3.6 的证明。设 $F, F', F'' \in \mathcal{F}^k$。我们需要证明，若 $\mathrm{dist}^k(F, F') \leq r$ 且 $\mathrm{dist}^k(F', F'') \leq r$，则 $\mathrm{dist}^k(F, F'') \leq z \cdot (\mathrm{dist}^k(F, F') + \mathrm{dist}^k(F', F''))$。为此，令 $\pi_1^* \in \arg\min_\pi \max^{i \in [k]}(F_i, F'_\pi(i))$，并令 $\pi_2^* \in \arg\min_\pi \max_{\in [k]}(F'_{\pi_1^*}(i)\ F''_\pi(i))$。由于 dist 满足 r-受限的 z-近似三角不等式

并且对于任意 i，若 $\mathrm{dist}(F_i, F'_{\pi_1^*(i)})$，$\mathrm{dist}(F'_{\pi_1^*(i)}, F''_{\pi_2^*(i)}) \le r$，则有

$$\begin{aligned}\mathrm{dist}(F_i, F''_{\pi_2^*(i)}) &\le z \cdot \left(\mathrm{dist}(F_i, F'_{\pi_1^*(i)}) + \mathrm{dist}(F'_{\pi_1^*(i)}, F''_{\pi_2^*(i)})\right) \\ &\le z \cdot \left(\mathrm{dist}^k(F, F') + \mathrm{dist}^k(F', F'')\right).\end{aligned}$$

特别是

$$\mathrm{dist}^k(F, F'') \le \max_{i\in[k]} \mathrm{dist}(F_i, F''_{\pi_2^*(i)}) \le z \cdot \left(\mathrm{dist}^k(F, F') + \mathrm{dist}^k(F', F'')\right), \tag{E.1}$$

如所要求。 □

F 引理 4.2 的证明

本节专门用于证明引理 4.2。特别是，我们将介绍满足引理 $\mathcal{B}_{\mathrm{Comp}}(w,\ \mu,\ \Sigma)$ 条件的掩蔽机制 4.2。为了向高斯分量$(w_i,\ \mu_i,\ \Sigma_i)$ 添加噪声，我们执行以下若干步骤:

1. 在小节 F.1中，我们讨论如何对单个分量的混合权重添加噪声。这是最直接的一步，因为我们只需使用高斯机制。2. 在小节 F.2中，我们讨论如何对单个分量的均值添加噪声。为此，我们使用经验重缩放高斯机制，其中利用经验协方差矩阵来调整添加到均值上的噪声。这与 Brown 等人 [BGSUZ21]使用的经验重缩放高斯机制有些相似。3. 在小节 F.3中，我们讨论如何对单个分量的协方差矩阵添加噪声。为此，我们使用 Ashtiani & Liaw [AL22]所述的加噪机制。

F.1 对混合权重加噪

为权重加噪时，我们只需使用高斯机制。令 $\mathcal{R}_{\mathrm{w}}(w,\eta) = \max(0, w+\eta g)$，其中$g \sim \mathcal{N}(0,1)$，且 $w, \eta \in \mathbb{R}$。

引理 F.1. 令 $\alpha, \beta, \delta > 0$, $\eta = \sqrt{2+2\frac{\alpha}{\ln(1/\beta)}}$，且 $\gamma \le \frac{\alpha\varepsilon}{2\sqrt{2}\left(2/\delta - \ln()\sqrt{1+\ln(1/\beta)}\right)}$。

1. 令 $w_1, w_2 \in \mathbb{R}$。若 $|w_1 - w_2| \le \gamma$，则 $\mathcal{R}_w(w_1,\eta)$ 和 $\mathcal{R}_w(w_2,\eta)$ 是(ε,δ)-不可区分的。*2.* 令 $w \in \mathbb{R}$。则 $|\mathcal{R}_w(w,\eta) - w| \le \alpha$，其成立概率至少为 $1-\beta$。

证明。 第一项直接由高斯机制定理 C.4 在分别代入$\Delta_2 f, \sigma$ 和 γ, η 后得到（再通过后处理处理 max）。第二项由高斯随机变量的标准尾界推出（例如，引理 A.5）。 □

F.2 对均值添加噪声

在本节中，我们证明机制 $\mathcal{R}_{\mathrm{Mean}}(\mu,\Sigma,\eta) = \mu + \eta g$ where $g \sim \mathcal{N}(0,\Sigma)$ 能有效地保护均值的隐私。

引理 F.2. 设 $\alpha, \beta, \delta > 0$, $\eta = \sqrt{3\ d + \frac{\alpha^2}{\ln(1/\beta)}}$，并设 $\gamma \le \min\left\{\frac{1}{2}, \frac{\varepsilon\alpha}{24\ln(2/\delta)\sqrt{d+\ln(1/\beta)}}\right\}$。设 $\mu_1, \mu_2 \in \mathbb{R}^d$，并设 Σ_1, Σ_2 是 $d \times d$ 正定矩阵。假设

1. $\max\{\|\Sigma_1^{1/2}\Sigma_2^{-1}\Sigma_1^{1/2} - I_d\|_F, \|\Sigma_2^{1/2}\Sigma_1^{-1}\Sigma_2^{1/2} - I_d\|_F\} \le \gamma$; *and*

2. $\max\{\|\mu_1-\mu_2\|_{\Sigma_1},\|\mu_1-\mu_2\|_{\Sigma_2}\}\le\gamma$。

那么，$\mathcal{R}_{MEAN}(\mu_1,\ \Sigma_1,\ \eta)$ 和 $\mathcal{R}_{MEAN}(\mu_2,\ \Sigma_2,\ \eta)$ 是$(\varepsilon,\ \delta)$-不可区分的。此外，若令 $\widetilde{\mu}=\mathcal{R}_{MEAN}(\mu,\ \Sigma,\ \eta)$，则 $\|\widetilde{\mu}-\mu\|_\Sigma\le\alpha$ 的概率至少为 $1-\beta$。

首先，我们证明一个关于隐私损失的界。

引理 F.3. 设 $\eta>0$ 和 $\gamma\in(0,\ 1/2]$。设 $\mu_1,\ \mu_2\in\mathbb{R}^d$，并设 $\Sigma_1,\ \Sigma_2$ 是 $d\times d$ 正定矩阵。假设

1. 最大值$\{\|\Sigma_1^{1/2}\Sigma_2^{-1}\Sigma_1^{1/2}-I_d\|_F,\|\Sigma_2^{1/2}\Sigma_1^{-1}\Sigma_2^{1/2}-I_d\|_F\}\le\gamma$;
以及 *2.* 最大值$\{\|\mu_1-\mu_2\|_{\Sigma_1},\|\mu_1-\mu_2\|_{\Sigma_2}\}\le\gamma$。

令 $Y\sim\mathcal{N}(\mu_1,\eta^2\Sigma_1)$ 并定义 $\mathcal{L}:=\mathcal{L}_{\mathcal{N}(\mu_1,\eta^2\Sigma_1)\|\mathcal{N}(\mu_2,\eta^2\Sigma_2)}(Y)$。则

$$\mathcal{L}\le\frac{\gamma^2}{2}+\frac{\gamma^2}{2\eta^2}+2\gamma\sqrt{\ln(2/\delta)}+2\gamma\ln(2/\delta)+2\gamma\sqrt{2\ln(2/\delta)}/\eta \tag{F.1}$$

概率至少为 $1-\delta$。

证明。 我们直接应用引理 A.6 并对式（A.1）中的每一项进行界定。对于第一项，利用事实 A.3 以及假设（由于 $\Sigma_2^{-1/2}\Sigma_1\Sigma_2^{-1/2}$ 的特征值至少为 $1/2$，且 $\gamma<1/2$），可得[6]

$$\begin{aligned}D_{\mathrm{KL}}\left(\mathcal{N}(\mu_1,\eta\Sigma_1)\,\|\,\mathcal{N}(\mu_2,\eta\Sigma_2)\right)&\le\frac{1}{2}\left[\|\Sigma_2^{-1/2}\Sigma_1\Sigma_2^{-1/2}-I_d\|_F^2+(\mu_2-\mu_1)^\top(\eta^2\Sigma_2)^{-1}(\mu_2-\mu_1)\right]\\&\le\frac{1}{2}\left[\gamma^2+\frac{\gamma^2}{\eta^2}\right]\end{aligned}$$

式（A.1）中的第二项有界于 $2\gamma\sqrt{\ln(2/\delta)}$。式（A.1）中的第三项有界于$2\gamma\ln(2/\delta)$。最后，第四项有界于 $(1+\gamma)\frac{\gamma}{\eta}\sqrt{2\ln(2/\delta)}$。 □

下一个引理表明，$\mathcal{R}_{\mathrm{MEAN}}(\mu,\Sigma,\eta)$ 在马氏距离意义下紧密集中于 μ。

引理 F.4。 令 $\widetilde{\mu}=\mathcal{R}_{MEAN}(\mu,\Sigma,\eta)$。则 $\mathbb{P}\left[\|\widetilde{\mu}-\mu\|_\Sigma^2\ge3\eta^2(d+\ln(1/\beta))\right]\le\beta$。

证明。 回忆 $\widetilde{\mu}=\mu+\eta\Sigma^{1/2}g$ 其中 $g\sim\mathcal{N}(0,I_d)$。因此，$\|\widetilde{\mu}-\mu\|_\Sigma^2=\eta^2\|g\|_2^2$。应用引理 A.5 可得

$$\begin{aligned}\mathbb{P}\left[\|\widetilde{\mu}-\mu\|_\Sigma^2\ge3\eta^2(d+\ln(1/\beta))\right]&=\mathbb{P}\left[\|g\|_2^2\ge3(d+\ln(1/\beta))\right]\\&\le\mathbb{P}\left[\|g\|_2^2\ge d+2\sqrt{d\ln(1/\beta)}+2\ln(1/\beta)\right]\\&\le1/\beta,\end{aligned}$$

其中，在第一个不等式中，我们使用了 $2\sqrt{d\ln(1/\beta)}\le d+\ln(1/\beta)$。 □

引理 *F.2* 的证明。 注意到

$$\gamma\le\frac{\varepsilon\alpha}{24\ln(2/\delta)\sqrt{d+\ln(1/\beta)}}\le\min\left\{\sqrt{\frac{\varepsilon}{2}},\sqrt{\frac{\varepsilon\alpha^2}{6(d+\ln(1/\beta))}},\frac{\varepsilon}{8\ln(2/\delta)},\frac{\varepsilon\alpha}{24\sqrt{\ln(2/\delta)(d+\ln(1/\beta))}}\right\}$$

因此，第一个结论由引理 C.9 得出；将 γ 和 η 代入引理 F.3，可使式（F.1）中的每一项都至多为 $\varepsilon/4$。根据引理 F.4 以及我们对 η的选择，可得准确性。 □

[6]Note that we use that $\Sigma_2^{-1/2}\Sigma_1\Sigma_2^{-1/2}$ and $\Sigma_1^{1/2}\Sigma_2^{-1}\Sigma_1^{1/2}$ have the same spectrum (see Fact A.9).

F.3 协方差矩阵加噪

定义 $\mathcal{R}_{\mathrm{Cov}}(\Sigma,\eta) = \Sigma^{1/2}(I_d+\eta G)(I_d+\eta G)^\top\Sigma^{1/2}$，其中 $G\in\mathbb{R}^{d\times d}$ 是一个矩阵，其元素独立地取自 $\mathcal{N}(0,1)$。我们需要以下引理，该引理改述自 [AL22]中的引理 5.1 和引理 5.2。证明见附录 F.5。

引理 F.5 ([AL22], 引理 5.1 和引理 5.2)。 存在绝对常数 $C_1, C_2 > 0$ ，使得以下结论成立。令 $\varepsilon,\delta,\beta\in(0,1]$，并设 $\eta = \frac{\alpha}{C_1\sqrt{d}(\sqrt{d}+\sqrt{\ln(4/\beta)})}$。

- 假设 $\gamma \le \frac{\varepsilon\alpha}{C_2\sqrt{d^2(d+\ln(4/\beta))\ln(2/\delta)}}$。若 Σ_1,Σ_2 是正定 $d\times d$ 矩阵，使得

$$\max\{\|\Sigma_1^{1/2}\Sigma_2^{-1}\Sigma_1^{1/2}-I_d\|,\|\Sigma_2^{1/2}\Sigma_1^{-1}\Sigma_2^{1/2}-I_d\|\}\le\gamma$$

- 则 $\mathcal{R}_{Cov}(\Sigma_1,\eta)$ 与 $\mathcal{R}_{Cov}(\Sigma_2,\eta)$ 是(ε,δ)-不可区分的。
  令 $\widetilde{\Sigma}=\mathcal{R}_{Cov}(\Sigma,\eta)$。则

$$\max\left\{\|\Sigma^{-1/2}\widetilde{\Sigma}\Sigma^{-1/2}-I_d\|_F,\|\widetilde{\Sigma}^{-1/2}\Sigma\widetilde{\Sigma}^{-1/2}-I_d\|_F\right\}\le\alpha$$

  以至少 $1-\beta$ 的概率。

F.4 掩蔽单个高斯分量

现在，我们利用前面三个小节来构造一种用于掩蔽单个分量的掩蔽机制。令 $\eta_{\mathrm{W}} = \frac{\alpha}{\sqrt{2+2\ln(1/\beta)}}$、$\eta_{\mathrm{Mean}} = \frac{\alpha}{\sqrt{3(d+\ln(1/\beta))}}$ 和 $\eta_{\mathrm{Cov}} = \frac{\alpha}{C_1(\sqrt{d}+\sqrt{\ln(4/\beta)})}$，其中常数 C_1 充分大。考虑如下机制

$$\mathcal{B}_{\mathrm{Comp}}(w,\mu,\Sigma)=(\mathcal{R}_{\mathrm{W}}(w,\eta_{\mathrm{W}}),\mathcal{R}_{\mathrm{Mean}}(\mu,\Sigma,\eta_{\mathrm{Mean}}),\mathcal{R}_{\mathrm{Cov}}(\Sigma,\eta_{\mathrm{Cov}})) \tag{F.2}$$

引理 *4.2* 的证明。 由 $\mathcal{B}_{\mathrm{Comp}}$ 是一个 $(\gamma,3\varepsilon,3\delta)$-掩蔽机制这一事实，可由引理 F.1、引理 F.2 和引理 F.5 结合基本组合得到。 是 $(\alpha,3\beta)$-集中的结论，也可由引理 F.1、引理 F.2 和引理 F.5 结合并集界得到。 □

引理 F.5 的证明

为证明引理 F.5，我们需要以下两个引理，它们出自 Ashtiani & Liaw [AL22]。注意，引理 F.7 与 Ashtiani & Liaw [AL22] 中的表述略有不同，但可由其证明轻易推出。

引理 F.6 ([AL22], 引理 5.1)。 设 $d\in\mathbb{N}$, $\eta>0$, $\varepsilon\in(0,1]$, $\delta\in(0,1]$, $\gamma>0$ 并假设

$$\gamma\le\min\left\{\sqrt{\frac{\varepsilon}{2d(d+1/\eta^2)}},\frac{\varepsilon}{8d\sqrt{\ln(2/\delta)}},\frac{\varepsilon}{8\ln(2/\delta)},\frac{\varepsilon\eta}{12\sqrt{d}\sqrt{\ln(2/\delta)}}\right\}. \tag{F.3}$$

设 Σ_1, Σ_2 是两个正定 $d\times d$ 矩阵。假设

$$\max\{\|\Sigma_1^{1/2}\Sigma_2^{-1}\Sigma_1^{1/2}-I_d\|,\|\Sigma_2^{1/2}\Sigma_1^{-1}\Sigma_2^{1/2}-I_d\|\}\le\gamma.$$

定义 $\mathcal{R}_{Cov}(\Sigma,\eta) = \Sigma^{1/2}(I+\eta G)(I+\eta G)^\top\Sigma^{1/2}$，其中 $G\sim\mathbb{R}^{d\times d}$ 是一个元素相互独立且服从$(0,1)$分布的矩阵。则 $\mathcal{R}_{Cov}(\Sigma_1,\eta)$ 与 $\mathcal{R}_{Cov}(\Sigma_2,\eta)$ 是(ε,δ)-不可区分的。

引理 F.7 ([AL22], 引理 5.2)。 存在一个足够大的常数 $C > 0$，使得以下结论成立。设 $\beta > 0$ 和 Σ 为正定矩阵，并令 $\eta = \frac{C\sqrt{d}}{\alpha}(\sqrt{d}+\sqrt{\ln(4/\beta)})$。若 $\Sigma = \mathcal{R}_{\mathrm{Cov}}(\Sigma, \eta)$，则

$$\max\left\{\|\Sigma^{-1/2}\widetilde{\Sigma}\Sigma^{-1/2} - I_d\|_F, \|\widetilde{\Sigma}^{-1/2}\Sigma\widetilde{\Sigma}^{-1/2} - I_d\|_F\right\} \le \alpha$$

概率至少为 $1-\beta$。

注 F.8. 引理*F.7* 在 *Ashtiani & Liaw* *[AL22]* 中是针对谱距离陈述的，而我们针对 *Frobenius* 距离陈述。因此，与 *Ashtiani & Liaw* η 相比，我们将其缩小了 $\sqrt{d}$ 倍 *[AL22]*。

引理的证明 *F.5*。 对于第一个断言，只需证明式（F.3）中的不等式成立。将 η 代入式（F.3）的第四项，可得

$$\gamma \le \frac{\varepsilon\alpha}{C_2\sqrt{d^2(d+\ln(4/\beta))}\ln(2/\delta)}. \tag{F.4}$$

因此，很明显 γ 被式（F.3）的第二项和第三项上界，只要 C_2 足够大。接下来，我们证明 γ 被式（F.3）的第一项上界。事实上，我们有

$$\eta^2 = \frac{\alpha^2}{C_1^2 d(\sqrt{d}+\sqrt{\ln(4/\beta)})^2} \ge \frac{\alpha^2}{2C_1^2 d(d+\ln(4/\beta))},$$

其中，在最后一个不等式中，我们利用了以下事实：$(a+b)^2 \le 2a^2+2b^2$ 对于任意实数 a，b。将此 η^2 上界代入式（F.3），经过一些计算可得

$$\sqrt{\frac{\varepsilon}{2d(d+1/\eta^2)}} \ge \sqrt{\frac{\varepsilon\alpha^2}{C_3 d^2(d+\ln(4/\beta))}}, \tag{F.5}$$

对于某个常数 $C_3 > 0$。因此，若 C_2 足够大，则式（F.4）右侧的上界为式（F.5）右侧。特别地，式（F.3）中最小的一项是第四项。最后，代入 η的值后，不难验证 γ 至多为式（F.4）中的最后一项。 □

G 第 5 节中的缺失证明

G.1 引理 5.1 的证明

证明。 将引理 3.5 应用于混合分布的掩蔽（将引理 3.5 中的 ε、δ 分别替换为 3ε、3δ），对于每个 $\delta' > 0$，有 $\mathcal{B}_{\mathrm{GMM}}$ 是一个 $(\gamma, \varepsilon', 3k\delta+\delta')$-掩蔽机制，其中

$$\varepsilon' = 3\sqrt{2k\ln(1/\delta')}\varepsilon + 3k\varepsilon(e^{3\varepsilon}-1).$$

一个 $(\gamma, 3\sqrt{2k\ln(1/\delta')}\varepsilon + 3k\varepsilon(e^{3\varepsilon}-1)\ 3k\delta+\delta')$-掩蔽机制。由于这对任意 δ'都成立，我们可以取$\delta' = 3k\delta$，并应用数值不等式 $e^x \le 1+2x$（当 $x < \ln(2)$ 时成立；参见事实 A.7），得到

$$\varepsilon' \le 3\sqrt{2k\ln(1/3k\delta)}\varepsilon + 18k\varepsilon^2,$$

最后，为了证明准确性部分（$\mathcal{B}_{\mathrm{GMM}}$ 是 $(\alpha,\ 3k\beta)$-集中），我们应用引理 3.5中关于混合分布掩蔽的准确性部分，该部分通过对所有 $i \in [k]$应用并集界得以证明。此外，将距离定义为三个分量参数中的最大值：权重 w、均值 μ和协方差矩阵 Σ。

$$\mathrm{dist}_{\mathrm{PARAM}}(\{(w_i,\mu_i,\Sigma_i)\}_{i\in[k]}, \{(w_i',\mu_i',\Sigma_i')\}_{i\in[k]}) = \min_{\pi}\max_{i\in[k]}\mathrm{dist}_{\mathrm{COMP}}((w_{\pi(i)},\mu_{\pi(i)},\Sigma_{\pi(i)}),(w_i',\mu_i',\Sigma_i')).$$

我们可以得出

$$\mathrm{dist}_{\mathrm{PARAM}}(\mathcal{B}_{\mathrm{GMM}}(\{(w_i,\mu_i,\Sigma_i)\}_{i\in[k]}),\{(w_i,\mu_i,\Sigma_i)\}_{i\in[k]})\le\alpha$$

以至少 $1-3k\beta$ 的概率。

现在，我们有 $\mathcal{B}_{\mathrm{GMM}}$ 是关于 $(\mathcal{F}_{\mathrm{GMM}},\mathrm{dist}_{\mathrm{PARAM}})$ 的 $(\gamma,3\sqrt{2k\ln(1/3k\delta)}\varepsilon+18k\varepsilon^2,6k\delta)$-掩蔽机制。此外，$\mathcal{B}_{\mathrm{GMM}}$ 是 $(\alpha,3k\beta)$-集中 的。

为简化表述，令 $\varepsilon'<\ln(2)/3$、$\delta'<1$、$\alpha'<\frac{1}{\varepsilon}$、$\beta'<1$ 为参数。我们设 $\delta=\delta'/6k$、$\beta=\beta'/3k$、$\alpha=\alpha'$ 和 $\varepsilon=\min\left\{\frac{\varepsilon'}{6\sqrt{2k}},\sqrt{\frac{\varepsilon'}{36k}}\right\}\ge\sqrt{72k\ln(2/\delta')}$。于是，对于充分大的常数 C，若 $\gamma\le C_2\sqrt{k\ln(2/\delta')}\varepsilon'\alpha'\ln()\sqrt{d(d+\ln(12k/\beta'))\ln(12k/\delta')}$，则 $\mathcal{B}_{\mathrm{GMM}}$ 是一个 $(\gamma,\varepsilon',\delta')$-掩蔽机制，并且是 (α',β')- 集中的。这证明了该结论。 □

G.2 引理的证明 5.2

引理的证明*5.2*。 引理 4.1 断言 $\mathrm{dist}_{\mathrm{COMP}}$ 满足 1-受限 $(3/2)$-近似三角不等式。因此，应用引理 3.6 （并回顾定义 3.1）$\mathrm{dist}_{\mathrm{PARAM}}$ 满足 1-受限$(3/2)$-近似三角不等式。 □

H 第 6 节的缺失证明 6

引理的证明 *6.3*。 回顾定义 1.4 可知 $\mathrm{dist}_{\mathrm{GMM}}$ 定义为

$$\mathrm{dist}_{\mathrm{GMM}}(F,F')=\min_{\pi}\max_{i\in[k]}\max\left\{|w_i-w'_{\pi(i)}|,d_{\mathrm{TV}}\left(\mathcal{N}(\mu_i,\Sigma_i),\mathcal{N}(\mu'_{\pi(i)},\Sigma'_{\pi(i)})\right)\right\}$$

其中 π 取自 $[k]$上的所有排列构成的集合。另外回顾一下

$$\mathrm{dist}_{\mathrm{PARAM}}(F,F')=\min_{\pi}\max_{i\in[k]}\mathrm{dist}_{\mathrm{COMP}}((w_{\pi(i)},\mu_{\pi(i)},\Sigma_{\pi(i)}),(w'_i,\mu'_i,\Sigma'_i)),$$

其中 $\mathrm{dist}_{\mathrm{COMP}}$ 的定义见第 4节。

根据定理 1.8，可以直接验证 $\frac{1}{200}$ 距离$_{\mathrm{PARAM}}(F,F')\le$距离$_{\mathrm{GMM}}(F,F')\le\frac{1}{\sqrt{2}}\mathrm{dist}_{\mathrm{PARAM}}(F,F')$。 □