Supplementary Material

This supplementary material consists of two sections. The first section provides basic formulae for the MAP estimates under the mixture of Gaussians model; and the second section provides moment calculations for the Laplace and Gaussian mechanisms.

1 MAP estimates under the MoG models

For the maximum a posteriori estimate, we impose the Dirichlet prior on $\boldsymbol{\pi} \sim \text{Dir}(\boldsymbol{\alpha})$ and Normal-inverse-Wishart prior on $p(\boldsymbol{\mu}_k, \Sigma_k) = \text{NIW}(\mathbf{0}, \kappa_0, \nu_0, S_0)$, where the MAP estimates are

$$\pi_k^{MAP} = \frac{N\pi_k^{MLE} + \alpha_k - 1}{N + \sum_k \alpha_k - K}, \quad \boldsymbol{\mu}_k^{MAP} = \frac{N_k \boldsymbol{\mu}_k^{MLE}}{N_k + \kappa_0},$$
$$\Sigma_k^{MAP} = \frac{S_0 + N_k \Sigma_k^{MLE} + \frac{\kappa_0 N_k}{\kappa_0 + N_k} \boldsymbol{\mu}_k^{MLE} \boldsymbol{\mu}_k^{MLE\top}}{\nu_0 + N_k + d + 2}.$$

In this paper we set hyperparameters to conventional values, e.g. $\boldsymbol{\alpha} = [2, 2, \cdots, 2], \kappa_0 = 1, \nu_0 = d + 2, S_0 = \text{diag}(0.1, \cdots 0.1)$, rather than optimizing them, cf. [1].

2 λ-th Moment Calculations

2.1 Laplace Mechanism

Univariate Laplace mechanism. Suppose we use the univariate Laplace mechanism where the sensitivity is 1 and we add Laplace noise with parameter $\frac{1}{\epsilon}$. Then the privacy loss r.v. is:

$$\begin{aligned} Z &= \epsilon, \quad w.p\, \frac{1}{2} \\ &= -\epsilon, \quad w.p\, \frac{e^{-\epsilon}}{2} \\ &= \epsilon(1-2t), \quad \text{with density } \frac{\epsilon}{2} e^{-\epsilon t}, 0 \le t \le 1 \end{aligned}$$

This leads to the moment generating function:

$$\alpha_M(\lambda) = \mathbb{E}[e^{\lambda Z}] = \left(\frac{\lambda+1}{2\lambda+1}\right) e^{\lambda\epsilon} + \left(\frac{\lambda}{2\lambda+1}\right) e^{-(\lambda+1)\epsilon}.$$

Multivariate Laplace Mechanism with bounded L_1 sensitivity Suppose we use the d-variate Laplace mechanism where the L_1-sensitivity is equal to Δ; in this case, we add Laplace noise with parameter Δ/ϵ to each coordinate of the vector. Then the privacy loss random variable may be written as follows:

$$Z = \log \frac{e^{-\epsilon|t|_1}/\Delta}{e^{-\epsilon|\mu-t|_1}/\Delta} \quad w.p. \quad \frac{\epsilon^d}{\Delta^d 2^d} e^{-\epsilon|t|_1/\Delta},$$

which is the same as:

$$Z = \frac{\epsilon}{\Delta}(|\mu - t|_1 - |t|_1), \quad w.p. \quad \frac{\epsilon^d}{(2\Delta)^d} e^{-\epsilon|t|_1/\Delta}$$

Here μ is the difference between $f(D)$ and $f(D')$ and has the property that $|\mu|_1 \leq \Delta$. Let $\varepsilon = \epsilon/\Delta$. For a given μ, this leads to the moment generating function:

$$\begin{aligned}
\mathbb{E}[e^{\lambda Z}] &= (\varepsilon/2)^d \int_{R^d} e^{\lambda\varepsilon(|\mu-t|_1-|t|_1)} \times e^{-\varepsilon|t|_1} dt \\
&= \left(\prod_j \frac{\varepsilon}{2} \int_{-\infty}^{\infty} e^{\lambda\varepsilon|\mu_j-t_j|-(\lambda+1)\varepsilon|t_j|} dt_j \right) \\
&= \left(\prod_j \left(\frac{\lambda+1}{2\lambda+1} e^{\lambda\varepsilon|\mu_j|} + \frac{\lambda}{2\lambda+1} e^{-(\lambda+1)\varepsilon|\mu_j|} \right) \right)
\end{aligned}$$

What we need is an upper bound on the functional $\mathbb{E}[e^{\lambda Z}]$ for any λ over all μ for which $|\mu|_1 \leq \Delta$. For positive λ, we note that the function $\mathbb{E}[e^{\lambda Z}]$ is convex in $|\mu|_j$, and therefore the maximum value occurs when $\mu = \Delta e_j$ where e_j is some coordinate vector. This maximum value is:

$$\frac{\lambda+1}{2\lambda+1} e^{\lambda\varepsilon\Delta} + \frac{\lambda}{2\lambda+1} e^{-(\lambda+1)\varepsilon\Delta}.$$

2.2 Multivariate Gaussian Mechanism

Suppose we use the d-variate Gaussian Mechanism where the L_2-sensitivity is 1 and we add multivariate spherical Gaussian noise $N(0, \sigma^2 I_d)$. Then, the privacy loss random variable can be written as follows:

$$Z = \frac{1 - 2x^\top \Delta}{2\sigma^2}, \quad w.p \ \frac{1}{\sigma(2\pi)^{d/2}} e^{-\|x\|^2/2\sigma^2}, \tag{1}$$

where Δ is any $d \times 1$ vector with unit norm. This in turn leads to the moment generating function:

$$\alpha_M(\lambda) = \mathbb{E}[e^{\lambda Z}] = e^{(\lambda+\lambda^2)/2\sigma^2}.$$

References

[1] C. M. Bishop. *Pattern recognition and machine learning*. Springer New York:, 2006.