Lecture : Approximate DP (... Contd.)

In the last lecture, we encountered the definition and properties of (ϵ, δ)-DP and discussed the Gaussian mechanism that respects (ϵ, δ)-DP (with a proof for at least certain $(\epsilon, \delta, \Delta)$ values). We shall now take a look at an important ramification of using (ϵ, δ)-DP (via the Gaussian mechanism).

Note first that for any given $f: \mathcal{D} \to \mathbb{R}^d$, we have $\Delta_2 \le \Delta_1 \le \sqrt{d}\, \Delta_2$.

<u>HW</u>: Prove the above assertion. <u>Hint</u>: One direction may require application of Jensen's inequality to a suitable RV.

Thus, the "amount of noise added" (i.e., the standard deviation of noise) is typically smaller for (ϵ, δ)-DP under the Gaussian mechanism, than for ϵ-DP under the Laplace mechanism, <u>for sufficiently large d</u>.

The following argument makes this more precise:

[<u>FACT</u>: For $\underline{Z} = (Z_1, \cdots, Z_d) \sim \mathcal{N}(\underline{0}, \sigma^2 I_d)$, we have

(i) $\mathbb{E}[\|\underline{Z}\|_2^2] = \sigma^2 d$

(ii) $\mathbb{E}[\|Z\|_2^{\cancel{2}}] \le \sigma\sqrt{d}$, and

(iii) $\mathbb{E}\left[\max(|Z_1|, \dots, |Z_d|)\right] \leq \sigma \cdot O(\sqrt{\ln d})$

Assume that $\Delta = \Delta_f = \Theta(1)$. Then,

- We have under the Laplace mechanism for ϵ-DP :

$$\mathbb{E}\left[\max_{j=1}^{d} \left| f_j(\underline{x}) - M_\epsilon^{Lap}(\underline{x}) \right| \right] \leq O\left(\frac{d \ln d}{\epsilon}\right),$$

- We have under the Gaussian mechanism for (ϵ, δ)-DP:

$$\mathbb{E}\left[\max_{j=1}^{d} \left| f_j(\underline{x}) - M_{\epsilon,\delta}^{G}(\underline{x}) \right| \right] \leq O\left(\frac{\sqrt{d \log d \cdot \log(1/\delta)}}{\epsilon}\right).$$

Thus, for sufficiently large d, the <u>maximum</u> error across the d queries in f is smaller under (ϵ, δ)-DP than under ϵ-DP.