

Theory of Differential Privacy

Lecture 4:

- Accuracy of RNM
- Approximate DP
- Gaussian Mechanism

EN.601.438/638 Fall 2026

Lydia Zakynthinou

Johns Hopkins University

Sept 14, 2026

Report Noisy Max

Step 1:
 $\forall y \in \mathcal{Y} : q(y; x) + Z_y = \tilde{q}(y; x), \quad Z_y \sim \text{Exp}\left(\frac{2\Delta}{\epsilon}\right).$

Step 2:
Output : $\hat{y} = \underset{y \in \mathcal{Y}}{\operatorname{argmax}} \tilde{q}(y; x)$

$\uparrow$
 $\Pr[Z_y \geq t] = e^{-t/b}, t \geq 0.$

Accuracy

let $y^* = \underset{y \in \mathcal{Y}}{\operatorname{argmax}} q(y; x).$

We release $\hat{y} : \tilde{q}(\hat{y}; x) = q(\hat{y}; x) + Z_{\hat{y}} \geq q(y^*; x) + Z_{y^*}.$

$\Leftrightarrow q(y^*; x) - q(\hat{y}; x) \leq Z_{\hat{y}}. \quad \geq q(y^*; x)$

$\Pr[q(y^*; x) - q(\hat{y}; x) > g] \leq \Pr[Z_{\hat{y}} > g] \quad (*)$

$$\Pr[Z \geq bt] = e^{-t}$$

$$\Pr[Z_{\max} \geq bt + b \log d] \leq d \cdot e^{-(\log d + t)} = e^{-t} \quad (1)$$

$$\text{w.p. } 1 - e^{-t} : Z_{\max} \leq b(t + \log d).$$

(of all d
expon. r.v.)

$$(*) \leq \Pr[Z_{\max} > g] = \Pr[Z_{\max} \leq b(t + \log d)] \stackrel{(1)}{\leq} e^{-t}$$

$$\xrightarrow{\text{replace } b \rightarrow \frac{2\Delta}{\epsilon}} \text{w.p. } 1 - e^{-t} : q(y^*; x) - q(\hat{y}; x) \leq \frac{2\Delta}{\epsilon} (t + \log d)$$

$$\Rightarrow \text{w.p. } 1 - \delta : q(y^*; x) - q(\hat{y}; x) \leq \frac{2\Delta}{\epsilon} (\log(1/\delta) + \log d) \quad \square$$

Approximate DP

An algorithm is (ϵ, δ) -DP if $\forall x \sim x'$, for every event E :

$$\Pr[A(x) \in E] \leq e^\epsilon \Pr[A(x') \in E] + \delta$$

Ex.

$$A(x) = \begin{cases} x & , \text{ w.p. } \delta \\ \perp & , \text{ w.p. } 1-\delta \end{cases}$$

$$\Pr[A(x) \in E \\ = 0]$$

$$\Pr[A(x') \in E \\ = 0]$$

A is $(0, \delta)$ -DP.

δ : very small $\rightarrow 10^{-6}$, $\ll \frac{1}{n}$.

Privacy loss

For x , p_x is the distribution of $A(x)$. For every $y \in \text{range}(A)$.

$$L_{x \rightarrow x'}(y) = \log \frac{p_x(y)}{p_{x'}(y)}$$

Pure DP: $L_{x \rightarrow x'}(y) \leq \epsilon \quad \forall y$

Approximate DP: let $Y \sim A(x)$:

$$\Pr_{Y \sim A(x)} [L_{x \rightarrow x'}(Y) > \epsilon] \leq \delta$$

then A is (ϵ, δ) -DP.

Proof sketch: BAD: $\{y : L_{x \rightarrow x'}(y) > \epsilon\}$.

$$\begin{aligned} \Pr[A(x) \in E] &= \Pr[A(x) \in E \cap B] + \Pr[A(x) \in E \cap B^c] \\ &\leq \delta + \Pr[A(x) \in E \cap B^c] \end{aligned}$$

$$\leq \delta + e^\varepsilon \Pr[A(x') \in E \cap B^c]$$

$$\leq \delta + e^\varepsilon \Pr[A(x') \in E]$$



Gaussian Mechanism

$$f: \mathcal{X}^n \rightarrow \mathbb{R}^d.$$

$$A(x) = f(x) + Z, \quad Z \sim N(0, \sigma^2 \mathbb{I}_d)$$

Thm. If $\sigma = \frac{\Delta_2 \sqrt{2 \log(2/\delta)}}{\varepsilon}$, where $\Delta_2 \geq \sup_{x \sim x'} \|f(x) - f(x')\|_2$.

then A is (ε, δ) -DP.

Proof: $Y = f(x) + Z, \quad Z \sim N(0, \sigma^2 \mathbb{I}_d) \Rightarrow Y \sim N(f(x), \sigma^2 \mathbb{I}_d).$

$\sup \|f(x) - f(x')\|_2 \leq \Delta$. write $f(x) - f(x') = v$.

$$L_{x \rightarrow x'}(Y) = \log \frac{\exp(-\|Y - f(x)\|^2 / 2\sigma^2)}{\exp(-\|Y - f(x')\|^2 / 2\sigma^2)} = \frac{\|Y - f(x')\|^2 - \|Y - f(x)\|^2}{2\sigma^2}.$$

$$= \frac{\|z+v\|^2 - \|z\|^2}{2\sigma^2} = \frac{\|v\|^2}{2\sigma^2} + \frac{\langle z, v \rangle}{\sigma^2} \quad (*)$$

$$\langle z, v \rangle \sim N(0, \sigma^2 \|v\|^2)$$

$$G = \frac{\langle z, v \rangle}{\sigma \|v\|} \sim N(0, 1) \text{ . Write } \alpha = \frac{\|v\|}{\sigma} \text{ .}$$

$$(*) \quad L = \alpha G + \frac{\alpha^2}{2} \quad \mathbb{E}[L] = \frac{\alpha^2}{2} \quad , \quad \text{Var}(L) = \alpha^2 \text{ .}$$

$$\Pr[L > \varepsilon] \stackrel{*}{=} \Pr\left[G > \underbrace{\frac{\varepsilon}{\alpha} - \frac{\alpha}{2}}_{h(\alpha)}\right] \leq \Pr\left[G > c - \frac{\varepsilon}{2c}\right] (**)$$

$$c = \sqrt{2 \log(2/\delta)} \quad , \quad \sigma = \frac{\Delta_2 \cdot c}{\varepsilon} \quad , \quad \alpha = \frac{\|v\|}{\sigma} \leq \frac{\Delta_2}{\sigma} = \frac{\varepsilon}{c}$$

$$h(\alpha) = \frac{\varepsilon}{\alpha} - \frac{\alpha}{2} \quad \searrow \quad h(\alpha) \geq c - \frac{\varepsilon}{2c} = h\left(\frac{\varepsilon}{c}\right)$$

$$* \quad \alpha G + \frac{\alpha^2}{2} > \varepsilon \Leftrightarrow G + \frac{\alpha}{2} > \frac{\varepsilon}{\alpha} \Leftrightarrow G > \frac{\varepsilon}{\alpha} - \frac{\alpha}{2}$$

(**)

use $\Pr[G > t] \leq e^{-t^2/2}$ (tail bound for $N(0,1)$)

$$t = c - \frac{\varepsilon}{2c}.$$

Remains to show $e^{-t^2/2} < \delta \Leftrightarrow t^2/2 > \log(1/\delta).$

$$\Leftrightarrow \left(c - \frac{\varepsilon}{2c}\right)^2 / 2 > \log(1/\delta).$$

Ex. $f: X \rightarrow \mathbb{R}$ $\Delta = \sup_{x \sim x'} |f(x) - f(x')|,$

Laplace.

ε -DP

$$\text{error} \leq \frac{\Delta}{\varepsilon}$$

Gaussian

(ε, δ) -DP

$$\text{error} = \frac{\Delta \sqrt{2 \log(2/\delta)}}{\varepsilon}.$$

Ex. 2. $f: \mathcal{X}^m \rightarrow \mathbb{R}^k$

$$f(x) = (f_1(x), \dots, f_k(x))$$

$$\Delta_1 = k$$

$$\Delta_2 = \sqrt{k}$$

Laplace

$$Z_j \sim \text{Lap}\left(\frac{\Delta_1}{\varepsilon}\right)$$

$$= \text{Lap}\left(\frac{k}{\varepsilon}\right)$$

$$\text{error} \approx \frac{k}{\varepsilon} \text{ per coordinate}$$

Gaussian

$$Z_j \sim N\left(0, \frac{\Delta_2^2 2 \log(2/\delta)}{\varepsilon^2}\right)$$

$$\approx N\left(0, \frac{k \log(1/\delta)}{\varepsilon^2}\right)$$

$$\text{error} \approx \frac{\sqrt{k \log(1/\delta)}}{\varepsilon} \text{ per coordinate}$$