Theory of Differential Privacy

Lecture 16: Local Sensitivity and PTR

EN.601.438/638 Fall 2026

Lydia Zakynthinou
Johns Hopkins University

Oct 26, 2026

Beyond Global Sensitivity

For $f: \mathcal{X}^n \to \mathbb{R}$, for $x \sim x'$ s.t. $d_H(x, x') = 1$:

$$\Delta f = \sup_{x \sim x'} |f(x) - f(x')| \quad \text{and} \quad M(x) = f(x) + \text{Lap}\left(\frac{\Delta f}{\varepsilon}\right) \text{ is } \varepsilon\text{-DP.}$$

E.g. 1: $f(x) = \text{med}(x)$ for $\forall x_i \in [0, R]$

$\Delta \text{med} = R$ (as large as domain)

$(0,0,0,0,R,R,R)$ $x^{(1)}$

$(0,0,0,R,R,R,R)$

E.g. 2: $f(x) = \bar{x}$

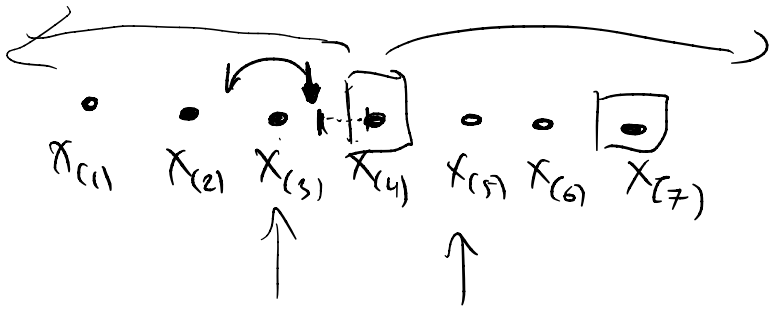
$\Delta \bar{x} = \infty$

Local Sensitivity

Def. $LS_f(x) = \sup_{x' : d_H(x,x')=1} |f(x) - f(x')|$ $\qquad \Delta f = \sup_x LS_f(x) \geq LS_f(x)$

Example: $n = 2m+1$, $x_{(1)} \leq x_{(2)} \leq x_{(3)} \leq \dots \leq x_{(n)}$

$med = x_{(m+1)}$ $\qquad LS_{med}(x) = \max\{ x_{(m+1)} - x_{(m)}, x_{(m+2)} - x_{(m+1)} \}$.



$LS_{med}(x^{(1)}) = R$

$LS_{med}(x^{(2)}) = 0$ $\qquad x^{(2)} = (0,0,0,0,0,R,R)$

for $k \leq m$, $\qquad LS^k_{med}(x) = \max\{ x_{(m+1+k)} - x_{(m+1)}, x_{(m+1)} - x_{(m+1-k)} \}$.

$$M_{naive}(x) = f(x) + Lap\left(\frac{LS(x)}{\varepsilon}\right)$$

$f = med$

$x = (0,0,0,0,0,R,R)$, $x' = (0,0,0,0,R,R,R)$

$LS_{med}(x) = 0$ $\qquad$ $LS_{med}(x') = R$

$med(x) = 0$ $\qquad$ $med(x') = 0$

for x: $M_{naive}(x) = 0$ w.p. 1. $\Rightarrow Pr[M_{naive}(x) = 0] = 1$

for x': $M_{naive}(x') = Lap\left(\frac{R}{\varepsilon}\right) \Rightarrow Pr[M_{naive}(x') = 0] = 0$

Cannot guarantee $1 \leq e^{\varepsilon} \cdot 0 + \delta$ for $\delta < 1$.

For $E = \{0\}$.

Down Sensitivity

Def. $DS_f(x) = \max_{i \in [n]} |f(x) - f(x^{-i})|$ $\quad f : \mathcal{X}^* \to \mathbb{R}$.

$$DS_f(x) \le LS_f^{\pm}(x)$$

Example: $\bar{x} = \frac{1}{n}\sum_{j=1}^{n} x_j$, $\bar{x}^{-i} = \frac{1}{n-1}\sum_{j \neq i} x_j = \frac{n\bar{x} - x_i}{n-1}$

$$DS_{\text{mean}}(x) = \max_i |\bar{x} - \bar{x}^{-i}| = \max_{i \in [n]} \left| \frac{x_i - \bar{x}}{n-1} \right|.$$

Assume $x \sim N(\mu, \sigma^2)^{\otimes n} \Rightarrow$ w.p. $DS_{\text{mean}}(x) \le O\left(\frac{\sigma\sqrt{\log n}}{n}\right)$.

Nevertheless, $LS^{\pm}_{\text{mean}}(x) = \max_{x' = \{y\} \cup x \text{ or } x' = x \setminus \{x_i\}} |\bar{x} - \bar{x}'| = \infty$

Smooth Sensitivity [NRS11]

Def. $$S^{\beta}_f(x) = \sup_{z \in X^n} e^{-\beta \cdot d_H(x,z)} LS_f(z)$$

Properties:

$$S^{\beta}_f(x) \geq LS_f(x)$$

$$S^{\beta}_f(x) \leq e^{\beta} S^{\beta}_f(x') \quad \text{for all } x \sim x'$$

$\hookrightarrow$

$$d_H(x,z) \geq d_H(x',z) - 1$$

$$\underbrace{e^{-\beta d_H(x,z)} \cdot LS_f(z)}_{S^{\beta}_f(x)} \leq \underbrace{e^{-\beta \cdot d_H(x',z)} \cdot e^{+\beta} \cdot LS_f(z)}_{S^{\beta}_f(x)}$$

Let $n = 2m+1$, $x = (0, \ldots, 0)$. If $d_H(x,z) < m$, $LS_{med}(z) = 0$.

$$S^{\beta}_{med}(x) = R \cdot e^{-\beta m} \quad \text{whereas} \quad \Delta med = R$$

Propose-Test-Release (PTR)

- Fix public $B > 0$ on LS_f.

  Define $U_B = \{ z \in \mathcal{X}^n : LS_f(z) > B \}$ "unsafe datasets".

- Measure distance to unsafety:

$$k_B(x) = \min_{z \in U_B} d_H(x, z).$$

$k_B(x) = 0$ iff $x \in U_B$ iff $LS_f(x) > B$.

- For any $x \sim x'$: $|k_B(x) - k_B(x')| \leq 1$.

- Test privately: $\hat{k}_B(x) = k_B(x) + Lap\left(\frac{1}{\varepsilon}\right)$ ← is ε-DP.

PTR $(f, B, \varepsilon, \delta)$:

$$k_B(x) = \min_{z \in V_B} d_H(x, z).$$

$$\hat{k}_B(x) = k_B(x) + W, \quad W \sim \mathrm{Lap}\left(\frac{1}{\varepsilon}\right)$$

Test: if $\hat{k}_B(x) < \dfrac{\log(1/2\delta)}{\varepsilon}$, output $\perp$.

Otherwise:

Release: $f(x) + Z$, where $Z \sim \mathrm{Lap}\left(\dfrac{B}{\varepsilon}\right)$.

Theorem PTR is $(2\varepsilon, \delta)$-DP.

Proof sketch: fix $x \sim x'$.

Case 1: $LS_f(x) \le B$. Then:

$\forall x'$: $|f(x) - f(x')| < B$ and $|k_B(x) - k_B(x')| < 1$.

Consider the joint law of $W, Z \Rightarrow (2\varepsilon, 0)$-DP.

Case 2: $LS_f(x) > B$.

Then $k_B(x) = 0$. $\Pr[\hat{E}_B(x) > \frac{\log(1/2\delta)}{\varepsilon}] = \Pr[0 + \text{Lap}(\frac{1}{\varepsilon}) > \frac{\log(1/2\delta)}{\varepsilon}] = \frac{1}{2} e^{-\frac{\log(1/2\delta)}{\varepsilon} \cdot \varepsilon} = \delta$.

$\Rightarrow$ w.p. at most δ, test passes and $M(x) \neq \perp$.

Let E be a measurable output event. Let $E_R = E \cap \mathbb{R}$.

$$\Pr[M(x) \in E] = \mathbb{1}\{E = \{\perp\}\} \cdot \Pr[M(x) \in E] + \Pr[M(x) \in E_R]$$

$$= \mathbb{1}\{E = \{\perp\}\} \cdot \Pr[M(x) \in E] + \delta$$

$$\leq e^{\varepsilon} \cdot \mathbb{1}\{E = \{\perp\}\} \cdot \Pr[M(x') \in E] + \delta$$

$$\leq e^{\varepsilon} \cdot \Pr[M(x') \in E] + \delta.$$

$\Rightarrow (\varepsilon, \delta)$-DP.

Overall $(2\varepsilon, \delta)$-DP.

Accuracy: If $k_B(x) \geq \frac{\log(1/2\delta\gamma)}{\varepsilon}$ then w.p. $1-\gamma$ x passes the test, and PTR outputs $M(x) \in \mathbb{R}$ with $|M(x) - f(x)| \leq \frac{B}{\varepsilon} \log(1/\gamma)$ (with another $1-\gamma$ prob.).