Lecture 10

Beyond Global Sensitivity

Local Sensitivity

$\Delta_{GS} = \max_{X,X'} \|f(X) - f(X')\|$

$f : \mathcal{X}^n \to \mathbb{R}$

$\Delta^{(f)}_{LS}(X) = \max_{X'} |f(X) - f(X')|$

X' nbrs to X

Before: $f(X) + Lap\left(\frac{\Delta_{GS}}{\varepsilon}\right)$ ✓ $(\varepsilon, 0)$-DP

Now: $f(X) + Lap\left(\frac{\Delta_{LS}(X)}{\varepsilon}\right)$ ✗

$f(X)$: dist btw 2 closest points in X $\quad X \in \mathbb{R}^n$

$\Delta_{GS} = \infty \quad X = \{0, 0\}, \; X' = \{0, \infty\}$

$X = \{0, 0, 0\} \qquad X' = \{0, 0, \infty\}$

$\Delta_{LS}(X) = 0$

$f(X) + Lap(0) = f(X) \Rightarrow 0$ deterministically

$X' = \{0, 0, 10000\}$

$\Delta_{LS}(X') = 10000$

$f(X') = Lap(10000/\varepsilon) = Lap(10000/\varepsilon)$ $f(X')$

Propose-Test-Release Dwork-Lei '09

1. Propose: bound on LS
2. Test: Is it?
3. Release: If yes, $f(X) + \mathrm{Lap}\left(\frac{LS}{\varepsilon}\right)$

Compute LS_i: $n|X|$

1. Propose a bound β on LS at X
2. Compute $\gamma = \min_{\hat{X}} d(X, \hat{X})$, where $\Delta_{LS}(\hat{X}) \geq \beta$ $\leftarrow |X|^n \leftarrow$ slow

Hamming dist, # of pts to change

ε-DP

3. $\hat{\gamma} = \gamma + \mathrm{Lap}(1/\varepsilon)$
4. If $\hat{\gamma} \leq \ln(1/\delta)/\varepsilon$, return $\perp$
5. If $\gamma > \ln(1/\delta)$, return $f(X) + \mathrm{Lap}(\beta/\varepsilon)$.

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

Proof: $\perp$

$\Pr[M(X) = \perp] \in [e^{-\varepsilon}, e^{\varepsilon}] \cdot \Pr[M(X') = \perp]$

Case 1: $\Delta_{LS}(X) > \beta$

$\gamma = 0$. $\Pr[\hat{\gamma} > \ln(1/\delta)/\varepsilon] \leq \delta$

$\Leftrightarrow \Pr[M(X) \neq \perp] \leq \delta$

$T \subseteq \mathbb{R} \cup \{\perp\}$

$$\Pr[M(X) \in T] = \Pr[M(X) \in \underbrace{T \cap \{\perp\}}_{\{\perp\} \text{ or } \emptyset}] + \Pr[M(X) \in T \cap \mathbb{R}]$$

$$\leq e^{\varepsilon} \Pr[M(X') \in T \cap \{\perp\}] + \Pr[M(X) \neq \perp]$$

$$\leq e^{\varepsilon} \Pr[M(X') \in T] + \delta$$

(ε, δ)-DP

Case 2: $\hat{\Delta}_{LS}(X) \leq \beta$

1. Release γ : ε-DP
2. Release $f(X) + Lap(\beta/\varepsilon)$: ε-DP

$(2\varepsilon, 0)$-DP ☐

Application: Histograms (modal element)

Laplace Histogram: L_∞ err $\approx \log |X|$ error ε-DP

Relax to approx $\Rightarrow$ no dependence on $|X|$.

Problem: $X \in \mathcal{X}^n$. Compute most freq elt.

$X = \{v, v, \ldots, v\}$, How many pts of x to change before mode changes?

$\Rightarrow \approx \frac{1}{2}$(count of most freq elt - count of 2nd most)

(ε,δ)-DP

1. Propose $LS \leq 0$.
2. $\gamma =$
3. $\hat{\gamma} = \gamma + Lap(1/\varepsilon)$. 4. If $\hat{\gamma} \leq \log(1/\delta)/\varepsilon$, $\perp$. 5. If $\hat{\gamma} \geq \log(1/\delta)/\varepsilon$, output mode(x).

$\Pr[Lap(1/\varepsilon) > \ln(1/\delta)/\varepsilon] \leq \delta$. Want: $\gamma \geq 2\log(1/\delta)/\varepsilon$.

Need: diff #1 and #2 elt $\geq 4\ln(1/\delta)/\varepsilon$,

Theorem 3. *There exists an (ε, δ)-differentially private algorithm which identifies the most frequent element from an arbitrary dataset with probability at least $1 - \delta$, as long as the gap between the count of the most frequent and the second most frequent element is at least $4\ln(1/\delta)/\varepsilon$.*

Thm 3.5 Vadhan '17

Theorem 4. *There exists an (ε, δ)-differentially private algorithm which can, with high probability, output the count of every item in a dataset up to additive $O(\log(1/\delta)/\varepsilon)$.*

ε-DP $O(\log|X|/\varepsilon)$

Privately Bounding Local Sensitivity

Before: Guessed LS bound

Now: Est LS.

1. Compute $\hat{\gamma} = \Delta_{LS}^{(f)}(X) + \mathrm{Lap}\left(\dfrac{\Delta_{GS}^{\Delta_{LS}^{(f)}}}{\varepsilon}\right) + \ln(1/\delta)/\varepsilon$ $\quad n(|X|-1)$

2. Output $f(X) + \mathrm{Lap}(\hat{\gamma}/\varepsilon)$.

'07

Smooth Sensitivity Nissim Raskhodnikova Smith

$$\Delta_{SS}^{(f)}(X) = \max_{\tilde{X} \in \mathcal{X}^n} \left\{ \Delta_{LS}^{(f)}(\tilde{X}) \, e^{-\varepsilon d(X,\tilde{X})} \right\}$$

Hamming.

$\cancel{f(X) + \mathrm{Lap}\left(\frac{\Delta_{SS}(X)}{\varepsilon}\right)}$ (ε,δ)-DP

$f(X) + \mathrm{Cauchy}\left(\frac{\Delta_{SS}(X)}{\varepsilon}\right)$ ε-DP