Lecture 6

Recap

- Laplace Mechanism.
  - Privacy guarantee
  - Accuracy guarantee.

Reminder

HW1 due on Sunday.

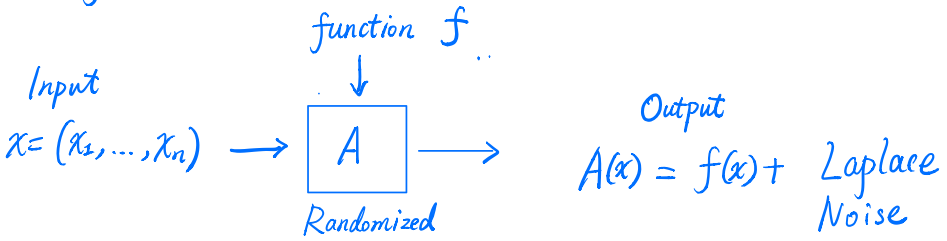
- Nice properties of DP
  - Composition
  - Post-Processing
  - Group Privacy

Definition. (Differential Privacy)

A is ε-differentially private if
for all neighbors x and x'
for all subsets E of outputs

$$\mathbb{P}[A(x) \in E] \leq e^{\varepsilon} \mathbb{P}[A(x') \in E]$$

Laplace Mechanism



- Goal: Release approximation to $f(x) \in \mathbb{R}^d$
- Global Sensitivity:

$$GS_f = \max_{x, x' \text{ neighbors}} \| f(x) - f(x') \|_1$$

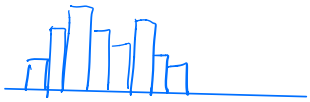
Examples.

- Proportion. $f(x) = \frac{1}{n} \sum_{i=1}^{n} x_i$

"fraction of people wearing socks"

$GS_f = \frac{1}{n}$.

- Histogram.



Data domain $\mathcal{X} = B_1 \cup B_2 \cup \dots \cup B_d$

$f(x) = (n_1, \dots, n_d)$, $n_j = \#\{i : x_i \in B_j\}$

$GS_f = 2$.

Fix any neighbors x, x'

$f(x) = (n_1, n_2, n_3 \dots, n_d)$

$f(x') = (n_1, n_2 - 1, n_3 + 1, \dots, n_d)$

$\|f(x) - f(x')\|_1 = |f(x)_1 - f(x')_1| + \dots + |f(x)_d - f(x')_d|$

(n_1)

$= |f(x)_2 - f(x')_2| + |f(x)_3 - f(x')_3|$

$= 2$.

Remark: sensitivity of histogram does not depend on $d :=$ # bins.

Examples

- Sequence of d statistical queries (averages)

properties $\phi_1, \dots, \phi_d$ with each $\phi_j : \mathcal{X} \mapsto [0,1]$

For each j, $f_j(x) = \frac{1}{n} \sum_{i=1}^{n} \phi_j(x_i)$

$f(x) = \left(f_1(x), f_2(x), \dots, f_d(x) \right)$.

Q: GS_f ?

answer: $\frac{d}{n}$? ✓ d ?

$GS_{f_j} = \frac{1}{n}$; $f_j(x) - f_j(x') \in [\frac{-1}{n}, \frac{1}{n}]$

$$\| f(x) - f(x') \|_1 = \sum_{j=1}^{d} |f_j(x) - f_j(x')| \le \frac{d}{n}$$

Examples

- Sequence of d statistical queries

  averages

  properties $\phi_1, \dots, \phi_d$ with each $\phi_j : X \mapsto [0,1]$

  For each j, $f_j(x) = \frac{1}{n} \sum_{i=1}^{n} \phi_j(x_i)$

  $GS_{f_j} \le \frac{1}{n}$

  $f(x) = (f_1(x), \dots, f_d(x))$, $f(x) - f(x') \in [-\frac{1}{n}, \frac{1}{n}]^d$

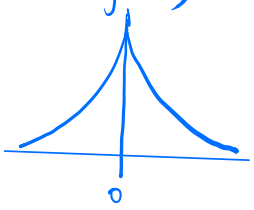
  $GS_f \le \frac{d}{n}$ err scales with d.

Laplace Mechanism.

$$A_L(x) = f(x) + (Z_1, \dots, Z_d)$$

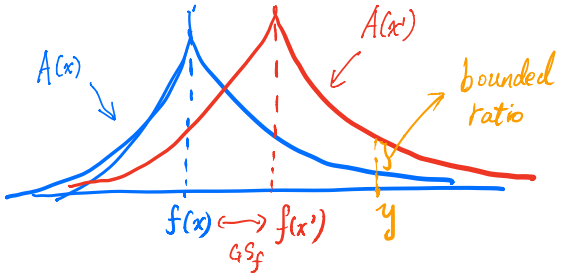
where each Z_i drawn i.i.d. from $Lap\left(\frac{GS_f}{\varepsilon}\right)$

Laplace Distribution: $Lap(b)$



$$PDF(x) = \frac{1}{2b} \exp\left(\frac{-|x|}{b}\right)$$

Theorem. A_L is ε-differentially private.



DP: $\forall y \in \mathbb{R}$ (real-value)

$$\mathbb{P}[A_L(x) = y] \le e^{\varepsilon}\, \mathbb{P}[A_L(x') = y]$$

Basic Proof Strategy:

for all neighbors x and x'
for all subsets E of outputs $(E \subseteq Y)$.

$$\mathbb{P}[A(x) \in E] \leq e^{\varepsilon}\, \mathbb{P}[A(x') \in E]$$

$$\Updownarrow$$

$$\mathbb{P}[A(x) = y] \leq e^{\varepsilon}\, \mathbb{P}[A(x') = y] \quad (*)$$

for all y in Y

Privacy Guarantee.

Theorem. A_L is ε-differentially private. $\boxed{\Delta = GS_f}$

Proof. Fix neighbors x and x', and output $y \in \mathbb{R}^d$

$h(x)$: $\mathbb{P}[A(x) = y] = \mathbb{P}[f(x) + \vec{Z} = y] = \left(\frac{\varepsilon}{2\Delta} e^{-|y_1 - f_1(x)| \cdot \frac{\varepsilon}{\Delta}}\right) \cdots \left(\frac{\varepsilon}{2\Delta} e^{-|y_d - f_d(x)| \frac{\varepsilon}{\Delta}}\right)$

want closeness; independent Laplace noise

$h(x')$: $\mathbb{P}[A(x') = y] = \mathbb{P}[f(x') + \vec{Z} = y] = \left(\frac{\varepsilon}{2\Delta} e^{-|y_1 - f_1(x')| \cdot \frac{\varepsilon}{\Delta}}\right) \cdots \left(\frac{\varepsilon}{2\Delta} e^{-|y_d - f_d(x')| \frac{\varepsilon}{\Delta}}\right)$

$\_\_\_ : \mathbb{P}[f_1(x) + z_1 = y_1] = \mathbb{P}[z_1 = y_1 - f_1(x)]$

$z_1 \sim Lap\left(\frac{\Delta}{\varepsilon}\right)$

$$\frac{h(x)}{h(x')} = \frac{\left(\frac{\varepsilon}{2\Delta}\right)^d \exp\left(\frac{-\varepsilon}{\Delta} \sum_{j=1}^{d} |y_j - f_j(x)|\right)}{\left(\frac{\varepsilon}{2\Delta}\right)^d \exp\left(\frac{-\varepsilon}{\Delta} \sum_{j=1}^{d} |y_j - f_j(x')|\right)}$$

$\sum |y_j - f_j(x)|$ ⟶ ℓ_1 norm

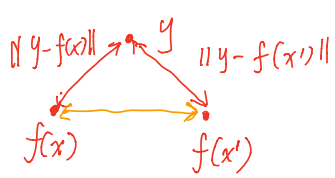
$$= \exp\left(\frac{\varepsilon}{\Delta}\left(\|y - f(x')\|_1 - \|y - f(x)\|_1\right)\right) \leftarrow$$

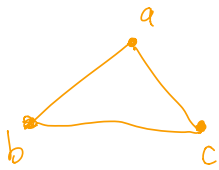
$\leq \Delta$?

$$\leq \exp\left(\frac{\varepsilon}{\Delta}\left(\|f(x) - f(x')\|_1\right)\right) \leq \exp(\varepsilon)$$

$\leq \Delta$?

Triangle inequality:

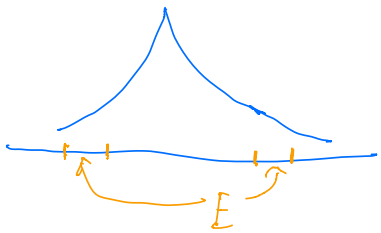




$\|b - c\| \leq \|a - b\| + \|a - c\|$

Extend from $\forall y$ to $\forall E$.

Let $E \subseteq \mathbb{R}^d$



$$\mathbb{P}[A(x) \in E] = \int_{y \in E} \mathbb{P}[A(x) = y]\, dy$$

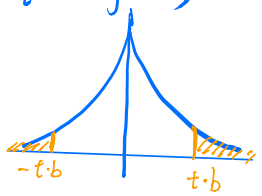
$$\leq \int_{y \in E} e^{\varepsilon}\, \mathbb{P}[A(x') = y]\, dy$$

$$= e^{\varepsilon} \int_{y \in E} \mathbb{P}[A(x') = y]\, dy$$

$$= e^{\varepsilon} \cdot \mathbb{P}[A(x') \in E].$$

Accuracy of Laplace Mechanism $\|f(x) - A_L(x)\|_1$

Laplace Distribution: $Z_i \sim Lap(b)$



$$PDF(x) = \frac{1}{2b} \exp\left(\frac{-|x|}{b}\right)$$

- $\mathbb{E}[|Z_i|] = b$
- for every $t > 0$: $\underbrace{\mathbb{P}[|Z_i| > t\,b]}_{\text{Tail bound.}} \leq \underbrace{e^{-t}}_{\text{exponentially decreasing.}}$

HW1, Last Question.

$\vec{Z} = (Z_1, \ldots, Z_d)$, $Z_i \sim Lap(b)$.

$\|Z\|_\infty = \max\{|Z_1|, \ldots, |Z_d|\}$.

Exercise: $\mathbb{P}[\|Z\|_\infty > \underbrace{b \cdot \ln(d) + b \cdot t}_{M}] \leq e^{-t}$.

For simplicity $d = 2$.

$$\mathbb{P}[\|Z\|_\infty > M] = \mathbb{P}[|Z_1| > M \text{ or } |Z_2| > M]$$
$$= \mathbb{P}[\{|Z_1| > M\} \cup \{|Z_2| > M\}]$$
$$\leq \mathbb{P}[|Z_1| > M] + \mathbb{P}[|Z_2| > M].$$

Union Bound

$A: |Z_1| > M$

$B: |Z_2| > M$

$\mathbb{P}[A \cup B] \leq \mathbb{P}[A] + \mathbb{P}[B]$