Lecture 5

- Recap
  - Differential Privacy (DP) definition.
  - Laplace Mechanism
    - → Privacy & Accuracy.

  | Randomized Response (Warner 65)

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

Definition. (Differential Privacy) ← about the algorithm

A is ε-differentially private if

for all neighbors x and x'

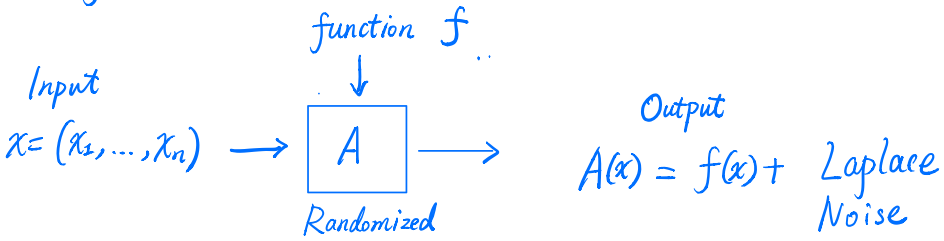
for all subsets E of outputs

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

ε: Privacy loss parameter

Small constant: $\frac{1}{10}$, 1, but not $\frac{1}{2^{80}}$ or 100

Laplace Mechanism



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

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

Example: $f(x) \equiv$ fraction of people wearing socks

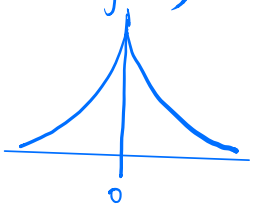
$$GS_f = \frac{1}{n}$$

Laplace Mechanism.

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

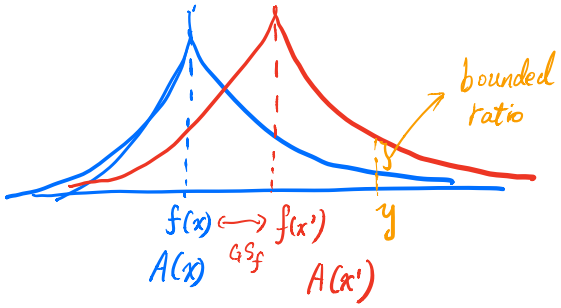
where each Z_i drawn i.i.d. from $Lap\left(\frac{GS_f}{\varepsilon}\right)$

Laplace Distribution: $Lap(b)$



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

Theorem. A_L is ε-differentially private.



Privacy Guarantee.

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

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

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

$h(x)$

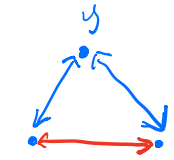
$$\mathbb{P}[A(x') = y] = \left(\frac{\varepsilon}{2\Delta} e^{-|y_1 - f(x')| \cdot \frac{\varepsilon}{\Delta}}\right) \cdots \left(\frac{\varepsilon}{2\Delta} e^{-|y_d - f_d(x')| \cdot \frac{\varepsilon}{\Delta}}\right)$$

$h(x')$

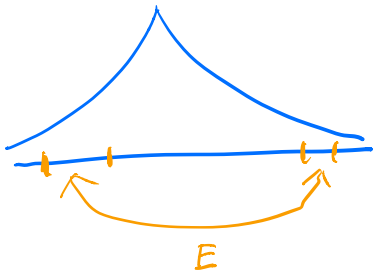
$$\frac{h(x)}{h(x')} = \exp\left(\frac{\varepsilon}{\Delta}\left(\|y - f(x')\|_1 - \|y - f(x)\|_1\right)\right)$$

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

$$\leq \exp(\varepsilon)$$



Triangle Inequality



Let $E \subseteq \mathbb{R}^d$ (measurable)

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

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

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

Randomized $f : \mathcal{X}^n \times \underbrace{R}_{\text{random seed}} \to \mathbb{R}^d$

Examples.

- Proportion. $f(x) = \frac{1}{n}\sum_{i=1}^{n} x_i \longrightarrow$ in $[0,1]$

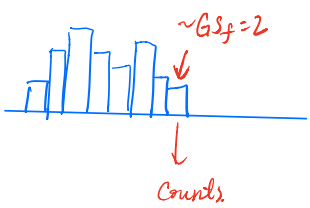
"fraction of people wearing socks"

$GS_f = \boxed{\frac{1}{n}}$ $\ll$ 1, 0.1, 0.2 ... (potential answers)

$n = 100$

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

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



$GS_f = 2.$

Examples

- Sequence of d statistical queries (averages)

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

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

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

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

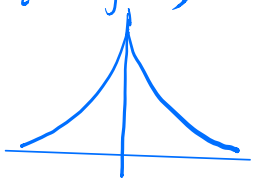
$GS_f \le \frac{d}{n}$ err scales with d.

Accuracy of Laplace Mechanism

$\|f(x) - A_L(x)\|_1 = \|Z\|_1$

$b = \frac{GS_f}{\varepsilon}$ ←

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



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

- $\mathbb{E}[|Z|] = b$
- for every $t > 0$: $\mathbb{P}[|Z| > t\,b] \leq e^{-t}$ (tail bound)

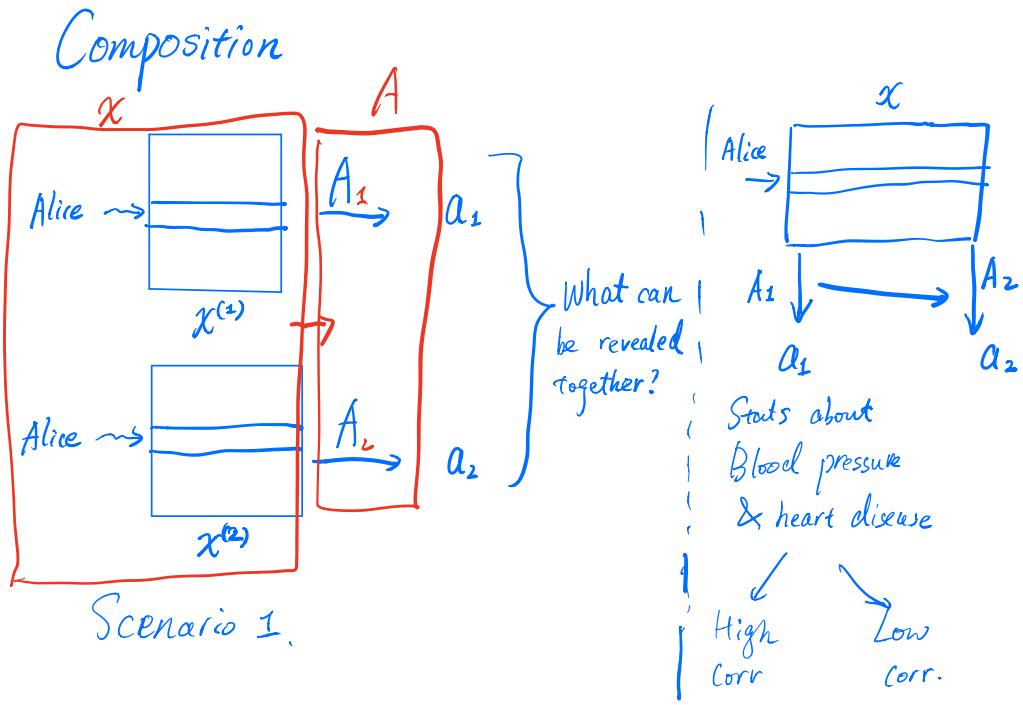
Let $Z_1, \ldots, Z_d \overset{i.i.d.}{\sim} Lap(b)$

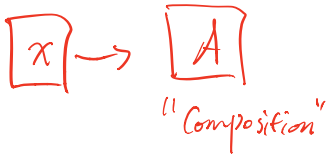
$\mathbb{E}[\|Z\|_1] = \mathbb{E}[\sum_{j \in [d]} |Z_j|] = \sum_i \mathbb{E}[|Z_j|] = d \cdot b.$

$M = \max\{|Z_1|, \ldots, |Z_d|\}$ → "worst coordinate error"

- $\mathbb{E}[M] \leq b(\ln(d) + 1)$
- $\forall t > 0$, $\mathbb{P}[M > \underbrace{b\ln(d)}_{\text{Expectation}} + \underbrace{b \cdot t}_{\text{deviation}}] \leq e^{-t}$

"Union bound"


Composition
x
A
Alice
A_1
a_1
$x^{(1)}$
Alice
A_2
a_2
$x^{(2)}$
What can be revealed together?
Scenario 1.
x
Alice
A_1
A_2
a_1
a_2
Stats about Blood pressure & heart disease
High Corr
Low corr.
Scenario 2


x
A
"Composition"

Composition

Suppose $A_1 : \mathcal{X}^n \to \mathcal{Y}_1$ is ε_1-DP.

$A_2 : (\mathcal{Y}_1 \times \mathcal{X}^n) \to \mathcal{Y}_2$ satisfies ε_2-DP $(\forall y_1 \in \mathcal{Y}_1)$.

Then. $A(x)$:
$a_1 \leftarrow A_1(x)$
$a_2 \leftarrow A_2(a_1, x)$
return (a_1, a_2)
is $(\varepsilon_1 + \varepsilon_2)$-DP.

("a" $\leftrightarrow$ "y")

Proof. Fix any neighbors x & x'. $\forall E \subseteq \mathcal{Y}_1 \times \mathcal{Y}_2$

Suffices to look at any $(y_1, y_2) \in E$

$$\begin{aligned}
\mathbb{P}[A(x) = (y_1, y_2)] &= \mathbb{P}[A_1(x) = y_1] \cdot \mathbb{P}[A_2(y_1, x) = y_2] \\
&\le e^{\varepsilon_1} \mathbb{P}[A_1(x') = y_1] \cdot e^{\varepsilon_2} \mathbb{P}[A_2(y_1, x') = y_2] \\
&= e^{\varepsilon_1 + \varepsilon_2} \mathbb{P}[A(x') = (y_1, y_2)]
\end{aligned}$$

ε: "Privacy Budget"

Composition of k algorithms $A_1, \ldots, A_k$

The choice of A_i depends on $A_1, \ldots A_{i-1}$'s outputs

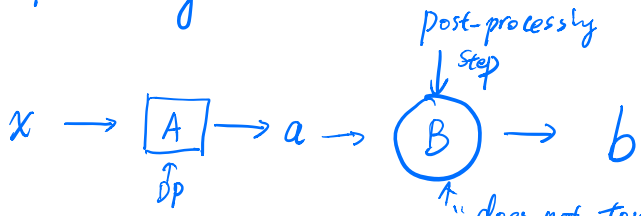
The "adaptive" composition of $A_1, \ldots, A_k$

is $\left(\sum_{i=1}^{k} \varepsilon_i\right)$

with ε_i being the privacy loss of each A_i

→ Proof by induction

Post-Processing Lemma



Lemma. If A is ε-DP, then so is $B(A(\cdot))$ for any B.

① Algorithmic tools

"sufficient stats" ⟶ more complex computations

② Protect. Against any adversary.

Group Privacy

"What is revealed about k people?"

Lemma. Let $A : \mathcal{X}^n \to \mathcal{Y}$ be ε-DP

If x and x' differ by k records,

then for any $E \subseteq \mathcal{Y}$

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