Introduction to Differential Privacy
Lecture 2 : Exploiting the sensitivity for privacy

Clément Lalanne

16/12/2020

Introduction

Differential privacy: Protect the inputs of a database.

Last talk: Definitions, examples and basic properties.

First idea: Release a **noisy** output.

Today's presentation

Plan of the talk:

- Differential privacy.
- The notion of sensitivity.
- Laplace mechanism.
- Exponential mechanism.
- Gaussian mechanism.
- Smoothed sensitivity.
- Local sensitivity and PTR algorithm.

(ϵ, δ)-differential privacy

Definition (Approximate Differential Privacy [DR+14])

A randomized function $\mathcal{K}$ gives (ϵ, δ)-approximate differential privacy if for all data sets D_1 and D_2 differing on at most one element, and all $S \subseteq \text{Range}(\mathcal{K})$

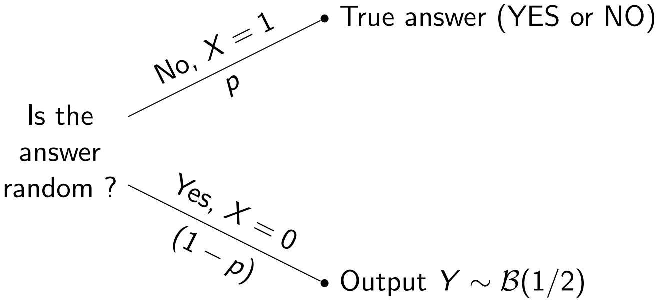
$$\mathbb{P}(\mathcal{K}(D_1) \in S) \leq e^{\epsilon} \times \mathbb{P}(\mathcal{K}(D_2) \in S) + \delta$$

The probability is taken over the coin tosses of $\mathcal{K}$.

Remarks:

- Few variations on close databases.
- The smaller ϵ and δ, the more privacy.
- Rough interpretation of δ: The probability of failure.
- The case $\delta = 0$ corresponds to pure DP.
- In parctice: $\delta < 1/n$

First example



$$A(D) = XD + (1 - X)Y$$

What about differential privacy?

$$\frac{\mathbb{P}(A(D)=1|D=1)}{\mathbb{P}(A(D)=1|D=0)} = \frac{p+(1-p)/2}{(1-p)/2} = 1+2\frac{p}{1-p}$$

$$\frac{\mathbb{P}(A(D)=0|D=0)}{\mathbb{P}(A(D)=0|D=1)} = \frac{p+(1-p)/2}{(1-p)/2} = 1+2\frac{p}{1-p}$$

A is $\log\left(1+2\frac{p}{1-p}\right)$-DP.

The notion of sensitivity

$f : \mathcal{D} \to \mathbb{R}$, D_1 and D_2 two databases.

$$\log\left(\frac{p((f+\mu)(D_1)=x)}{p((f+\mu)(D_2)=x)}\right) = \log\left(\frac{p(\mu = x - f(D_1))}{p(\mu = x - f(D_2))}\right)$$
$$\leq |\lambda||f(D_2) - f(D_1)|, p(x) \propto e^{\lambda|x|}$$

Definition (l_1-sensitivity [DMNS06])

For $f : \mathcal{D} \to \mathbb{R}^k$, the sensivity of f is

$$\Delta f = \sup_{D_1, D_2} ||f(D_1) - f(D_2)||_1$$

for all D_1, D_2 differing on at most one element.

Laplace mechanism

Definition (Laplace mechanism [DMNS06])

Let us consider the Laplace distribution defined for a real number $\alpha > 0$ and with respect to Lebesgue measure as $\mathrm{Lap}(\alpha)(x) \propto \exp(-|x|/\alpha)$. Let $f : \mathcal{D} \to \mathbb{R}^k$, we call the Laplace mechanism of f with privacy parametter α the mechanism defined as

$$\mathcal{L}_f^{(\alpha)}(D) = f(D) + (Lap(\alpha))^k$$

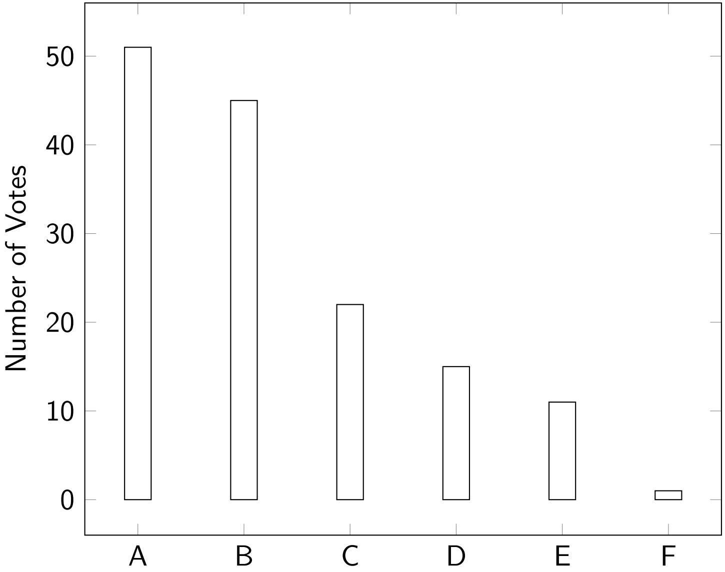
where $(Lap(\alpha))^k$ refers to a vector of size k of i.i.d. samples of distribution $\mathrm{Lap}(\alpha)$.

Laplace mechanism

Theorem (Differential Privacy of Laplace Mechanism [DMNS06])

For any $f : \mathcal{D} \to \mathbb{R}^k$ with finite sensitivity, if $\alpha \geq \Delta f / \epsilon$, then the mechanism $\mathcal{L}_f^{(\alpha)}$ is ϵ-DP. Furthermore the mechanism is tight in the sense that for all $\epsilon' < \epsilon$, $\mathcal{L}_f^{(\Delta f / \epsilon)}$ is not ϵ'-DP.

Example: Histograms



Example: Histograms

Sensitivity: Adding or removing one vote modifies one of the columns by at most $1 \Rightarrow \Delta\text{Hist} = 1$.

Laplace mechanism: Adding independent noise to each column sampled from $\text{Lap}(1/\epsilon)$ gives ϵ-DP.

Interpretability: Round (post processing) or ...

In metric spaces

Definition (Sensitivity in metric spaces [DMNS06])

Let $\mathcal{M}$ be a metric space with distance function $d_{\mathcal{M}}(.,.)$. The sensitivity of $f : \mathcal{D} \to \mathcal{M}$ is defined as

$$\Delta_{\mathcal{M}} f = \sup_{D_1, D_2} d_{\mathcal{M}}(f(D_1), f(D_2))$$

for all D_1, D_2 differing on at most one element.

In metric spaces

Definition (Exponential mechanism [DMNS06])

Let $\mathcal{M}$ be a metric space with distance function $d_{\mathcal{M}}(.,.)$. Let $f : \mathcal{D} \to \mathcal{M}$. We call exponential mechanism of f with privacy parametter α the sampling mechanism $\mathcal{E}^{(\alpha)}_{\mathcal{M},f} : \mathcal{D} \to \mathcal{M}$ such that

$$\forall y \in \mathcal{M}, \mathbb{P}\left(\mathcal{E}^{(\alpha)}_{\mathcal{M},f}(D) = y\right) \propto e^{-d(y,f(D))/\alpha}$$

Theorem (Privacy of the exponential mechanism [DMNS06])

If $\alpha \geq \frac{2\Delta_{\mathcal{M}} f}{\epsilon f}$ then $\mathcal{E}^{(\alpha)}_{\mathcal{M},f}$ is ϵ-DP. Furthermore, if the quantity $\sum_{y \in \mathcal{M}} e^{-d(y,f(D))/\alpha}$ is independent of D then $\alpha \geq \frac{\Delta_{\mathcal{M}} f}{\epsilon}$ ensures that $\mathcal{E}^{(\alpha)}_{\mathcal{M},f}$ is ϵ-DP and this result is tight.

In metric spaces

Proof.

Let D_1 and D_2 be two databases that differ on only one input.

$$\forall y \in \mathcal{M}, \frac{e^{-d(y,f(D_1))/\alpha}}{e^{-d(y,f(D_2))/\alpha}} \leq e^{d(f(D_1),f(D_2))/\alpha}$$

Let $y \in \mathcal{M}$,

$$\frac{\mathbb{P}\left(\mathcal{E}^{(\alpha)}_{\mathcal{M},f}(D_1) = y\right)}{\mathbb{P}\left(\mathcal{E}^{(\alpha)}_{\mathcal{M},f}(D_2) = y\right)} = \frac{e^{-d(y,f(D_1))/\alpha}}{e^{-d(y,f(D_2))/\alpha}} \frac{\sum_{y' \in \mathcal{M}} e^{-d(y',f(D_1))/\alpha}}{\sum_{y' \in \mathcal{M}} e^{-d(y',f(D_2))/\alpha}}$$

$$\leq e^{d(f(D_1),f(D_2))/\alpha} e^{d(f(D_1),f(D_2))/\alpha} \frac{\sum_{y' \in \mathcal{M}} e^{-d(y',f(D_2))/\alpha}}{\sum_{y' \in \mathcal{M}} e^{-d(y',f(D_2))/\alpha}}$$

$$\leq e^{2\Delta_{\mathcal{M}} f/\alpha}$$

What about other noise structures?

Definition (Gaussian Mechanism [DMNS06, DR+14])

Let $f : \mathcal{D} \to \mathbb{R}^k$. We call the Gaussian mechanism of f with standard derivation $\sigma > 0$ the mechanism defined as

$$\mathcal{G}_f^{(\sigma)}(D) = f(D) + (\mathcal{N}(0, \sigma^2))^k$$

where $(\mathcal{N}(0, \sigma^2))^k$ refers to a vector of size k of i.i.d. samples of law $\mathcal{N}(0, \sigma^2)$.

Pure DP with gaussian noise?

Let $f : \mathcal{D} \to \mathbb{R}^k$ be non-constant and $\sigma > 0$. Let $x \in \mathbb{R}^k$.

$$\log\left(\frac{p(\mathcal{G}_f^{(\sigma)}(D_1) = x)}{p(\mathcal{G}_f^{(\sigma)}(D_2) = x)}\right) = \log\left(\frac{e^{-||x-f(D_1)||_2^2/(2\sigma^2)}}{e^{-||x-f(D_2)||_2^2/(2\sigma^2)}}\right)$$

$$= \frac{1}{2\sigma^2}\left(||x - f(D_1)||_2^2 - ||x - f(D_2)||_2^2\right)$$

$$= \frac{1}{2\sigma^2}\langle f(D_2) - f(D_1), 2x - f(D_1) - f(D_2)\rangle$$

Pure DP with gaussian noise?

So, by taking $x_n = \frac{1}{2}\left(n(f(D_2) - f(D_1)) + f(D_1) + f(D_1)\right)$,

$$\log\left(\frac{p(\mathcal{G}_f^{(\sigma)}(D_1) = x_n)}{p(\mathcal{G}_f^{(\sigma)}(D_2) = x_n)}\right) \rightarrow_{n\rightarrow\infty} +\infty,$$

which proves that no pure differential privacy is possible.

DP via relaxation

Definition (l_2-sensitivity [DR+14])

For $f : \mathcal{D} \to \mathbb{R}^k$, the l_2-sensivity of f is

$$\Delta_2 f = \max_{D_1, D_2} ||f(D_1) - f(D_2)||_2$$

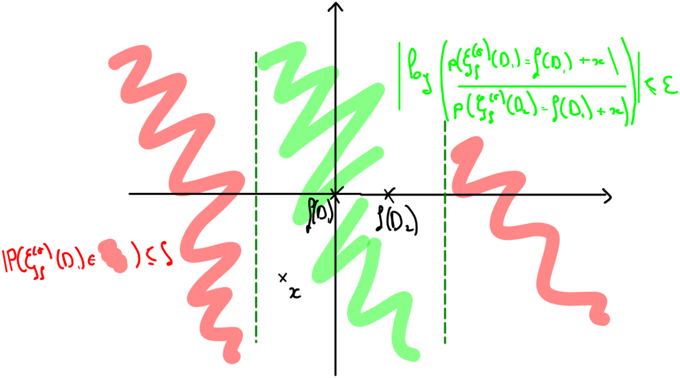
for all D_1, D_2 differing on at most one element.

Theorem (Approximate Differential Privacy of Gaussian Mechanism [DR+14])

Let $f : \mathcal{D} \to \mathbb{R}^k$ be with finite l_2-sensitivity and $\epsilon \in (0, 1)$. For $c^2 > \max(9/4, 2\log(1.25/\delta))$, the gaussian mechanism of f with standard derivation $\sigma \geq c\Delta_2 f/\epsilon$ is (ϵ, δ)-differentially private.

DP via relaxation

Proof.



$\square$

Is global sensitivity good enough?

Setup: Estimation of the median of $X \in [a, b]$ from n i.i.d. samples.

Algorithm: Empirical median + noise.

Sensitivity: $\Delta f = \Delta_2 f = b - a$

Problem: The noise kills the information.

Using local sensitivity?

Definition (Local sensitivity [NRS07])

For $f : \mathcal{D} \to \mathbb{R}^k$, the l_q-sensivity of f is a function defined of $\mathcal{D}$ by

$$\forall D_1 \in \mathcal{D}, (L\Delta)_q f(D_1) = \sup_{D_2 : d(D_1, D_2) \leq 1} ||f(D_1) - f(D_2)||_q$$

Remark: For $f : \mathcal{D} \to \mathbb{R}^k$,

$$\Delta_q f = \sup_{D_1 \in \mathcal{D}} (L\Delta)_q f(D_1).$$

Problem: We have no control over the variations of $(L\Delta)_q f(D)$.

Solution 1: Smoothing

Definition (Smoothed sensitivity [NRS07])

For $f : \mathcal{D} \to \mathbb{R}$ and $\beta > 0$, the β-smooth sensitivity of f is the function defines as

$$\forall D_1 \in \mathcal{D}, \Delta^{(\beta)} f(D_1) = \sup_{D_2 \in \mathcal{D}} \left(e^{-\beta d(D_1, D_2)} (L\Delta) f(D_2) \right)$$

Proposition (Variations of sensitivity [NRS07])

Let $f : \mathcal{D} \to \mathbb{R}$, $0 < \beta_1 \leq \beta_2$ *and* $D \in \mathcal{D}$,

$$0 \leq (L\Delta) f(D) \leq \Delta^{(\beta_2)} f(D) \leq \Delta^{(\beta_1)} f(D) \leq \Delta f \leq \infty$$

Solution 1: Smoothing

Theorem (Privacy with smoothed sensitivity [NRS07])

$f : \mathcal{D} \to \mathbb{R}$ such that $\forall D \in \mathcal{D}, (L\Delta)f(D) < \infty$.

- *Let $\epsilon, \delta > 0$, if $\beta \leq \frac{\epsilon}{2(\gamma+1)}$ and $\gamma > 1$, the random function $D \mapsto f(D) + \frac{2(\gamma+1)}{\epsilon}\Delta^{(\beta)}f(D)Z$ where Z is sampled with density $\propto \frac{1}{1+|z|^\gamma}$ is ϵ-DP.*
- *Let $\epsilon > 0$, if $\beta \leq \frac{\epsilon}{2\log(2/\delta)}$, the random function $D \mapsto f(D) + \frac{2}{\epsilon}\Delta^{(\beta)}f(D)Z$ where Z is sampled from $Lap(1)$ is (ϵ, δ)-DP.*
- *Let $\epsilon > 0$, if $\beta \leq \frac{\epsilon}{4(1+\log(2/\delta))}$, the random function $D \mapsto f(D) + \frac{5\sqrt{2\log(2/\delta)}}{\epsilon}\Delta^{(\beta)}f(D)Z$ where Z is sampled from $Lap(1)$ is (ϵ, δ)-DP.*

Solution 2: PTR

Let $f : \mathcal{D} \to \mathbb{R}$,

Idea: Measure how far from a problematic local sensitivity the database is.

$$A_{\eta,f}(D_1) = \min \{k \in \mathbb{N} : \exists D_2 \in \mathcal{D}, d(D_1, D_2) \leq k, |f(D_1) - f(D_2)| > \eta\}$$

Propose Test Release: If the local sensitivity is not stable: halt the algorithm. Otherwise, add noise to the output.

Solution 2: PTR

Inputs: $f, D, \eta, a_\delta, b_\delta$
$Z_1, Z_2 \leftarrow$ Two independent samples of a random variable Z
$\tilde{A}_{\eta,f}(D) \leftarrow A_{\eta,f}(D) + \frac{a_\delta}{\epsilon} Z_1$
if $\tilde{A}_{\eta,f}(D) \leq 1 + \frac{b_\delta}{\epsilon}$ **then**
  return $\perp$ (halt)
else
  return $f(D) + \frac{\eta}{\epsilon} a_\delta Z_2$
end if

Figure: Propose Test Release [DL09, BAM20]

Solution 2: PTR

Theorem (Privacy of PTR [BAM20])

- *If* $Z_1, Z_2 \sim Lap(1)$, $a_\delta = 1$ *and* $b_\delta = \log(2/\delta)$, *PTR gives* $(2\epsilon, \delta)$*-DP.*
- *If* $Z_1, Z_2 \sim \mathcal{N}(0, 1)$, $a_\delta = \sqrt{2\log(1.25/\delta)}$ *and* $b_\delta = 2\log(1.25/\delta)$, *PTR gives* $(2\epsilon, 2e^\epsilon\delta + \delta^2)$*-DP.*

Applications:

- First private algorithm for the unbounded median with sub-Gaussian concentration with high probability.
- First private algorithm for the unbounded mean with sub-Gaussian concentration with high probability (Median of means).

Conclusion

We saw that it is possible to achieve privacy by:

- Adding noise from a Laplace or Gaussian distribution.
- Sampling from the output space with an exponential law.

We refined the results using:

- Smoothed sensitivity.
- the Propose Test Release algorithm.

For the next talks:

- Privacy in optimization problems.
- Advanced composition.

References I

- Victor-Emmanuel Brunel and Marco Avella-Medina, *Propose, test, release: Differentially private estimation with high probability*, arXiv preprint arXiv:2002.08774 (2020).
- Cynthia Dwork and Jing Lei, *Differential privacy and robust statistics*, Proceedings of the forty-first annual ACM symposium on Theory of computing, 2009, pp. 371–380.
- Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith, *Calibrating noise to sensitivity in private data analysis*, Theory of cryptography conference, Springer, 2006, pp. 265–284.
- Cynthia Dwork, Aaron Roth, et al., *The algorithmic foundations of differential privacy.*, Foundations and Trends in Theoretical Computer Science **9** (2014), no. 3-4, 211–407.

References II

Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith, *Smooth sensitivity and sampling in private data analysis*, Proceedings of the thirty-ninth annual ACM symposium on Theory of computing, 2007, pp. 75–84.