Statistics for Data Science, WS2023

Chapter 6:

Differential Privacy

Overview

Issues of data privacy protection

Definition of Differential Privacy

Designing ε-DP mechanisms

Approximate differential privacy

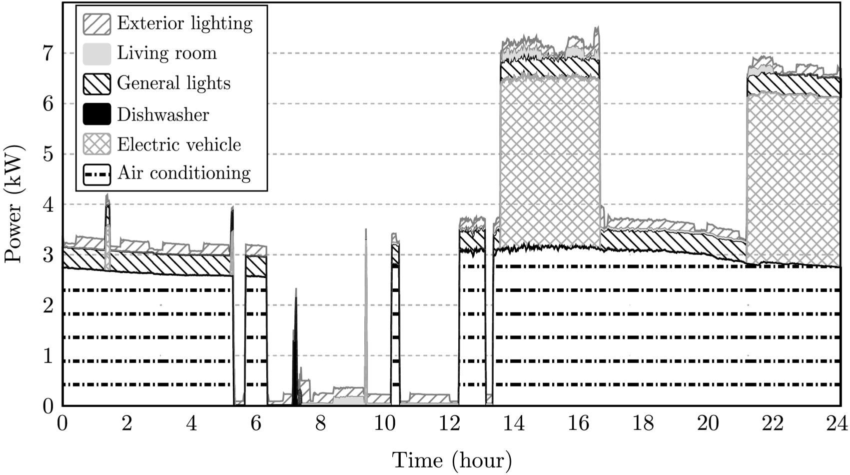
Issues of data privacy protection

Issues of data privacy protection

This is an old problem with increasing relevance in the modern era of big data. For instance:

- official statistics
- large scale medical research
- smart phone user data
- social media data
- IoT
- etc.

Example: Data from smart meter



Issues of data privacy protection

Traditional solutions:

- anonymize
- aggregate

ANONYMIZATION -> 'RE-IDENTIFICATION ATTACKS'

Example: Student survey

ID	age	sex	#sib.	firstSem.	best	worst	cheated	drugs
01622490	21	f	3	SS2017	1	5	no	no
10628491	23	m	1	WS2017	1	5	yes	yes
14937612	24	m	1	WS2017	1	4	no	no
11274513	23	f	1	SS2017	1	3	yes	yes
09663822	20	f	0	WS2017	1	2	no	yes
⋮								
07257738	21	m	0	WS2017	1	1	no	yes

$n = 24$

ANONYMIZATION -> 'RE-IDENTIFICATION ATTACKS'

Example: Student survey

ID	age	sex	#sib.	firstSem.	best	worst	cheated	drugs
______	21	f	3	SS2017	1	5	no	no
______	23	m	1	WS2017	1	5	yes	yes
______	24	m	1	WS2017	1	4	no	no
______	23	f	1	SS2017	1	3	yes	yes
______	20	f	0	WS2017	1	2	no	yes
⋮								
______	21	m	0	WS2017	1	1	no	yes

$n = 24$

ANONYMIZATION -> 'RE-IDENTIFICATION ATTACKS'

```
> # use only age
> agg <- aggregate(data$age, by=data["age"], length)
> agg
  age x
1  20 1
2  21 6
3  22 4
4  23 4
5  24 1
6  25 2
7  26 1
8  27 4
9  31 1
```

ANONYMIZATION -> 'RE-IDENTIFICATION ATTACKS'

```
> (agg <- aggregate(data$age, by=data[c("sex",
"age")], length))
   sex age x
1    f  20 1
2    f  21 5
3    m  21 1
4    f  22 2
5    m  22 2
6    m  23 4
7    f  24 1
8    f  25 1
9    m  25 1
10   m  26 1
11   f  27 2
12   m  27 2
13   f  31 1
> sum(agg$x==1)/n # fraction uniquely identified
[1] 0.2916667
```

ANONYMIZATION -> 'RE-IDENTIFICATION ATTACKS'

```
> # sex, age, first semester
> agg <- aggregate(data$age, by=data[c("sex", "age",
 "start")], length)
> sum(agg$x==1)/n # fraction uniquely identified
[1] 0.625


> # sex, age, first semster, worst grade
> agg <- aggregate(data$age, by=data[c("sex", "age",
"start", "worst")], length)
> sum(agg$x==1)/n # fraction uniquely identified
[1] 0.6666667


> # sex, age, first semester, worst grade, #siblings
> agg <- aggregate(data$age, by=data[c("sex", "age",
"start", "siblings", "worst")], length)
> sum(agg$x==1)/n # fraction uniquely identified
[1] 0.75
```

ANONYMIZATION -> 'RE-IDENTIFICATION ATTACKS'

- personal identifiers may look unsuspicious (e.g., age)
- **sets** of attributes/variables can be personal identifiers
- **auxiliary information** may be available
- the problem worsens for **high-dimensional data**

Real world examples:

Narayanan, A. and Shmatikov, V. (2006). How to break anonymity of the netflix prize dataset. arXiv preprint cs/0610105.

Sweeney L, Abu A, and Winn J. (2013). Identifying Participants in the Personal Genome Project by Name. Harvard University. Data Privacy Lab. White Paper 1021-1.

AGGREGATION -> DE-AGGREGATION

- Publish only summary statistics: $S_n = \sum_{i=1}^{n} X_i$.

Statistical agencies compute sensitivity/privacy measures:
e.g., p-percent rule: for $X_i \geq 0$, (e.g., revenue of companies)

$$\frac{X_{(n)}}{\sum_{i \neq n-1} X_{(i)}} > p.$$

Worst case: $S_n - \sum_{i=2}^{n} X_i = X_1$.

Whether S_n is publishable depends on the original data $X_1, \ldots, X_n$. What is the 'correct' sensitivity measure?

AGGREGATION -> DIFFERENCING

- Publish only answers to counting queries.

How many students are 21 and male? Answer: 1

How many students are 21, male and took drugs? Answer: 1

Definition of Differential Privacy

Definition of Differential Privacy

$$\begin{array}{ccccc} \text{individuals} & & \text{database} & & \text{public} \\ \text{Alice} & \xrightarrow{x_1} & & & \\ \text{Bob} & \xrightarrow{x_2} & x & \xrightarrow[q]{\text{randomization}} & Z_x \\ \vdots & & & & \\ \text{Zoey} & \xrightarrow{x_n} & & & \end{array}$$

For each possible database $x \in \mathcal{X}^n$ with n rows, we specify a randomization mechanism, that is, a random variable Z_x taking values in some output space $\mathcal{Z}$. Typically $\mathcal{Z} \subseteq \mathbb{R}^m$.

Z_x should not depend too much on any individual contribution x_i.

Definition of Differential Privacy

For $x, x' \in \mathcal{X}^n$, define the Hamming distance

$$d_0(x, x') := |\{i : x_i \neq x'_i\}|.$$

Definition (Dwork et al. 2006)

Fix a privacy parameter $\varepsilon \in (0, \infty)$. The randomization mechanism outputting Z_x on $\mathcal{Z}$ for a given $x \in \mathcal{X}^n$, is called ε-differentially private if for all $x, x' \in \mathcal{X}^n$ with $d_0(x, x') \leq 1$, we have

$$\mathbb{P}(Z_x \in A) \leq e^{\varepsilon} \cdot \mathbb{P}(Z_{x'} \in A), \quad \forall A \subseteq \mathcal{Z} \text{ (measurable)}.$$

We call Z_x an ε-differentially private view of $x \in \mathcal{X}^n$.

Definition of Differential Privacy

The idea is the following:

- If the true database is $x \in \mathcal{X}^n$, the distribution of the output Z_x (in case $\mathcal{Z} = \mathbb{R}$) has cdf $F_x(t) := \mathbb{P}(Z_x \leq t) = \mathbb{P}(Z_x \in (-\infty, t])$.
- If I decide not to contribute my data x_i and the corresponding row of x is erased (x_i set to an arbitrary value), we obtain a new database, $x' \in \mathcal{X}^n$, say, with $x_i \neq x'_i$, that is, $d_0(x, x') = 1$.
- If Z_x is ε-DP, then

$$e^{-\varepsilon} \leq \frac{F_x(t)}{F_{x'}(t)} \leq e^{\varepsilon}, \quad \forall t \in \mathbb{R}.$$

- If ε is close to 0, this means that $F_x \approx F_{x'}$.
- Thus, the distribution of the output Z_x is almost the same, no matter if I contribute my data or not.

Verifying differential privacy using a pdf or pmf

For given $x \in \mathcal{X}^n$, let $q(\cdot|x)$ be a pdf or pmf of Z_x satisfying

$$q(z|x) \ \le e^{\varepsilon} q(z|x'), \quad \forall z \in \mathcal{Z}, \forall x, x' \in \mathcal{X}^n : d_0(x, x') \le 1.$$

Then , for every (measurable) $A \subseteq \mathcal{Z}$ and every $x, x' \in \mathcal{X}^n$ with $d_0(x, x') \le 1$,

$$\mathbb{P}(Z_x \in A) = \int_A q(z|x) dz \ \le \int_A e^{\varepsilon} q(z|x') dz = e^{\varepsilon} \mathbb{P}(Z_{x'} \in A), \quad \text{(pdf)}$$
$$\mathbb{P}(Z_x \in A) = \sum_{z \in A} q(z|x) \ \le \sum_{z \in A} e^{\varepsilon} q(z|x') = e^{\varepsilon} \mathbb{P}(Z_{x'} \in A), \quad \text{(pmf)}$$

Example: Sample mean

- Data: $x = (x_1, \dots, x_n)^T \in \mathbb{R}^n$, $-M \leq x_i \leq M$
- We want to publish $f(x) := \bar{x}_n = \frac{1}{n} \sum_{i=1}^n x_i$.
- Let $W \sim Laplace(\theta)$, with pdf $g_\theta(z) := \frac{\theta}{2} e^{-\theta|z|}$, $\theta > 0$.
- Publish $Z_x = f(x) + Laplace\left(\frac{n\varepsilon}{2M}\right)$.

$$q(z|x) = \frac{n\varepsilon}{4M} e^{-\frac{n\varepsilon}{2M}|z-f(x)|}$$

Properties of Differential Privacy

Proposition 5.1 (post-processing)

If Z_x is an ε-differentially private view of $x \in \mathcal{X}^n$ and $h : \mathcal{Z} \to \mathcal{Z}'$, then $h(Z_x)$ is also an ε-differentially private view of x.

Proposition 5.2 (sequential composition)

If $Z_x^{(1)}$ is an ε_1-DP view of $x \in \mathcal{X}^n$ and $Z_x^{(2)}$ is an ε_2-DP view of $x \in \mathcal{X}^n$, independent of $Z_x^{(1)}$, then $Z_x = (Z_x^{(1)}, Z_x^{(2)})$ is an $\varepsilon_1 + \varepsilon_2$-DP view of x.

Proposition 5.3 (parallel composition)

For $x = (x_1, \ldots, x_n)^T \in \mathcal{X}^n$, write $\xi = (x_1, \ldots, x_{n_1})^T \in \mathcal{X}^{n_1}$ and $\zeta = (x_{n_1+1}, \ldots, x_n)^T \in \mathcal{X}^{n-n_1}$. If Z_ξ is an ε_1-DP view of ξ and Z_ζ is an ε_2-DP view of ζ, independent of Z_ξ, then $Z_x = (Z_\xi, Z_\zeta)$ is a $\max(\varepsilon_1, \varepsilon_2)$-DP view of x.

Properties of Differential Privacy

Designing ε-DP mechanisms

SENSITIVITY OF QUERY FUNCTIONS

- Data: $x \in \mathcal{X}^n$
- Analyst would like to know $f(x)$ for some *query function* $f : \mathcal{X}^n \to \mathbb{R}$ (e.g., $f(x) = \bar{x}_n$).
- Define the *(global) sensitivity* of f by

$$\Delta_f := \sup_{\substack{x,x' \in \mathcal{X}^n \\ d_0(x,x') \leq 1}} |f(x) - f(x')|.$$

- Publish $Z_x = f(x) + Laplace\left(\frac{\varepsilon}{\Delta_f}\right)$.

$$q(z|x) = \frac{\varepsilon}{2\Delta_f} \exp\left(-\frac{\varepsilon}{\Delta_f}|z - f(x)|\right)$$

EXAMPLES OF (GLOBAL) SENSITIVITIES

Data: $x = (x_1, \ldots, x_n)^T \in \mathbb{R}^n$, $-M \leq x_i \leq M$.

- $f(x) = \bar{x}_n$
- $\Delta_f = \frac{2M}{n}$

- $f(x) = \max\{x_1 \ldots, x_n\}$
- $\Delta_f = 2M$

- $f(x) = med(x)$, n odd ($med(x) = x_{(\frac{n+1}{2})}$).
- $\Delta_f = 2M$

Attention: $M = M(x) := \max_i |x_i|$ is not allowed!!!

LOCAL SENSITIVITY OF QUERY FUNCTIONS

- Data: $x \in \mathcal{X}^n$
- Analyst would like to know $f(x)$ for some *query function* $f : \mathcal{X}^n \to \mathbb{R}$ (e.g., $f(x) = \bar{x}_n$).
- Define the *global sensitivity* of f by

$$\Delta_f := \sup_{\substack{x,x' \in \mathcal{X}^n \\ d_0(x,x') \leq 1}} |f(x) - f(x')|.$$

- Define the *local sensitivity* of f at $x \in \mathcal{X}^n$ by

$$\Delta_f(x) := \sup_{\substack{x' \in \mathcal{X}^n \\ d_0(x,x') \leq 1}} |f(x) - f(x')|.$$

EXAMPLES OF LOCAL SENSITIVITIES

Data: $x = (x_1, \ldots, x_n)^T \in \mathbb{R}^n$, $-M \leq x_i \leq M$.

- $f(x) = \bar{x}_n$
- $\Delta_f(x) = \frac{1}{n} \max_i \max\{|-M - x_i|, |M - x_i|\} \in [\frac{M}{n}, \frac{2M}{n}]$

- $f(x) = \max\{x_1 \ldots, x_n\} = x_{(n)}$
- $\Delta_f(x) = \max\{M - x_{(n)}, x_{(n)} - x_{(n-1)}\} \in [0, 2M]$

- $f(x) = med(x)$, n odd ($med(x) = x_{(\frac{n+1}{2})}$).
- $\Delta_f(x) = \max\{x_{(\frac{n+1}{2}+1)} - x_{(\frac{n+1}{2})}, x_{(\frac{n+1}{2})} - x_{(\frac{n+1}{2}-1)}\} \in [0, 2M]$

LOCAL SENSITIVITY OF QUERY FUNCTIONS

- Define the *local sensitivity* of f at $x \in \mathcal{X}^n$ by

$$\Delta_f(x) := \sup_{\substack{x' \in \mathcal{X}^n \\ d_0(x,x') \leq 1}} |f(x) - f(x')|.$$

Releasing

$$Z_x = f(x) + Laplace\left(\frac{\varepsilon}{\Delta_f(x)}\right)$$

is not ε-DP!

See *"approximate DP"* below!

INVERSE SENSITIVITY OF QUERY FUNCTIONS

- Data: $x \in \mathcal{X}^n$
- Analyst would like to know $f(x)$ for some *query function* $f : \mathcal{X}^n \to \mathbb{R}$.
- Define the *range* of f by $\mathcal{F} := f(\mathcal{X}^n) := \{f(x) : x \in \mathcal{X}^n\}$.
- Define the *inverse local sensitivity* of f at $(x, z) \in \mathcal{X}^n \times \mathcal{F}$ by

$$\Delta_f^{-1}(x, z) := \min\{d_0(x, x') : f(x') = z, x' \in \mathcal{X}^n\}.$$

- Define the *inverse local sensitivity* of f at $(x, z) \in \mathcal{X}^n \times \mathcal{F}$ by

$$\Delta_f^{-1}(x, z) := \min\{d_0(x, x') : f(x') = z, x' \in \mathcal{X}^n\}.$$

Then Z_x distributed with pmf

$$q(z|x) := \frac{\exp(-\frac{\varepsilon}{2}\Delta_f^{-1}(x, z))}{\sum_{u \in \mathcal{F}} \exp(-\frac{\varepsilon}{2}\Delta_f^{-1}(x, u))}, \quad z \in \mathcal{F}, x \in \mathcal{X}^n,$$

is ε-DP and

$$q(f(x)|x) \geq q(z|x), \quad \forall z \in \mathcal{F}.$$

INVERSE SENSITIVITY FOR DISCRETE $\mathcal{F}$

Proof:

Example: inverse sensitivity of counting query

$f(x) = \sum_{i=1}^{n} \mathbb{1}_A(x_i) \in \mathcal{F} = [n]$

$\Delta_f^{-1}(x, z) = \min\{d_0(x, x') : f(x') = z, x' \in \mathcal{X}^n\} =$

Repeated queries of the same database

- Data: $x = (x_1, \ldots, x_n)^T \in [-M, M]^n$
- m Analysts want to compute $f(x) = \bar{x}_n$.
- Let $W^{(1)}, \ldots, W^{(m)} \overset{i.i.d.}{\sim} Laplace(1)$.
- Publish $Z_x^{(j)} = f(x) + \frac{2M}{n\varepsilon} W^{(j)}$, $j = 1, \ldots, m$.

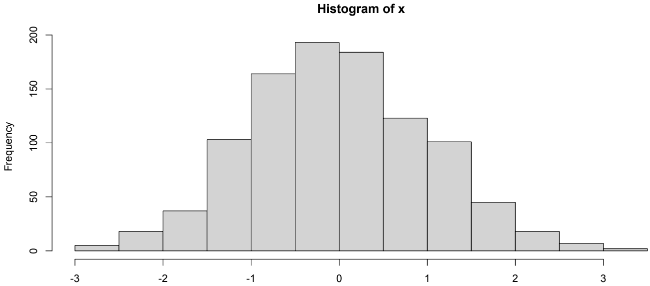
Adversary computes aggregate (recall sequential composition)

$$Z_x = \frac{1}{m} \sum_{j=1}^{m} Z_x^{(j)} = f(x) + \frac{2M}{n\varepsilon} \frac{1}{m} \sum_{j=1}^{m} W^{(j)} \quad \xrightarrow[m \to \infty]{LLN} \quad f(x).$$

Would like to release an ε-DP synthetic multi-purpose database once and for all.

Releasing a private histogram

- Data: $x = (x_1, \ldots, x_n)^T \in [L, U)^n$



$$k \in \mathbb{N}, h = (U - L)/k, \quad B_j := L + [(j-1)h, jh), \quad j \in [k],$$
$$\hat{c}_j := |\{i \in [n] : x_i \in B_j\}|,$$

Releasing a private histogram

- Data: $x = (x_1, \dots, x_n)^T \in [L, U)^n$
- $k \in \mathbb{N}, h = (U - L)/k, \quad B_j := L + [(j-1)h, jh), \quad j \in [k],$
- $\hat{c}_j(x) := |\{i \in [n] : x_i \in B_j\}|$

randomize:

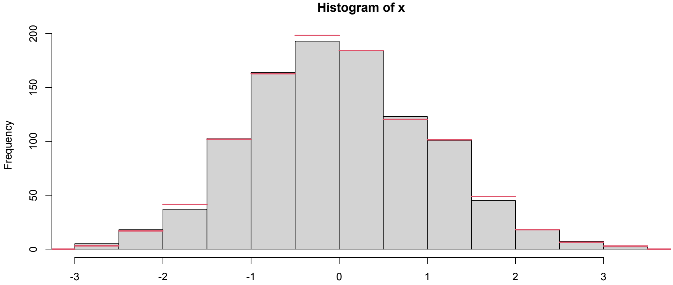
- $\tilde{c}_j := \hat{c}_j(x) + W_j, \quad W_j \overset{iid}{\sim} Laplace(\varepsilon/2).$
- $Z_x = (\tilde{c}_1, \dots, \tilde{c}_k)^T.$

$$q(z|x) = \prod_{j=1}^{k} \left[\frac{\varepsilon}{4} \exp\left(-\frac{\varepsilon}{2} |z_j - \hat{c}_j(x)| \right) \right], \quad z_j \in \mathbb{R}.$$

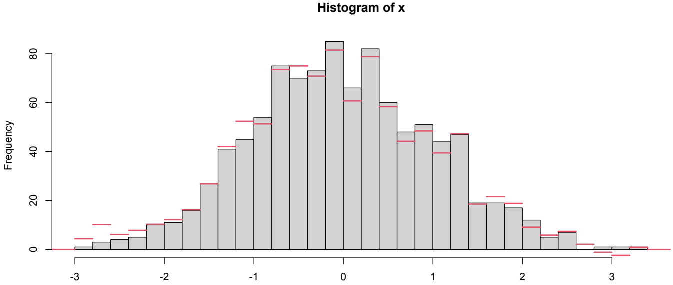
Releasing a private histogram

$$q(z|x) = \left(\frac{\varepsilon}{4}\right)^k \exp\left(-\frac{\varepsilon}{2}\|z - \hat{c}(x)\|_1\right), \qquad z \in \mathbb{R}^k$$

Releasing a private histogram

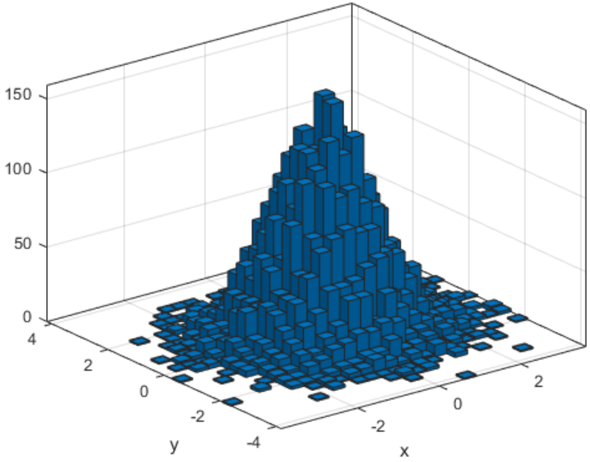


$\varepsilon = 1$



Releasing a private histogram

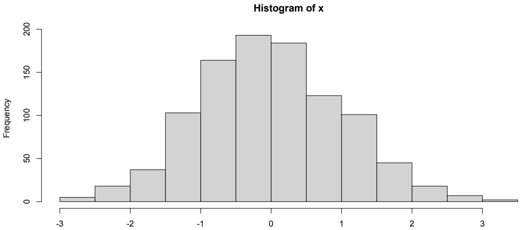
Can do the same for multivariate data $x = (x_1, \ldots, x_n)^T$, $x_i \in \mathbb{R}^p$.



RELEASING A PRIVATE HISTOGRAM

Suppose an analyst wants to compute $\bar{x}_n$.

Idea: Treat the histogram as a probability density function.



$$\hat{p}_n(y) := \sum_{j=1}^{k} \frac{\hat{c}_j}{nh} \mathbb{1}_{B_j}(y) \geq 0, \quad \int_{-\infty}^{\infty} \hat{p}_n(y)\, dy = \sum_{j=1}^{k} \frac{\hat{c}_j}{nh} h = 1$$

Releasing a private histogram

$$B_j = [l_j, l_j + h) = [L + (j-1)h, L + jh)$$

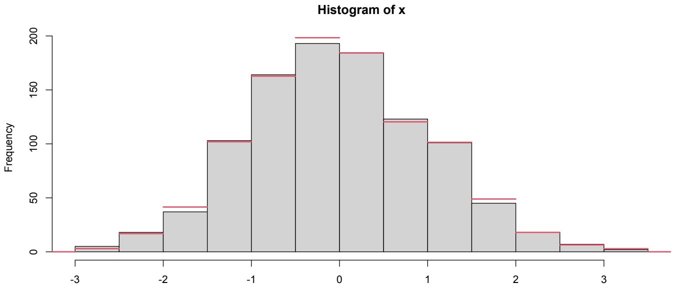
$$\bar{x}_n \approx \mathbb{E}_n[X] := \int_{-\infty}^{\infty} y \cdot \hat{p}_n(y)\, dy = \sum_{j=1}^{k} \frac{\hat{c}_j}{nh} \int_{l_j}^{l_j+h} y\, dy$$

$$= \sum_{j=1}^{k} \frac{\hat{c}_j}{2nh}((l_j + h)^2 - l_j^2) = \sum_{j=1}^{k} \frac{\hat{c}_j}{2nh}(2l_j h + h^2)$$

$$= \sum_{j=1}^{k} \frac{\hat{c}_j(l_j + \frac{h}{2})}{n}$$

Here $\bar{x}_n = -0.0075$, $\mathbb{E}_n[X] = -0.0095$.

Releasing a private histogram

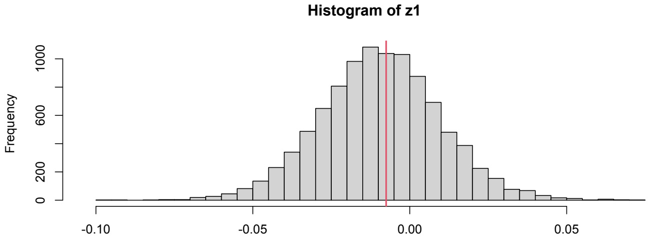


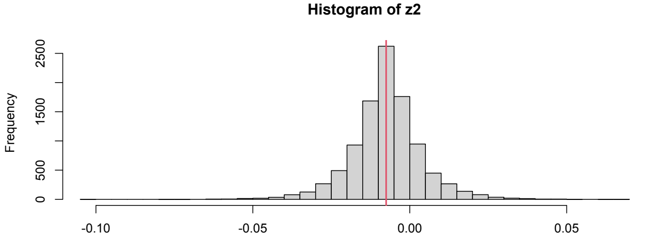
$$\mathbb{E}_n[X] = \sum_{j=1}^{k} \frac{\hat{c}_j(l_j + \frac{h}{2})}{n}, \quad \mathbb{E}_n[Z_x] := \sum_{j=1}^{k} \frac{\tilde{c}_j(l_j + \frac{h}{2})}{n}$$

Here $\mathbb{E}_n[Z_x] = -0.0845$ and $\bar{x}_n + Laplace(\frac{n\varepsilon}{2M}) = -0.03176$. $(M = 4)$

Releasing a private histogram: simulation

Compare mean from private histogram ($\bar{Z}_1$) with perturbed sample mean ($\bar{Z}_2$). $x \in \mathbb{R}^n$ fixed, $\bar{x}_n = -0.0075$





Approximate differential privacy

Definition of Differential Privacy

For $x, x' \in \mathcal{X}^n$, define the Hamming distance

$$d_0(x, x') := \#\{i : x_i \neq x'_i\}.$$

Definition (Dwork et al. 2006)

Fix a privacy level $\varepsilon \in (0, \infty)$. The randomization mechanism outputting Z_x on $\mathcal{Z}$ for a given $x \in \mathcal{X}^n$, is called ε-differentially private if for all $x, x' \in \mathcal{X}^n$ with $d_0(x, x') \leq 1$, we have

$$\mathbb{P}(Z_x \in A) \ \leq e^{\varepsilon}\mathbb{P}(Z_{x'} \in A), \quad \forall A \subseteq \mathcal{Z} \textit{ (measurable).}$$

We call Z_x an ε-differentially private view of $x \in \mathcal{X}^n$.

Definition of Approx. Differential Privacy

For $x, x' \in \mathcal{X}^n$, define the Hamming distance

$$d_0(x, x') := \#\{i : x_i \neq x_i'\}.$$

Definition

Fix $\varepsilon \in (0, \infty)$ and $\delta \in [0, 1]$. The randomization mechanism outputting Z_x on $\mathcal{Z}$ for a given $x \in \mathcal{X}^n$, is called (ε, δ)-approximately differentially private if for all $x, x' \in \mathcal{X}^n$ with $d_0(x, x') \leq 1$, we have

$$\mathbb{P}(Z_x \in A) \leq e^{\varepsilon}\mathbb{P}(Z_{x'} \in A) + \delta, \quad \forall A \subseteq \mathcal{Z} \text{ (measurable)}.$$

We call Z_x an (ε, δ)-approximately differentially private view of $x \in \mathcal{X}^n$.

Failure of ADP

Consider the following mechanism:

- $\mathcal{Z} = \mathcal{X}^n \cup \{\varnothing\}$, $\delta \in [0, 1]$

$$Z_x = \begin{cases} x, & \text{with probability } \delta, \\ \varnothing, & \text{with probability } 1 - \delta. \end{cases}$$

$$q(z|x) = \mathbb{P}(Z_x = z) = \left\{\begin{matrix} \delta, & \text{if } z = x, \\ 1-\delta, & \text{if } z = \varnothing, \\ 0, & \text{else} \end{matrix}\right\} \leq e^{\varepsilon} q(z|x') + \delta$$

- This is (ε, δ)-ADP for any $\varepsilon \geq 0$!!!

Local sensitivities revisited

- Recall: *local sensitivity* of f at $x \in \mathcal{X}^n$

$$\Delta_f(x) := \sup_{\substack{x' \in \mathcal{X}^n \\ d_0(x,x') \leq 1}} |f(x) - f(x')|.$$

- Note: For many query functions $f : \mathcal{X}^n \to \mathbb{R}$

$$Z_x = f(x) + \frac{\Delta_f(x)}{\varepsilon} W, \quad \text{with } W \sim \mathit{Laplace}\,(1)$$

is (ε, δ)-ADP, if and only if, $\delta = 1$.

Local sensitivities revisited

$$Z_x = f(x) + \frac{\Delta_f(x)}{\varepsilon} W, \quad \text{with } W \sim Laplace\,(1)$$

Propose-test-release

Define

$$
\begin{aligned}
A_f(x,k) &:= \sup_{y: d_0(x,y) \leq k} \Delta_f(y) \\
D_f(x,b) &:= \min\{k \in \mathbb{N}_0 : A_f(x,k) > b\} \\
&\quad \min\ \varnothing := \infty
\end{aligned}
$$

1. The analyst proposes a value $b > 0$.
2. If $D_f(x,b) + \frac{1}{\varepsilon} Laplace(1) < \frac{\log(2/\delta)}{2\varepsilon}$, output $Z_x = \varnothing$.
3. Otherwise, output

$$
Z_x = f(x) + \frac{b}{\varepsilon} W, \quad \text{with } W \sim Laplace\,(1)\,.
$$

This satisfies (ε, δ)-ADP.

Propose-test-release

Define

$$A_f(x,k) := \sup_{y:d_0(x,y)\leq k} \Delta_f(y)$$

$$D_f(x,b) := \min\{k \in \mathbb{N}_0 : A_f(x,k) > b\}$$

In step 2 we do the test

$$D_f(x,b) + \frac{1}{\varepsilon} Lap(1) < \frac{\log(2/\delta)}{2\varepsilon}.$$

Note:

$$\begin{aligned} b_1 \leq b_2 \quad &\Rightarrow \quad D_f(x,b_1) \leq D_f(x,b_2) \\ b < \Delta_f(x) \quad &\Rightarrow \quad D_f(x,b) = 0 \\ b \geq \Delta_f \quad &\Rightarrow \quad D_f(x,b) = \infty. \end{aligned}$$

Differential Privacy: Summary

Pros:

- DP provides a mathematically rigorous definition of privacy protection.
- Can develop a theory of optimal privacy mechanisms.
- It protects against worst case adversaries using any kind of auxiliary information.

Cons:

- Results are always noisy. Too much noise?
- Especially difficult for high-dimensional and unbounded data.
- Many alternative definitions are in use (e.g., ADP, etc.).
- Optimal data release mechanism depends on the query of interest/the statistical estimation problem. No universally optimal synthetic data release.
- Many open questions remain...