PDS, 3.11.

5.4) ε – Closeness

Dataset, sensitive attr. $\mathcal{S}$

Here: $\mathcal{S} = \{S\}$

- Initial assumption

characterized by a random variable (r.v.) A over S

$$A \in S : \sum_{s \in S} P_A(s) = 1$$

Ex. 1 not dependent on dataset!

iOS	And.	Mac	Win	Linux
$1/5$	$1/5$	$1/5$	$1/5$	$1/5$

- Completely generalized dataset, statistic over S, a r.v. Q

$Q \in S$, with

$$P_Q(s) = \frac{\text{no. entries with } S=s}{\text{no. entries}}$$

In Ex. 1:

Q

s	And.	iOS	Mac	Win.	Lin
$P_Q(s)$	$2/9$	$1/9$	$2/9$	$3/9$	$1/9$

P_Q is empirical distr.

- When observer learns values of Q.I. in one partition, then one equiv. class C remains.

Let L denote the r.v. of attr. S restricted to C: this is the information leaked.

$$L \in S: \; P_L(s) = \frac{\text{no. entries in } C \text{ with } S=s}{\text{no. entries in } C}$$

- Recall: P_A, P_Q, P_L are distributions over S

Def: An equivalence class C is ε-close to the dataset whenever

$$D(P_L \,;\, P_Q) \leq \varepsilon .$$

A dataset has ε-closeness when all its equivalence classes are ε-close to the dataset.

D is a distance "measure" between prob. distributions.

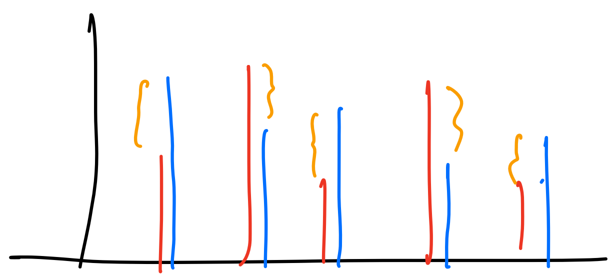
Some examples are:

- L_2 - norm

- L_1 - distance

Variational distance

$$\Delta(P_L; P_Q) = \frac{1}{2} \sum_{s \in S} \left| P_L(s) - P_Q(s) \right|$$



- Kullbach-Leibler divergence

(relative entropy)

$$KL(P_L \| P_Q) = \sum_{s \in S} P_L(s) \log_2 \frac{P_L(s)}{P_Q(s)}$$

Last name	First name	PLZ	Points	System
I	I	QI	QI	S

Sample data set

Andreasyan	Narek	3270	89	iOS
Asadauskas	Marius Paulius	3294	77	Android
Ayinkamiye	Leïla	3400	90	MacOS
Berger	Reto	2608	42	Windows
Bucheli	Philippe	3177	38	Linux
Bühlmann	Noah Florian	2740	35	Windows
Brunner	Julien Pierre	3763	25	MacOS
Egger	Dominic Mathias	3860	33	Windows
Gerig	Pascal Dominik	3770	30	Android

3-Anonymous data set

		3200-3299	75-90	iOS
		3200-3299	75-90	Android
		3200-3299	75-90	MacOS
		2600-3199	35-45	Windows
		2600-3199	35-45	Linux
		2600-3199	35-45	Windows
		3700-3899	25-34	MacOS
		3700-3899	25-34	Windows
		3700-3899	25-34	Android

Revisit Ex. 1:

Q

s	And.	iOS	Mac	Win.	Lin
$P_Q(s)$	$2/9$	$1/9$	$2/9$	$3/9$	$1/9$

L_{32}

And	iOS	Mac
$1/3$	$1/3$	$1/3$

$$\Delta(P_{L32}; P_Q) = \frac{1}{2}\left(\frac{1}{9} + \frac{2}{9} + \frac{1}{9} + \frac{3}{9} + \frac{1}{9}\right)$$

$$= \frac{1}{2} \frac{8}{9} = \frac{4}{9} = 0.44\ldots$$

<u>Def:</u> An equivalence class C is <u>(n, ε)-close</u> to the full dataset iff

there exists a subset M of dataset s.t. $|M| \geq n$ and

$$D(P_L; P_{Q|M}) \leq \varepsilon$$

where $P_{Q|M}$ denotes the empirical distr. of in Q restricted to M.

A partitioning C is <u>(n, ε)-close</u> to the dataset iff. exists a subset M of dataset with $|M| \geq n$ s.t.

each each equiv. class L satisfies

$$D(P_L ; P_{Q|M}) \leq \varepsilon .$$

- Uses any subset of sufficient size for reference to hide the disclosed distr. among this set.

Recap

Persons $\quad \underline{P_1} \quad \underline{P_2} \quad \ldots \quad \underline{P_n}$

sensitive data

Trusted aggregator $\quad T$

sanitized dataset

Consumes statistic, learns data $\quad$ Public

6) Differential privacy

6.1) Randomized response

n persons, each has a sensitive value $X_i \in \{0,1\}$

Suppose each X_i is Bernoulli r.v. with prob. p, i.e.,

$$P[X_i = 1] = p$$

(unknown p)

Observer wants to learn (estimate) the value of p, but must not violate privacy of persons.

Ex. $n = 18$ students
1 observer / teacher

Q: Have you ever cheated in an exam?

Idea: Add randomization that lets each P_i deny the sensitive value.

$$P_i \text{ sends } Y_i = \begin{cases} X_i & \text{w/prob. } \overset{1/2}{\overset{\shortparallel}{\alpha}} \\ R_i & \text{w/prob. } 1-\alpha \end{cases}$$

where $R_i \in \{0, 1\}$ is uniformly random

⚠ Up to two random choices.

Observer receives all Y_i values.

no. of $Y_i = 1$: 9

$Y_i = 0$: 9

- Observer can still estimate the true value of p

- Role α?

Tradeoff between utility and privacy:

$\alpha = 0$: no utility, full privacy

$\alpha = 1$: full utility, no privacy

- What do we learn?

$$Y = \sum_i Y_i \qquad (= 3)$$

Recall $P_{X_i}(1) = p$, $E[X_i] = p$

$$E[Y_i] = \alpha E[X_i] + (1-\alpha) \cdot E[R_i]$$
$$= \alpha \cdot p + \frac{1-\alpha}{2}$$

<u>or</u>

$$p = \frac{1}{\alpha}\left(E[Y_i] - \frac{1-\alpha}{2}\right)$$

After observing Y, compute estimator for p as

$$\tilde{p} = \frac{1}{\alpha}\left(\frac{Y}{n} - \frac{1-\alpha}{2}\right)$$

$$= \frac{1}{\alpha}\left(\frac{\sum_i Y_i}{n} - \frac{1-\alpha}{2}\right)$$

$$= \frac{1}{\alpha n} \underbrace{\sum Y_i} - \frac{1-\alpha}{2\alpha}$$

$\alpha = \frac{1}{2}$

g

$$\tilde{p} = 2 \cdot \frac{1}{2} - \frac{1-\frac{1}{2}}{1} = \frac{1}{2}$$

How accurate?

$$\text{Var}[\tilde{p}] = \text{Var}\left[\frac{1}{\alpha n}\sum Y_i - \frac{1-\alpha}{2\alpha}\right]$$

$$= \frac{1}{\alpha^2 n^2} \text{Var}\left[\sum_i Y_i\right]$$

$$= \frac{1}{\alpha^2 n^2} \sum_i \text{Var}[Y_i]$$

$$\text{Var}[Y_i] \leq 1$$

$$= \frac{1}{\alpha^2 n}$$

Using Chebshev inequality:

$$P\left[|\tilde{p} - p| \geq \varepsilon \right] \leq \frac{Var[\tilde{p}]}{\varepsilon^2}$$

$$\leq \frac{1}{\alpha^2 \cdot n \cdot \varepsilon^2}$$

Increasing n leads to a better estimate.
Decreasing α leads to less accurate estimation.

6.2) Defining Differential Privacy (DP)

- Given n data values

$$[X_1, \ldots, X_n] = X^n$$

corresp. to sensitive values of n individuals; $X_i \in \mathcal{X}$

- $\mathcal{X} = \{0, 1\}$
- $\mathcal{X} = \mathbb{N}$

- An <u>algorithm</u> $M: \mathcal{X}^n \longrightarrow \mathcal{Y}$ sanitizes a vector $X^n \in \mathcal{X}^n$ and outputs $Y \in \mathcal{Y}$.

- M must be randomized
- DP is feature of the algorithm

<u>Def:</u> Two datasets X^n and $\bar{X}^n$ are <u>neighbouring</u>, denoted

$$X^n \sim \bar{X}^n$$

whenever $\exists i: X_i \neq \bar{X}_i \wedge$

$$\forall j \neq i: X_j = \bar{X}_j$$

(Differ in exactly one component.)

<u>Def:</u> A (randomized) alg. $M: \mathcal{X}^n \rightarrow \mathcal{Y}$ is <u>ε-differentially private</u> iff.

$\forall Y \subseteq \mathcal{Y}$ and

$\forall X^n$ and $\bar{X}^n$ s.t. $X^n \sim \bar{X}^n$:

$$\mathbb{P}\left[M(X^n) \in Y\right] \leq e^{\varepsilon} \cdot \mathbb{P}\left[M(\tilde{X}^n) \in Y\right].$$