Differential Privacy: An Introduction

Financial Statistics & Risk Management

Rohit Rao. Smrithi Shankar.

Summary / Abstract

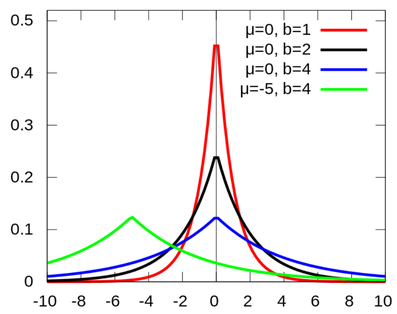
We aim to introduce the idea of differential privacy with motivation, definitions, and some basic theorems. We then provide an example of differential privacy applied to the problem of finding the interquartile range (IQR). We give an algorithm to find IQR using differential privacy and show a proof sketch that this algorithm guarantees at least $(3\epsilon, n^{-\epsilon \ln n})$-differential privacy.

Problem and Motivation

- Sample scenario: Census Bureau gathers sensitive information and wants to release statistics about the population without compromising people's privacy.
- This is where differential privacy is useful as it provides a mathematically rigorous guarantee of protecting privacy while sharing data.
- This idea is especially important in many fields like finance, healthcare, and the social sciences.

Preliminary Definitions and Notation

- A **database** D is a set of rows. Databases D and D' are **adjacent** if their hamming distance is 1
  - Ex: If we have n people each of whose data is d bits, then $D \in (\{0,1\}^d)^n$.
- **Definition 1:** A randomized function $\mathcal{K}$ gives (ϵ, δ)-differential privacy if for all pairs of adjacent databases D and D', and all $S \subseteq Range(\mathcal{K})$, we have
  $$P[\mathcal{K}(D) \in S] \leq e^{\epsilon} P[\mathcal{K}(D') \in S] + \delta$$
- When using P(*) and P'(*), the first is for input database D and the other is for input database D'.
- $\tilde{P}(*)$ factors in randomness in both D and $\mathcal{K}$.
- **Definition 2:** For $f: \mathcal{D} \to \mathbb{R}^d$, the sensitivity of f is $\Delta f = \max_{D,D'} \|f(D) - f(D')\|_1$ for all adjacent D, D'
- The **laplace distribution** $Lap(b)$ has PDF $p(x) = \frac{1}{2b} * e^{-|x|/b}$.



Differentially Private Interquartile Range (IQR)

Theorem 3: Let $\mathcal{D}$ denote the universe of databases. For $f: \mathcal{D} \to \mathbb{R}^d$, the mechanism $\mathcal{K}_f$, that on input a database D, computes $f(D)$ and then adds independently generated noise with distribution $\text{Lap}(\Delta f/\epsilon)$ to each of the k output terms satisfies ϵ-differential privacy. (Similar to Definition 1 without δ.)

Propose-Test-Release Framework

- Propose an upper bound on the local sensitivity.
- Test in a private manner whether that bound is sufficiently large.
- If so, release the answer with noise, otherwise do not release the answer (return "no response" denoted $\perp$).

Scale

- A classical problem of measuring the variability or dispersion of data by computing the IQR.
- Below we give an algorithm $\mathcal{S}$ to compute IQR using differential privacy.

The algorithm $\mathcal{S}$:

- Input: (D, n, ε).

1. For the jth discretization $(j = 1, 2)$
   - Compute $R_0(D) = A_0(D) + z_0$, where z_0 is a random draw from $\text{Lap}(1/\varepsilon)$.[a]
   - If $R_0 \leq \ln^2 n + 1$, let $s^{(j)} = \perp$.
   - Otherwise let $s^{(j)} = IQR(D) \times (1 + \frac{1}{\ln n})^{z_s^{(j)}}$, where $z_s^{(j)}$ is another random draw from $\text{Lap}(1/\varepsilon)$.
2. If $s^{(1)} \neq \perp$, return $s^{(1)}$.
   Otherwise return $s^{(2)}$.

[a] $IQR(D) = 0$ is fine, since one can define $\log 0 = -\infty$, $\lfloor -\infty \rfloor = -\infty$, and let $[-\infty, -\infty) = \{-\infty\}$.

Intuition

- Suppose the data is IID drawn from an underlying distribution F.
- If the sample IQR (SIQR) is very sensitive, return $\perp$.
- Else, SIQR is not sensitive – we can return this with some additive noise $Lap(1/\varepsilon)$
- We now define query Q_0 as follows:
  Q_0: How many data points need to change in order to get a new database $\widehat{D}$ such that $H_n(\widehat{D}) \notin B_{k_1}^{(1)}$?
- The query:
  1. ensures that returning $\perp$ doesn't disclose information
  2. helps test whether the magnitude of noise is sufficient for differential privacy
- For 2, we discretize $\mathbb{R}$ into disjoint bins $\{[kw_n, (k+1)w_n]\}_{k \in \mathbb{Z}}$ where $w_n = \ln(1 + 1/\ln n)$. Viewing $\ln(IQR(D))$ on the scale of w_n is equivalent to viewing $\log_{1+1/\ln n}(IQR(D))$ on the scale of 1.
- Let $H_n(D) = \log_{1+1/\ln n}(IQR(D))$, and $B_k^{(1)} = [k,\ k+1]$, for $k \in \mathbb{Z}$, where these are scaled bins. Then, there exists a k_1 such that $H_n(D) \in [k_1, k_1 + 1)$.
  - If $H_n(D)$ is close to an integer, then it's likely that it returns $\perp$. So, we also consider discretization $B_k^{(2)} = [k - 0.5, k + 0.5], k \in \mathbb{Z}$.
- For the analysis, let the true answer to $\boldsymbol{Q_0}$ be $A_0(D)$ and $R_0(D) = A_0(D) + z_0$ where $z_0 \sim Lap(1/\epsilon)$.

Please refer to section 4, page 12 of Dwork and Lei's work for more detailed intuition.

Proofs Regarding Algorithm $\mathcal{S}$

Lemma 4: The sensitivity of $\boldsymbol{Q_0}$ is at most 1.

Proof

If $H_n(D)$ and $H_n(D')$ are in different bins, then $A_0(D) = A_0(D') = 1$. Else, they are in the same bin. Thus, in both cases $|A_0(D) - A_0(D')| \leq 1$.

Lemma 5: Let s be shorthand for the result obtained with a single discretization. Let $\mathcal{D}_0 = \{D: A_0(D) \geq 2\}$.

a) $P(s = \perp) \leq e^{\epsilon} P'(s = \perp)$

b) $P(s \neq \perp) \leq \frac{1}{2} n^{-\epsilon \ln n}$ for all $D \notin \mathcal{D}_0$

c) $P(s \in C) \leq e^{2\epsilon} P'(s \in C)$, for all $C \in \mathbb{R}^+$ and $D \in \mathcal{D}_0$.

Proofs

a) For all $D \in \mathcal{D}$, $s(D) = \perp \Leftrightarrow R_0(D) \leq \ln^2 n + 1$. Also, for small $R_0(D)$, $\boldsymbol{Q_0}$ returns $\perp$. By lemma 4, the sensitivity is at most 1 so applying theorem 3, we get the desired result.

b) When $D \notin \mathcal{D}_0$, then $A_0(D_1) \leq 1$. So,

$$P(s \neq \perp) \leq P(R_0(D) \geq \ln^2 n + 1) = P(A_0(D) + z_0 \leq \ln^2 n + 1) \leq P(z_0 \geq \ln^2(n)) \leq \frac{1}{2} n^{-\epsilon \ln n}$$

c) When $D \in \mathcal{D}_0$, $A_0(D_1) \geq 2$, and so $|H_n(D) - H_n(D')| \leq 1$. So $P(s \in C) =$

$$\int_{v \in C} \int_{u > (\ln n)^2 + 1} p\,(R_0 = u) p\left(H_n + z_s = \log_{1+1/\ln n}(v) \,|R_0 = u\right) du dv \leq$$

$$\int_{v \in C} \int_{u > (\ln n)^2 + 1} e^{\varepsilon} p'\,(R_0 = u) e^{\varepsilon} p'\left(z_s = \log_{1+1/\ln n}(v) - H_n\right) du dv = e^{2\varepsilon} P'(s \in C).$$

Theorem 6: $\mathcal{S}$ is $\left(3\epsilon, n^{-\epsilon \ln n}\right)$-differentially private.

Proof

By Lemma 5, both $s^{(1)}$ and $s^{(2)}$ are $\left(2\epsilon, \frac{1}{2} n^{-\varepsilon \ln n}\right)$-differentially private $\Rightarrow$ for any $C^* \subseteq \mathbb{R}^{\geq 0} \cup \{\perp\}$, we have $P\left(s^{(j)} \in C^*\right) \leq e^{2\varepsilon} P'^{\left(s^{(j)} \in C^*\right)} + \frac{1}{2} n^{-\varepsilon \ln n}$. Then, by independence, similar to the conditional argument of Lemma 5, for any $C \subseteq \mathbb{R}^{\geq 0} \cup \{\perp\}$, $P(\mathcal{S} \in C) \leq$

$$P\left(s^{(1)} \in C \setminus \{\perp\}\right) + P\left(s^{(1)} = \perp, s^{(2)} \in C \setminus \{\perp\}\right) + P\left(s^{(1)} \in C \cap \{\perp\}, s^{(2)} \in C \cap \{\perp\}\right)$$

$$\leq e^{2\varepsilon} P'\left(s^{(1)} \in C \setminus \{\perp\}\right) + \frac{1}{2} n^{-\varepsilon \ln n} + e^{2\varepsilon} P'\left(s^{(1)} = \perp, s^{(2)} \in C \setminus \{\perp\}\right) + \frac{1}{2} n^{-\varepsilon \ln n} +$$

$$e^{2\varepsilon} P'\left(s^{(1)} \in C \cap \{\perp\}, s^{(2)} \in C \cap \{\perp\}\right) \leq e^{3\varepsilon} P'(\mathcal{S} \in C) + n^{-\varepsilon \ln n}.$$

Other Properties of Algorithm $\mathcal{S}$

We state the following without proof:

1. The computation for $\mathcal{S}$ is $O(n)$ if the data is sorted.
2. If $D = (X_1, \ldots, X_n)$, $X_i \overset{\text{i.i.d.}}{\sim} F$, where F is differentiable with positive derivatives at upper and lower quartiles, then $\tilde{P}(\mathcal{S}(D) = \perp) = O\left(n^{-\varepsilon \ln n}\right)$, and $\mathcal{S}(D) - IQR(F) \overset{\tilde{P}}{\to} 0$
3. Under the same conditions as in 2, for any $\alpha > 0$, $P(\mathcal{S}(D) \in [n^{-\alpha} IQR(D), n^{\alpha} IQR(D)]) \geq 1 - O\left(n^{-\alpha\varepsilon \ln n}\right)$, as a result of which we have $\tilde{P}(\mathcal{S}(D) \in [1/2\, n^{-\alpha} IQR(F), 2n^{\alpha} IQR(F)]) \geq 1 - O\left(n^{-\alpha\varepsilon \ln n}\right)$.

Conclusions

- Through this study, not only were privacy-preserving estimators established, but they were in fact established right from known robust procedures.
- The differentially private algorithm covered in this study always ensures privacy, with distortion vanishing as dataset size increases under mild statistic assumptions

References

- C. Dwork and A. Smith, "Differential Privacy for Statistics: What we Know and What we Want to Learn", JPC, vol. 1, no. 2, Apr. 2010.
- C. Dwork and J. Lei, "Differential Privacy and Robust Statistics", Nov. 2008.