A Statistical Framework for Differential Privacy

Yang Yu

Department of Statistics
Purdue University

Nov 24, 2015

(Work by Larry Wasserman and Shuheng Zhou)

Introduction

Goals:

- To explain differential privacy in statistical language.
- To show how to compare different privacy mechanisms by computing the rate of convergence of distributions and densities based on the released data Z.
- To study a general privacy method, called the exponential mechanism, due to McSherry and Talwar (2007).

Introduction

Goals:

- To explain differential privacy in statistical language.
- To show how to compare different privacy mechanisms by computing the rate of convergence of distributions and densities based on the released data Z.
- To study a general privacy method, called the exponential mechanism, due to McSherry and Talwar (2007).

Two disclaimers:

- We will not attempt to review all approaches to privacy or to compare differential privacy with other approaches.
- We focus only on statistical properties and shall not be concerned with computational efficiency.

Outline

Differential Privacy

Notations

- $X_1, \dots, X_n \overset{iid}{\sim} P$, where $X_i \in \mathcal{X}$.
- $\mathcal{X} \equiv [0,1]^r = [0,1] \times [0,1] \times \cdots \times [0,1]$ for some integer $r \geq 1$.
- μ: Lebesgue measure.
- $p = dP/d\mu$ if the density exist.
- Take a database $X \in \mathcal{X}^n$ as input and output a sanitized database $Z = (Z_1, \dots, Z_k) \in \mathcal{X}^k$ for public release.
- $k \equiv k(n)$ changes with n.

- Scheme:

$$\text{input database } X = (X_1, \ldots, X_n)$$
$$\xrightarrow[\text{sanitize}]{Q_n(Z \mid X)} \text{output database } Z = (Z_1, \ldots, Z_k)$$

- Input database: $X = (X_1, \ldots, X_n) \in \mathcal{X}^n$
- Output database: $Z = (Z_1, \ldots, Z_k) \in \mathcal{X}^k$
- Data-release mechanism $Q_n(\cdot \mid X)$: $Q_n(B \mid X = x) = \mathbb{P}(Z \in B \mid X = x)$ for $B \in \mathcal{B}$, where $\mathcal{B}$ are the measurable subsets of $\mathcal{X}^k$.

Definition 1 (Hamming Distance)

Given two databases $X = (X_1, \ldots, X_n)$ and $Y = (Y_1, \ldots, Y_n)$, let $\delta(X, Y)$ denote the Hamming distance between X and Y:
$\delta(X, Y) = \#\{i : X_i \neq Y_i\}$.

Definition 2 (Differential Privacy)

Let $\alpha \geq 0$. We say that Q_n satisfies α-differential privacy if

$$\sup_{\substack{x,y \in \mathcal{X}^n \\ \delta(x,y)=1}} \sup_{B \in \mathcal{B}} \frac{Q_n(B \mid X = x)}{Q_n(B \mid X = y)} \leq e^{\alpha}, \tag{1}$$

where $\mathcal{B}$ are the measurable sets on $\mathcal{X}^k$. The ratio is interpreted to be 1 whenever the numerator and denominator are both 0.

Differential Privacy

Definition

Definition 2 (Differential Privacy)

Let $\alpha \geq 0$. We say that Q_n satisfies α-differential privacy if

$$\sup_{\substack{x,y \in \mathcal{X}^n \\ \delta(x,y)=1}} \sup_{B \in \mathcal{B}} \frac{Q_n(B \mid X = x)}{Q_n(B \mid X = y)} \leq e^{\alpha}, \tag{1}$$

where $\mathcal{B}$ are the measurable sets on $\mathcal{X}^k$. The ratio is interpreted to be 1 whenever the numerator and denominator are both 0.

- This definition of privacy is based on ratios of probabilities. It protects rare cases which have small probability under Q_n.
- If changing one entry in the database X cannot change the probability distribution $Q_n(\cdot \mid X = x)$ very much, then a single individual cannot guess whether he is in the original database or not.
- The closer e^{α} is to 1, the stronger privacy guarantee is.
- Typically, α is chosen to be close to 0.

Differential Privacy

Justification

Suppose that two subjects each believe that one of them is in the original database. Given Z and full knowledge of P and Q_n can they test who is in X?

Theorem 3 (Justifying the Definition)

Suppose that Z is obtained from a data release mechanism that satisfies α-differential privacy. Any level γ test which is a function of Z, P, and Q_n of $H_0 : X_i = s$ versus $H_1 : X_i = t$ has power bounded above by γe^{α}.

Differential Privacy

Justification

Suppose that two subjects each believe that one of them is in the original database. Given Z and full knowledge of P and Q_n can they test who is in X?

Theorem 3 (Justifying the Definition)

Suppose that Z is obtained from a data release mechanism that satisfies α-differential privacy. Any level γ test which is a function of Z, P, and Q_n of $H_0 : X_i = s$ versus $H_1 : X_i = t$ has power bounded above by γe^{α}.

- In this result, we drop the assumption that the user does not know Q_n.
- If Q_n satisfies differential privacy, then it is virtually impossible to test the hypothesis that either of the two subjects is in the database, since the power of such a test is nearly equal to its level.

Informative Mechanisms

Assumption

- A challenge in privacy theory: To find Q_n that satisfies differential privacy and yet yields datasets that preserve information.
- Whether or not a mechanism is informative will depend on the goals of the inference.
- We would like to infer P or functionals of P from Z.
- Assume that the user has access to the sanitized data Z but not the mechanism Q_n.

Informative Mechanisms

Definition

- F: The cdf on $\mathcal{X}$ corresponding to P.
- $\hat{F} \equiv \hat{F}_X$: The empirical distribution function corresponding to X.
- $\hat{F}_Z$: The empirical distribution function corresponding to Z.
- ρ: Any distance measure on distribution functions.

Definition 4 (Informative Mechanism)

Q_n is consistent with respect to ρ if $\rho(F, \hat{F}_Z) \xrightarrow{P} 0$. Q_n is ϵ_n-informative if $\rho(F, \hat{F}_Z) = O_P(\epsilon_n)$.

Informative Mechanisms

Definition

- F: The cdf on $\mathcal{X}$ corresponding to P.
- $\hat{F} \equiv \hat{F}_X$: The empirical distribution function corresponding to X.
- $\hat{F}_Z$: The empirical distribution function corresponding to Z.
- ρ: Any distance measure on distribution functions.

Definition 4 (Informative Mechanism)

Q_n is consistent with respect to ρ if $\rho(F, \hat{F}_Z) \xrightarrow{P} 0$. Q_n is ϵ_n-informative if $\rho(F, \hat{F}_Z) = O_P(\epsilon_n)$.

- This way to measure the information in Z is through distribution functions.
- Alternatives to requiring $\rho(F, \hat{F}_Z)$ to be small:
  - To require $\rho(\hat{F}, \hat{F}_Z)$ to be small.
  - To require $Q_n(\rho(F, \hat{F}_Z) > \epsilon \,|\, X = x)$ to be small.

Informative Mechanisms

Distance Function

Main possible choices for ρ:

- Kolmogorov-Smirnov (KS) distance: $\rho(F, G) = \sup_x |F(x) - G(x)|$.
- Squared L_2 distance: $\rho(F, G) = \int (f(x) - g(x))^2 dx$ where $f = dF/d\mu$ and $g = dG/d\mu$.

Sampling From a Histogram

Introduction

Two concrete, simple data-release methods that achieve differential privacy.

- Idea: To draw a random sample from a histogram.
- First scheme: To draw observations from a smoothed histogram.
- Second scheme: To draw observations from a perturbed histogram.

Sampling From a Histogram

Introduction

Two concrete, simple data-release methods that achieve differential privacy.

- Idea: To draw a random sample from a histogram.
- First scheme: To draw observations from a smoothed histogram.
- Second scheme: To draw observations from a perturbed histogram.

Why histogram?

- Familiarity and simplicity.
- Used in applications of differential privacy.

Sampling From a Histogram

Assumption

- Let $L > 0$ be a constant and suppose that $p = dP/d\mu \in P$ where

$$\mathcal{P} = \{p : |p(x) - p(y)| \leq L \|x - y\|\} \tag{2}$$

  is the class of Lipchitz functions.
- The minimax rate of convergence for density estimators in KS distance for $\mathcal{P}$ is $n^{-1/2}$.
- The minimax rate of convergence for density estimators in squared L_2 distance for $\mathcal{P}$ is $n^{-2/(2+r)}$ (Scott 1992).

Sampling From a Histogram

Histogram Estimator

- Let $h = h_n$ be a binwidth s.t. $0 < h < 1$ and $m = 1/h^r$ is an integer. Partition $\mathcal{X}$ into m bins $\{B_1, \ldots, B_m\}$ where each bin B_j is a cube with sides of length h.
- $\hat{f}_m$: The histogram estimator on $\mathcal{X}$, namely,

$$\hat{f}_m(x) = \sum_{j=1}^{m} \frac{\hat{p}_j}{h^r} I(x \in B_j),$$

where $\hat{p}_j = C_j/n$ and $C_j = \sum_{i=1}^{n} I(X_i \in B_j)$ is the number of observations in B_j.

Sampling From a Smoothed Histogram

Definition

- Fix a constant $0 < \delta < 1$ and define the smoothed histogram

$$\hat{f}_{m,\delta}(x) = (1 - \delta)\hat{f}_m(x) + \delta. \tag{3}$$

Sampling From a Smoothed Histogram

Privacy

Theorem 5 (Achieving Differential Privacy)

Let $Z = (Z_1, \ldots, Z_k)$ where $Z_1, \ldots, Z_k$ are k iid draws from $\hat{f}_{m,\delta}(x)$. If

$$k \log\left(\frac{(1-\delta)m}{n\delta} + 1\right) \leq \alpha \tag{4}$$

then α-differential privacy holds.

Sampling From a Smoothed Histogram

Privacy

Theorem 5 (Achieving Differential Privacy)

Let $Z = (Z_1, \ldots, Z_k)$ where $Z_1, \ldots, Z_k$ are k iid draws from $\hat{f}_{m,\delta}(x)$. If

$$k \log\left(\frac{(1-\delta)m}{n\delta} + 1\right) \leq \alpha \tag{4}$$

then α-differential privacy holds.

- For $\delta \to 0$ and $\frac{m}{n\delta} \to 0$, $\log(\frac{(1-\delta)m}{n\delta} + 1) = \frac{m}{n\delta}(1 + o(1)) \approx \frac{m}{n\delta}$. Thus (4) is approximately the same as requiring

$$\frac{mk}{\delta} \leq n\alpha. \tag{5}$$

  This inequation shows an interesting tradeoff between m, k, and δ.
- Sampling from the usual histogram corresponding to $\delta = 0$ does not preserve differential privacy.

Sampling From a Smoothed Histogram

Accuracy

- $\mathbb{E}$ is the expectation under the randomness due to sampling from P and due to the privacy mechanism Q_n. Thus, for any measurable function h,

$$\mathbb{E}(h(Z)) = \int \int h(z_1, \ldots, z_k) dQ_n(z_1, \ldots, z_k \,|\, x_1, \ldots, x_n) dP(x_1) \cdots P(x_n).$$

Sampling From a Smoothed Histogram

Accuracy

How to choose m, k, δ to minimize $\mathbb{E}(\rho(F, \hat{F}_Z))$ while satisfying (4):

Theorem 6 (Rate of Convergence in KS Distance)

Suppose that $Z = (Z_1, \cdots, Z_k)$ are drawn as described in the previous theorem. Suppose (2) holds. Let ρ be the KS distance. Then choosing

$$m \asymp n^{r/(6+r)}, \quad k \asymp m^{4/r} = n^{4/(6+r)}, \quad \delta = (mk/n\alpha)$$

minimizes $\mathbb{E}\rho(F, \hat{F}_Z)$ subject to (4). In this case, $\mathbb{E}\rho(F, \hat{F}_Z) = O(\frac{\sqrt{\log n}}{n^{2/(6+r)}})$.

Sampling From a Smoothed Histogram

Accuracy

How to choose m, k, δ to minimize $\mathbb{E}(\rho(F, \hat{F}_Z))$ while satisfying (4):

Theorem 6 (Rate of Convergence in KS Distance)

Suppose that $Z = (Z_1, \cdots, Z_k)$ are drawn as described in the previous theorem. Suppose (2) holds. Let ρ be the KS distance. Then choosing

$$m \asymp n^{r/(6+r)}, \quad k \asymp m^{4/r} = n^{4/(6+r)}, \quad \delta = (mk/n\alpha)$$

minimizes $\mathbb{E}\rho(F, \hat{F}_Z)$ subject to (4). In this case, $\mathbb{E}\rho(F, \hat{F}_Z) = O(\frac{\sqrt{\log n}}{n^{2/(6+r)}})$.

- This result shows how accurate the inferences are in the KS distance using the smoothed histogram sampling scheme.
- We have consistency since $\rho(F, \hat{F}_Z) = o_P(1)$ but the rate is slower than the minimax rate of convergence for density estimators in KS distance, which is $n^{-1/2}$.

Sampling From a Smoothed Histogram

Accuracy

- Define the squared L_2 distance:

$$\rho(F, \hat{F}_Z) = \int (p(x) - \hat{f}_Z(x))^2 dx, \tag{6}$$

where

$$\hat{f}_Z(x) = h^{-r} \sum_{j=1}^{m} \hat{q}_j I(x \in B_j)$$

and $\hat{q}_j = \# \{Z_i \in B_j\} / k$.

Theorem 7 (Rate of Convergence in L_2 Distance)

Assume the conditions of the previous theorem. Let ρ be the squared L_2 distance as defined in (6). Then choosing

$$m \asymp n^{r/(2r+3)}, \quad k \asymp n^{(r+2)/(2r+3)}, \quad \delta \asymp n^{-1/(r+3)}$$

minimizes $\mathbb{E}\rho(F, \hat{F}_Z)$ subject to (4). In this case, $\mathbb{E}\rho(F, \hat{F}_Z) = O(n^{-2/(2r+3)})$.

Sampling From a Smoothed Histogram

Accuracy

Theorem 7 (Rate of Convergence in L_2 Distance)

Assume the conditions of the previous theorem. Let ρ be the squared L_2 distance as defined in (6). Then choosing

$$m \asymp n^{r/(2r+3)}, \quad k \asymp n^{(r+2)/(2r+3)}, \quad \delta \asymp n^{-1/(r+3)}$$

minimizes $\mathbb{E}\rho(F, \hat{F}_Z)$ subject to (4). In this case, $\mathbb{E}\rho(F, \hat{F}_Z) = O(n^{-2/(2r+3)})$.

- We have consistency but the rate is slower than the minimax rate which is $n^{-2/(2+r)}$ (Scott 1992).

Sampling From a Perturbed Histogram

Definition

- C_j: The number of observations in bin B_j.
- $D_j = C_j + v_j$ where $v_1, \ldots, v_m$ are independent, identically distributed draws from a Laplace density with 0 and variance $8/\alpha^2$. Thus the density of v_j is $g(v) = (\alpha/4)e^{-|v|\alpha/2}$.
- $\tilde{D}_j = \max\{D_j, 0\}$
- $\hat{q}_j = \tilde{D}_j / \sum_s \tilde{D}_s$
- Define the perturbed histogram $\tilde{f}(x) = h^{-r} \sum_{j=1}^{m} \hat{q}_j I(x \in B_j)$.

Sampling From a Perturbed Histogram

Privacy

- Dwork et al. (2006) show that releasing $D = (D_1, \ldots, D_m)$ preserves differential privacy.
- We can show that $(\hat{q}_1, \ldots, \hat{q}_m)$ also preserve differential privacy, and moreover, any sample $Z = (Z_1, \ldots, Z_k)$ from $\tilde{f}$ preserve differential privacy for any k.

Sampling From a Perturbed Histogram

Accuracy

Theorem 8 (Rate of Convergence in L_2 Distance and in KS Distance)

Let $Z = (Z_1, \cdots, Z_k)$ be drawn from $\tilde{f}(x) = h^{-r} \sum_{j=1}^{m} I(x \in B_j)$. Assume that there exists a constant $1 \leq C \leq \infty$ such that $\sup_x p(x) = C$.

(1) Let ρ be the L_2 distance. Let $m \asymp n^{r/(2+r)}$ and let $k \geq n$. Then we have $\mathbb{E}\rho(F, \hat{F}_Z) = O(n^{-2/(2+r)})$.

(2) Let ρ be the KS distance. Let $m \asymp n^{r/(2+r)}$. Then $\mathbb{E}\rho(F, \hat{F}_Z) = O(\min(\frac{\log n}{n^{2/(2+r)}}, \sqrt{\frac{\log n}{n}}))$.

Sampling From a Perturbed Histogram

Accuracy

Theorem 8 (Rate of Convergence in L_2 Distance and in KS Distance)

Let $Z = (Z_1, \cdots, Z_k)$ be drawn from $\tilde{f}(x) = h^{-r} \sum_{j=1}^{m} I(x \in B_j)$. Assume that there exists a constant $1 \leq C \leq \infty$ such that $\sup_x p(x) = C$.

(1) Let ρ be the L_2 distance. Let $m \asymp n^{r/(2+r)}$ and let $k \geq n$. Then we have $\mathbb{E}\rho(F, \hat{F}_Z) = O(n^{-2/(2+r)})$.

(2) Let ρ be the KS distance. Let $m \asymp n^{r/(2+r)}$. Then $\mathbb{E}\rho(F, \hat{F}_Z) = O(\min(\frac{\log n}{n^{2/(2+r)}}, \sqrt{\frac{\log n}{n}}))$.

- The perturbation method achieves the minimax rate of convergence in L_2 while the first data-release method does not. This suggests that the perturbation method is preferable for the L_2 distance.
- The perturbation method does not achieve the minimax rate of convergence in KS distance.

Exponential Mechanism

Definition

A general exponential mechanism:

- $\xi : \mathcal{X}^n \times \mathcal{X}^k :\to [0, \infty)$: Any function.
- Each such ξ defines a different exponential mechanism.
- Let

$$\Delta \equiv \Delta_{n,k} = \sup_{\substack{x,y \in \mathcal{X}^n \\ \delta(x,y)=1}} \sup_{z \in \mathcal{X}^k} |\xi(x,z) - \xi(y,z)|. \tag{7}$$

- $\Delta_{n,k}$: The maximum change to ξ caused by altering a single entry in x.
- Let $(Z_1, \ldots, Z_k)$ be a random vector drawn from the density

$$h(z \,|\, x) = \frac{\exp(-\alpha \xi(x,z)/(2\Delta_{n,k}))}{\int_{\mathcal{X}^k} \exp(-\alpha \xi(x,s)/(2\Delta_{n,k})) ds}, \tag{8}$$

  where $\alpha \geq 0$, $z = (z_1, \ldots, z_k)$, and $x = (x_1, \ldots, x_n)$.
- Q_n has density $h(z \,|\, x)$.

Exponential Mechanism

Definition

A specific exponential mechanism:

- $\xi(x, z) = \rho(\hat{F}_x, \hat{F}_z)$
- We draw the vector $Z = (Z_1, \ldots, Z_k)$ from $h(z \,|\, x)$ where

$$h(z \,|\, x) = \frac{g_x(z)}{\int_{\mathcal{X}^k} g_x(s)ds}, \quad \text{where} \tag{9}$$

$$g_x(z) = \exp\left(-\frac{\alpha\rho(\hat{F}_x, \hat{F}_z)}{2\Delta_{n,k}}\right) \quad \text{and}$$

$$\Delta \equiv \Delta_{n,k} = \sup_{\substack{x,y \in \mathcal{X}^n \\ \delta(x,y)=1}} \sup_{z \in \mathcal{X}^k} |\rho(\hat{F}_x, \hat{F}_z) - \rho(\hat{F}_y, \hat{F}_z)|.$$

Exponential Mechanism

Assumption

- Assume that P has a bounded density p.
- This is a weaker condition than (2).

Theorem 9 (Achieving Differential Privacy, McSherry and Talwar 2007)

The exponential mechanism satisfies the α-differential privacy.

Exponential Mechanism

Privacy

Theorem 9 (Achieving Differential Privacy, McSherry and Talwar 2007)

The exponential mechanism satisfies the α-differential privacy.

- This result shows that the exponential mechanism always preserves differential privacy.

Definition 10 (Small Ball Probability)

Let F denote the cumulative distribution function on $\mathcal{X}$ corresponding to P. Let $\hat{G}$ denote the empirical cdf from a sample of size k from P, and let

$$R(k, \epsilon) = P^k(\rho(F, \hat{G}) \leq \epsilon).$$

$R(k, \epsilon)$ is called the small ball probability associated with ρ.

Exponential Mechanism

Accuracy

Definition 10 (Small Ball Probability)

Let F denote the cumulative distribution function on $\mathcal{X}$ corresponding to P. Let $\hat{G}$ denote the empirical cdf from a sample of size k from P, and let

$$R(k,\epsilon) = P^k(\rho(F,\hat{G}) \leq \epsilon).$$

$R(k,\epsilon)$ is called the small ball probability associated with ρ.

- Small ball probabilities are well studied in probability theory.

Exponential Mechanism

Accuracy

Theorem 11 (Bound on Accuracy Involving Small Ball Probability)

Assume that P has a bounded density p, and that there exists $\epsilon_n \to 0$ such that

$$\mathbb{P}\left(\rho(F, \hat{F}_X) > \frac{\epsilon_n}{16}\right) = O\left(\frac{1}{n^c}\right) \tag{10}$$

for some $c > 1$. Further suppose that ρ satisfies the triangle inequality. Let $Z = (Z_1, \cdots, Z_k)$ be drawn from $g_x(z)$ given in (9). Then,

$$\mathbb{P}\left(\rho(F, \hat{F}_Z) > \epsilon_n\right) \le \frac{(\sup_x p(x))^k \exp(-3\alpha\epsilon_n/(16\Delta))}{R(k, \epsilon_n/2)} + O\left(\frac{1}{n^c}\right). \tag{11}$$

Exponential Mechanism

Accuracy

Theorem 11 (Bound on Accuracy Involving Small Ball Probability)

Assume that P has a bounded density p, and that there exists $\epsilon_n \to 0$ such that

$$\mathbb{P}\left(\rho(F, \hat{F}_X) > \frac{\epsilon_n}{16}\right) = O\left(\frac{1}{n^c}\right) \tag{10}$$

for some $c > 1$. Further suppose that ρ satisfies the triangle inequality. Let $Z = (Z_1, \cdots, Z_k)$ be drawn from $g_x(z)$ given in (9). Then,

$$\mathbb{P}\left(\rho(F, \hat{F}_Z) > \epsilon_n\right) \leq \frac{(\sup_x p(x))^k \exp(-3\alpha\epsilon_n/(16\Delta))}{R(k, \epsilon_n/2)} + O\left(\frac{1}{n^c}\right). \tag{11}$$

- This theorem bounds the accuracy of the estimator from the sanitized data by a simple formula involving the small ball probability.
- This is the first time a connection has been made between differential privacy and small ball probabilities.
- If we can choose $k = k_n$ in such a way that the RHS of (11) goes to 0, then the mechanism is consistent.

Theorem 12 (Rate of Convergence in KS Distance)

Suppose that P has a bounded density p and let $B := \log \sup_x p(x) > 0$. Let $Z = (Z_1, \cdots, Z_k)$ be drawn from $g_x(z)$ given in (9) with ρ being the KS distance. By requiring that $k_n \asymp (\frac{3\alpha}{B})^{2/3} n^{2/3}$, we have for $\epsilon_n = 2(\frac{B}{3\alpha})^{1/3} n^{-1/3}$, and for ρ being the KS distance,

$$\rho(F, \hat{F}_Z) = O_P(\epsilon_n). \tag{12}$$

Exponential Mechanism

Accuracy

Theorem 12 (Rate of Convergence in KS Distance)

Suppose that P has a bounded density p and let $B := \log \sup_x p(x) > 0$. Let $Z = (Z_1, \cdots, Z_k)$ be drawn from $g_x(z)$ given in (9) with ρ being the KS distance. By requiring that $k_n \asymp (\frac{3\alpha}{B})^{2/3} n^{2/3}$, we have for $\epsilon_n = 2(\frac{B}{3\alpha})^{1/3} n^{-1/3}$, and for ρ being the KS distance,

$$\rho(F, \hat{F}_Z) = O_P(\epsilon_n). \tag{12}$$

- $\rho(F, \hat{F}_Z)$ converges to 0 at a slower rate than $\rho(F, \hat{F}_X)$.
- In the proof, we see that (10) holds for some constant $c > 1/2$.
- Thus, the rate after sanitization is $n^{-1/3}$ which is slower than the optimal rate of $n^{-1/2}$.

Orthogonal Series Density Estimation

Assumption

- Take $r = 1$.
- $\{1, \psi_1, \psi_2, \dots\}$: An orthonormal basis for $L_2(0,1) = \left\{ f : \int_0^1 f^2(x)dx < \infty \right\}$.
- Hence

$$p(x) = 1 + \sum_{j=1}^{\infty} \beta_j \psi_j(x), \quad \text{where} \quad \beta_j = \int_0^1 \psi_j(x) p(x) dx,$$

  for $p \in L_2(0,1)$.
- Assume that the basis functions are uniformly bounded so that

$$c_0 \equiv \sup_j \sup_x |\psi_j(x)| < \infty. \tag{13}$$

Orthogonal Series Density Estimation

Assumption

- $\mathcal{B}(\gamma, C)$: The Sobolev ellipsoid

$$\mathcal{B}(\gamma, C) = \left\{ \beta = (\beta_1, \beta_2, \dots) : \sum_{j=1}^{\infty} \beta_j^2 j^{2\gamma} \leq C^2 \right\},$$

  where $\gamma > 1/2$.

- Let

$$\mathcal{P}(\gamma, C) = \left\{ p(x) = 1 + \sum_{j=1}^{\infty} \beta_j \psi_j(x) : \beta \in \mathcal{B}(\gamma, c) \right\}.$$

- Assume that $p \in \mathcal{P}(\gamma, C)$.
- The minimax rate of convergence in L_2 norm for $\mathcal{P}(\gamma, C)$ is $n^{-2\gamma/(2\gamma+1)}$ (Efromovich 1999).

Orthogonal Series Density Estimation

Definition of Exponential Mechanism

- $\|u\|_{l_2} = (\int_0^1 |u(x)|^2 dx)^{1/2}$ for a function $u \in L_2(0,1)$, which is a norm on $L_2(0,1)$.
- Consider an exponential mechanism based on

$$\xi(X,Z) = \left(\int (\hat{p}(x) - \hat{p}^*(x))^2 dx\right)^{1/2} := \|\hat{p} - \hat{p}^*\|_{l_2}, \quad \text{where} \tag{14}$$

$$\hat{p}(x) = 1 + \sum_{j=1}^{m_n} \hat{\beta}_j \psi_j(x), \quad m_n = n^{1/(2\gamma+1)} \quad \text{and} \quad \hat{\beta}_j = n^{-1} \sum_{i=1}^{n} \psi_j(X_i). \tag{15}$$

$$\hat{p}^*(x) = 1 + \sum_{j=1}^{m_k} \hat{\beta}_j^* \psi_j(x), \quad m_k = k^{1/(2\gamma+1)} \quad \text{and} \quad \hat{\beta}_j^* = k^{-1} \sum_{i=1}^{k} \psi_j(Z_i). \tag{16}$$

Lemma 13 (Definition of Exponential Mechanism)

Under the above scheme we have $\Delta \leq \frac{2c_0^2 m_n}{n}$ for c_0 as defined in (13). Hence,

$$g(z \,|\, x) = \exp\left(-\frac{\alpha \left\|\hat{p}^* - \hat{p}\right\|_{l_2}}{\Delta}\right)$$

$$\leq \exp\left(-\frac{\alpha n \left\|\hat{p}^* - \hat{p}\right\|_{l_2}}{2c_0^2 m_n}\right) \quad \text{almost surely.} \tag{17}$$

Theorem 14 (Rate of Convergence in L_2 Distance)

Let $Z = (Z_1, \cdots, Z_k)$ be drawn from $g_x(z)$ given in (17). Assume that $\gamma > 1$. If we choose $k \asymp \sqrt{n}$ then

$$\rho^2(p, \hat{p}^*) = O_P(n^{-\gamma/(2\gamma+1)}).$$

Theorem 14 (Rate of Convergence in L_2 Distance)

Let $Z = (Z_1, \cdots, Z_k)$ be drawn from $g_x(z)$ given in (17). Assume that $\gamma > 1$. If we choose $k \asymp \sqrt{n}$ then

$$\rho^2(p, \hat{p}^*) = O_P(n^{-\gamma/(2\gamma+1)}).$$

- The sanitized estimator converges at a slower rate than the minimax rate.

Orthogonal Series Density Estimation

Definition of Perturbation Approach

- Let $Z = (Z_1, \ldots, Z_k)$ be an iid sample from

$$\hat{q}(x) = 1 + \sum_{j=1} m_n(\hat{\beta}_j + v_j)\psi_j(x),$$

  where $v_1, \ldots, v_m$ are iid draws from a Laplace distribution with density $g(v) = (n\alpha/(2c_0 m))e^{-n\alpha|v|/(c_0 m)}$.
- If $\hat{q}(x) < 0$ for any x then we replace $\hat{q}$ by $\hat{q}(x)I(\hat{q}(x) > 0)/\int \hat{q}(s)I(\hat{q}(s) > 0)ds$ as in Hall and Murison (1993).
- We can show that, for any k, this preserves differential privacy.

Theorem 15 (Rate of Convergence in L_2 Distance)

Let $Z = (Z_1, \cdots, Z_k)$ be drawn from $\hat{q}$. Assume that $\gamma > 1$. If we choose $k \geq n$, then

$$\rho^2(p, \hat{p}_Z) = O_P(n^{-2\gamma/(2\gamma+1)})$$

where $\hat{p}_Z$ is the orthogonal series density estimator based on Z.

Theorem 15 (Rate of Convergence in L_2 Distance)

Let $Z = (Z_1, \cdots, Z_k)$ be drawn from $\hat{q}$. Assume that $\gamma > 1$. If we choose $k \geq n$, then

$$\rho^2(p, \hat{p}_Z) = O_P(n^{-2\gamma/(2\gamma+1)})$$

where $\hat{p}_Z$ is the orthogonal series density estimator based on Z.

- The perturbation technique achieves the minimax rate of convergence and so appears to be superior to the exponential mechanism.

Summary of Results

Result 1

If the data are in $\mathbb{R}^r$ and the density p of P is Lipschitz, the rates of convergence are reported below.

Table 1:

	Distance	L^2	Kolmogorov-Smirnov
Data-release mechanism	Smoothed histogram	$n^{-2/(2r+3)}$	$\sqrt{\log n} \times n^{-2/(6+r)}$
	Perturbed histogram	$n^{-2/(2+r)}$	$\min(\sqrt{\log n/n}, \log n \times n^{-2/(2+r)})$
	Exponential mechanism	NA	$n^{-1/3}$
	Minimax rate	$n^{-2/(2+r)}$	$n^{-1/2}$

Summary of Results

Result 2

If the dimension of X is $r = 1$ and the density p is assumed to be in a Sobolev Space of order γ, the rates of convergence are reported below.

Table 2:

	Distance	L^2
Data-release mechanism	Exponential mechanism	$n^{-\gamma/(2\gamma+1)}$
	Perturbed orthogonal series estimator	$n^{-2\gamma/(2\gamma+1)}$
	Minimax rate	$n^{-2\gamma/(2\gamma+1)}$

Example

Simulation

Consider a small simulation study to see the effect of perturbation on accuracy.

- We focus on the histogram perturbation method with $r = 1$.
- We take the true density of X to be a Beta$(10, 10)$ density.
- We considered sample sizes $n = 100$ and $n = 1000$ and privacy levels $\alpha = 0.1$ and $\alpha = 0.01$.
- We take ρ to be squared error distance.

Example

Results

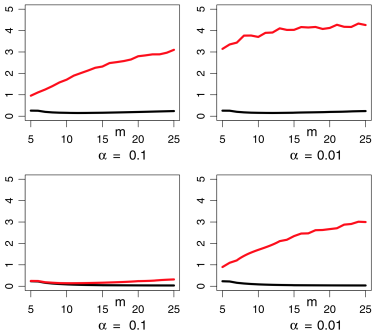

Figure 1: Top two plots $n = 100$. Bottom two plots $n = 1000$. Each plot shows the mean integrated squared error of the histogram. The lower line is from the histogram based on the original data. The upper line is based on the perturbed histogram.

Example

Conclusion

- Smaller values of α induce a larger information loss which manifests itself as a larger mean squared error.
- Despite the fact that the perturbed histogram achieves the minimax rate, the error is substantially inflated by the perturbation. This means that the constants in the risk are important, not just the rate.
- The risk of the sanitized histograms is much more sensitive to the choice of the number of cells than the original histogram is.

Conclusion

Differential Privacy

- Goal:
  - To present the idea in statistical language.
  - To compare mechanisms by distance functions.
- Two histogram based mechanisms: Both lead to differential privacy.
  - Smoothed: Slower rate.
  - Perturbed: Faster rate, but large risk and sensitive to the choice of the smoothing parameter.
- Exponential mechanism: Accuracy linked to small ball probabilities.
- Minimaxity: Desirable, but achieved only in some cases.

References

- McSherry, F., and Talwar, K. (2007), "Mechanism Design via Differential Privacy," in *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, New York: Springer, pp. 94–103. [375–377]
- Scott, D. W. (1992), *Multivariate Density Estimation: Theory, Practice, and Visualization*, New York: Wiley. [378]
- Dwork, C., McSherry, F., Nissim, K., and Smith, A. (2006), "Calibrating Noise to Sensitivity in Private Data Analysis," in *Proceedings of the 3rd Theory of Cryptography Conference*, New York: Springer, pp. 265?284. [375,377,379]
- Efromovich, S. (1999), *Nonparametric Curve Estimation: Methods, Theory and Applications*, New York: Springer-Verlag. [380,387]
- Hall, P., and Murison, R. D. (1993), "Correcting the Negativity of High-Order Kernel Density Estimators," *Journal of Multivariate Analysis*, 47, 103–122. [380]