Lecture 15 Propose-Test-Release

Yu-Xiang Wang
Logistics

• Please submit your HW2.

• The coding part should be pretty easy given my template.
  • Let me know if you run into troubles.

• HW3 will be light-weighted so you have time to work on your project.
Recap: Beyond worst-case noise in DP query release

- Global sensitivity
  \[ CS_q(x) = \max_{x' \sim x} \|q(x) - q(x')\| \]

- Local sensitivity
  \[ LS_q(x) = \max \{ |q(x) - q(x')| : x' \sim x \} \]

- Smooth sensitivity
  \[ SS_q(x, \beta) = \max \left\{ LS_q(x), \max_{x' \sim x} LS_q(x', \beta) \cdot e^{-\beta d(x, x')} \right\} \]
Recap: Admissible noise

**Notation.** For a subset $S$ of $\mathbb{R}^d$, we write $S + \Delta$ for the set $\{z + \Delta \mid z \in S\}$, and $e^\lambda \cdot S$ for the set $\{e^\lambda \cdot z \mid z \in S\}$. We also write $a \pm b$ for the interval $[a - b, a + b]$.

**Definition 2.5 (Admissible Noise Distribution).** A probability distribution on $\mathbb{R}^d$, given by a density function $h$, is $(\alpha, \beta)$-admissible (with respect to $\ell_1$) if, for $\alpha = \alpha(\epsilon, \delta)$, $\beta = \beta(\epsilon, \delta)$, the following two conditions hold for all $\Delta \in \mathbb{R}^d$ and $\lambda \in \mathbb{R}$ satisfying $\|\Delta\|_1 \leq \alpha$ and $|\lambda| \leq \beta$, and for all measurable subsets $S \subseteq \mathbb{R}^d$:

* Sliding Property:*
  \[
  \Pr_{Z \sim h} \left[Z \in S\right] \leq e^{\frac{\epsilon}{2}} \cdot \Pr_{Z \sim h} \left[Z \in S + \Delta\right] + \frac{\delta}{2}.
  \]

* Dilation Property:*
  \[
  \Pr_{Z \sim h} \left[Z \in S\right] \leq e^{\frac{\epsilon}{2}} \cdot \Pr_{Z \sim h} \left[Z \in e^\lambda \cdot S\right] + \frac{\delta}{2}.
  \]

![Figure 1: Sliding and dilation for the Laplace distribution with p.d.f. $h(z) = \frac{1}{2}e^{-|z|}$, plotted as a solid line. The dotted lines plot the densities $h(z + 0.3)$ (left) and $e^{0.3}h(e^{0.3}z)$ (right).](image)

• Then $A(x) = f(x) + \left[\frac{S(x)}{\alpha}\right] \cdot Z$ satisfies $(\epsilon, \delta)$-DP.
Recap: Summary of the noises that are known to work

- Cauchy distribution
- Student t-distribution
- Laplace-log-normal
- Uniform-log-normal
- Arcsinh-normal
- Gaussian
- Laplace
Recap: Laplace-log-normal noise and CDP

• Adding log-normal noise

\[ Z = X \cdot e^{\sigma Y} \]

• X drawn from Laplace and Y from a standard Normal.

**Proposition 3.** Let \( f : \mathcal{X}^n \rightarrow \mathbb{R} \) and let \( Z \leftarrow \text{LLN}(\sigma) \) for some \( \sigma > 0 \). Then, for all \( s, t > 0 \), the algorithm \( M(x) = f(x) + \frac{1}{s} \cdot S_f(x) \cdot Z \) guarantees \( \frac{1}{2} \varepsilon^2 \)-CDP for \( \varepsilon = t/\sigma + e^{3\sigma^2/2s} \).

This lecture

• Finish smooth sensitivity
  • Sketching the idea of the zCDP proof for Laplace log-normal.
  • Empirical results on truncated mean.

• Propose-Test-Release

• Easy-to-use recipes for PTR and examples
Reading materials

• Vadhan book Section 3.2 – 3.4

• Dwork and Lei “Differential Privacy and Robust Statistics”
  • Original paper for PTR.

  • A good example for deriving data—dependent DP algorithm
Concentrated DP analysis of Smoothed Sensitivity

• Adding log-normal noise

\[ Z = X \cdot e^{\sigma Y} \]

• X drawn from Laplace and Y from a standard Normal.

**Proposition 3.** Let \( f : \mathcal{X}^n \to \mathbb{R} \) and let \( Z \leftarrow \text{LLN}(\sigma) \) for some \( \sigma > 0 \). Then, for all \( s, t > 0 \), the algorithm \( M(x) = f(x) + \frac{1}{s} \cdot S^t_f(x) \cdot Z \) guarantees \( \frac{1}{2} \varepsilon^2 \)-CDP for \( \varepsilon = \frac{t}{\sigma} + e^{3\sigma^2/2} s \).

Summary of the noises that are known to work

• Cauchy distribution
• Student t-distribution
• Laplace-log-normal
• Uniform-log-normal
• Arcsinh-normal
• Gaussian
• Laplace
Sketch of the proof for the Laplace-Log-Normal

• Let’s say for all neighboring datasets
  \[ |f(x) - f(x')| \leq g(x) \quad \text{and} \quad e^{-t}g(x) \leq g(x') \leq e^{t}g(x). \]

• Algorithm: \[ M(x) = f(x) + \frac{g(x)}{s} \cdot Z \quad \text{for} \quad Z \leftarrow \text{LLN}(\sigma). \]

• We have that
  \[ D_{\alpha}(M(x) \| M(x')) = D_{\alpha}\left(Z \left\| \frac{f(x') - f(x)}{g(x)} \cdot s + \frac{g(x')}{g(x)} \cdot Z \right\| \right). \]

  \[ \leq \max \left\{ D_{\alpha}(Z \| s + e^{t}Z), D_{\alpha}(s + e^{t}Z \| Z) \right\} \]
Technical tools

• Group privacy for CDP:

**Lemma 11.** Let $P, Q, R$ be probability distributions. Suppose $D_\alpha (P\|R) \leq a \cdot \alpha$ and $D_\alpha (R\|Q) \leq b \cdot \alpha$ for all $\alpha \in (1, \infty)$. Then, for all $\alpha \in (1, \infty)$,

$$D_\alpha (P\|Q) \leq \alpha \cdot (\sqrt{a} + \sqrt{b})^2 \leq 2 \alpha \cdot (a + b).$$

• Decompose what we want to bound

$$D_\alpha (Z\|e^t Z + s)$$

$$D_\alpha (e^t Z + s\|Z)$$
Bounding the two parts separately

Lemma 19. Let $Z \leftarrow \text{LLN}(\sigma)$ for $\sigma > 0$. Let $t \in \mathbb{R}$ and $\alpha \in (1, \infty)$. Then

$$D_\alpha (Z \| e^t Z) \leq \frac{\alpha t^2}{2\sigma^2}.$$

**Proof:**

$$D_\alpha (Z \| e^t Z) = D_\alpha (X e^{\sigma Y} \| X e^{\sigma Y + t}) \leq \sup_x D_\alpha (x e^{\sigma Y} \| x e^{\sigma Y + t}) \leq D_\alpha (\sigma Y \| \sigma Y + t).$$

Lemma 20. Let $Z \leftarrow \text{LLN}(\sigma)$ for $\sigma > 0$. Let $s \in \mathbb{R}$ and $\alpha \in (1, \infty)$. Then

$$D_\alpha (Z \| Z + s) \leq \min \left\{ \frac{1}{2} e^{3\sigma^2} s^2 \alpha, e^{\frac{3}{2} \sigma^2} s \right\}.$$

**Proof:**

$$\left[ \log \text{clarsity ratio} \right] \leq e^{\frac{3}{2} \sigma^2} s.$$
Improvement from running smoothed sensitivity is substantial!

\[ \text{trim}_m(x) = \frac{x(m+1) + x(m+2) + \cdots + x(n-m)}{n - 2m}, \]

Drawbacks of Smooth Sensitivity

• Restricted to numerical valued outputs.

• Requires elaborate design of the noise, generally with a much heavier tail

• Does not generalize well to high-dimension

• Are there more flexible recipes for deriving data-dependent DP algorithms?
Example: Releasing reciprocal

- Let $f(D)$ be a counting query, define $g(D) = 1/f(D)$
  - What is the global and local sensitivity of $g(D)$?
  - What is the smooth sensitivity of $g(D)$?

Example: the prediction variance of linear regression on a new dataset
  - Useful for statistical inference / uncertainty quantification
Examples: Private Argmax

• Voting: Who won the election?

• Model selection: Which is the best performing model when evaluating on a private dataset?

• Netflix: What is the Top-k most-popular movie last week?

\[
\text{argmax}_{S \in |\{S|\text{ok}\}} \sum_{c \in \mathcal{N}} \text{popularity}(c) \\
S \\
S \\
\mathcal{N} \\
\text{popularity}(c)
\]
Release Stable Values without adding noise.

Define “Dist2Instability” function:

\[
\text{Dist2Instability}(x) = \text{dist}(x, x') - \frac{1}{\text{cap}(\frac{1}{\varepsilon})} \\
\text{How many 'step' before x' becomes x'}
\]

“Dist2Instability”:

1. \[d_0 = d(x) + \text{cap}(\frac{1}{\varepsilon})\]

2. if \[d > \frac{\log \frac{1}{\delta}}{\varepsilon}\], then output \(f(x)\)
   else (\(d \leq \frac{\log \frac{1}{\delta}}{\varepsilon}\)), then output “\(L\)"
The privacy analysis of 
“Dist2Instability”

- Case A: $f(x') \neq f(x) \Rightarrow d(x) = d(x') = 0$
  
- Case B: $d(x) = 0 \Rightarrow \exists x' \text{ neighbor of } x, \ d(x') = 0$

\[ d(x') = \max_d \{d(x', x) : f(x') \neq f(x)\} \]

\[ \text{choose } x' = x \]

\[ d(x') = \min \{d(x', x') - 1 : f(x') \neq f(x)\} = 0 \]

output is $\{ \}$ in face process of Lap Mechanism.

\[ \frac{d}{\epsilon} > \frac{\log \frac{1}{1-\delta}}{\epsilon} \]

\[ d = \Delta x + \log \left(\frac{1}{1-\delta}\right) \]
Utility of “Dist2Instability”

• Perfect utility with high probability when “margin is large”

• No utility at all when the margin is small.

• Comparing to exponential mechanism
  • Homework 3 question.
Propose-Test-Release

1. Propose a bound on local-sensitivity $\beta$

2. Test the validity of this bound
   $\hat{d} = d(x, \{x' : LS_q(x') > \beta\}) + \text{Lap}(1/\varepsilon)$,

3. Release:
   \[
   \text{return } q(x) + \text{Lap}(\frac{\beta}{\varepsilon}) \text{ if } \hat{d} > \frac{\log \frac{1}{\delta}}{\varepsilon}
   \]
   \[
   \text{else return } "\text{no}"
   \]

**Proposition 3.2** (propose-test-release [33]). For every query $q : X^n \rightarrow \mathbb{R}$ and $\varepsilon, \delta, \beta \geq 0$, the above algorithm is $(2\varepsilon, \delta)$-differentially private.
The privacy analysis of PTR

• Case 1: 

\[ L_q(x) > \beta \Rightarrow d(x, q'' \mid L_q(x'') > \beta) = 0 \]

\[ \delta_q = 0 + \text{Cov} \left( \frac{1}{\varepsilon} \right) \]

\[ P \left( d(x) > \frac{1}{\varepsilon} \right) \leq \delta \]

\[ \text{Prob} \left( m(x) \in S \right) = \text{Prob} \left( m(x) \in \mathbb{R} \setminus \mathbb{E} \right) + \text{Prob} \left( m(x) \in \mathbb{R} \setminus \mathbb{E} \right) = \delta \]

\[ \text{Prob} \left( m(x) = "I" \right) \leq e^{\varepsilon} \text{Prob} \left( m(x) \in \mathbb{R} \setminus \mathbb{E} \right) + \delta \]

• Case 2:

\[ L_q(x) \leq \beta \]

\[ |q(x) - q(x')| \leq \beta \]

Laplace mechanism that outputs \[ M(x) \in \{ \varepsilon \text{-DP} \} \]

Composition of \[ \varepsilon \text{-DP} \] and \[ \delta(x) + \log \left( \frac{1}{2\varepsilon} \right) \]

Post-processing of \[ \varepsilon \text{-DP} \]
Two remaining issues with PTR

1. How do I know what bound to propose?

2. Isn’t it still relying on local sensitivity and noise-adding? How does it help to go beyond releasing numerical queries?
How do I know what bound to propose? Privately releasing “a high probability bound” of local sensitivity.

- Example: Estimating the number of triangles in a graph under Edge Differential Privacy.

- Global sensitivity: $n-2$

- Local sensitivity: the max degree of $G$

- Private releasing local sensitivity?
Privacy analysis of the approach to release local sensitivity privately.

**Lemma:** Let \( \tilde{\Delta}_f(D) \) satisfies \( \varepsilon \)-DP and
\[
\mathbb{P} \left[ \Delta_f(D) \geq \tilde{\Delta}_f(D) \right] \leq \delta
\]
Then \( f(D) + \text{Lap}(\tilde{\Delta}_f(D)/\varepsilon) \) satisfies \((2\varepsilon, \delta)\)-DP.

**Proof:**
\[
\Delta \text{ is } \varepsilon \text{-DP, } y = f(x) + \text{Lap}(\tilde{\Delta}_f(D)/\varepsilon) - \varepsilon x
\]
Beyond local sensitivity / noise-adding approaches

• What happens when the output space is not numerical?

• How to design data-adaptive versions of posterior-sampling, or objective-perturbation, or NoisySGD rather than just noise adding?
Topic of the next (and final) lecture

• Beyond local sensitivity
  • Per-instance differential privacy
  • pDP to DP conversion

• Data-dependent algorithms in differentially private machine learning