Differential Privacy: Algorithmic Building Blocks

CompSci 590.03
Instructor: Ashwin Machanavajjhala
Announcement

• Choose project ideas by next Thursday.

• Please meet with me at least once before then to discuss your project idea.

• Sample project ideas posted online.

• You can choose your own project (that is not listed on the webpage).
Differential Privacy

For every pair of inputs that differ in one row

\[ \frac{\Pr[A(D_1) = O]}{\Pr[A(D_2) = O]} \] < \( \varepsilon \) \( (\varepsilon > 0) \)

Adversary should not be able to distinguish between any \( D_1 \) and \( D_2 \) based on any \( O \)

[Dwork ICALP 2006]

For every output ...

\[ \text{Lecture 6: 590.03 Fall 16} \]
Algorithms

• Non-trivial deterministic algorithms do not satisfy differential privacy
  – Necessary condition: for every input database D and every output O, we need \( \Pr[A(D) = O] > 0 \) for any differentially private algorithm A.

• Random sampling does not satisfy differential privacy
  – Violates the above necessary condition
Laplace Mechanism

• Suppose $q$ is a query on the database that returns a vector of reals in $\mathbb{R}^d$.

• $S(q) = \max_{\text{neighbors } D, D'} ||q(D) - q(D')||_1$

• Let $n = [n_1, n_2, ..., n_d]$ be a vector of noise values, each drawn independently and identically from $\text{Lap}(S(q)/\varepsilon)$

• Returning $q(D) + n$ results in $\varepsilon$-differential privacy.
Lecture 6: 590.03 Fall 16
Error Analysis

• If true count is $c$.

• Noisy count is $c'$.

• $|c - c'| < S(q)/\varepsilon \log(1/\delta)$ with probability $1-\delta$
This means ...

• Sum of all cells may not add up to the true total count.

• Some cells can have negative counts

• Cells can have fractional counts.
Limitations of output perturbation

• What if the answer is non-numeric?
  – “what is the most common nationality in this room”: Chinese/Indian/American...
  – Other examples?

• What if the perturbed answer is not as good as the real answer?
  – “Which price would bring the most money from a set of buyers?”
Example: Items for sale

- If price is set at $100, make a revenue of $400
- If price is set at $401, make a revenue of $401

- Best price: $401, Next best: $100

- Revenue at $402 = $0
- Revenue at $101 = $101
Exponential Mechanism

- Consider some algorithm A (can be deterministic or probabilistic):

- How to construct a differentially private version of A?
Exponential Mechanism

• Construct a scoring function \( w: \text{Inputs} \times \text{Outputs} \rightarrow \mathbb{R} \)

• For good utility \( w(D,O) \) should mirror the true algorithm as well as possible.
Exponential Mechanism

• Construct a scoring function $w: Inputs \times Outputs \rightarrow R$

• Sensitivity of $w$

$$\max_O \max_{D,D'} |w(D,O) - w(D',O)|$$

where $D, D'$ differ in one tuple
Exponential Mechanism

Algorithm $\mathcal{E}_w^\varepsilon(D)$

• Given an input $D$, and a scoring function $w$,
  Randomly sample an output $O$ from $Outputs$ with probability

$$\frac{\varepsilon}{e^{2\Delta} \cdot w(D,O)}$$

$$\sum_{Q \in Outputs} e^{\frac{\varepsilon}{2\Delta} \cdot w(D,Q)}$$

• Note that for every output $O$, probability $O$ is output $> 0$. 
Theorem

Algorithm $\mathcal{E}_w^\varepsilon(D)$ satisfies $\varepsilon$ differential privacy.
Utility of the Exponential Mechanism

• Depends on the choice of scoring function – weight given to the best output.

• E.g.,
  “What is the most common nationality?”
  \( w(D, \text{nationality}) = \# \text{ people in } D \text{ having that nationality} \)

Sensitivity of \( w \) is 1.

• Q: What will the output look like?
Utility of Exponential Mechanism

• Let $\text{OPT}(D) = \text{nationality with the max score}$
• Let $\mathcal{O}_{\text{OPT}} = \{O \in \text{Outputs} : w(D,O) = \text{OPT}(D)\}$

• Let the exponential mechanism return an output $O^*$

Theorem:

$$\Pr\left[w(D, O^*) \leq \text{OPT}(D) - \frac{2\Delta}{\varepsilon}\left(\log \frac{|\text{Outputs}|}{|\mathcal{O}_{\text{OPT}}|} + t\right)\right] \leq e^{-t}$$
Utility of Exponential Mechanism

Theorem:

\[
\Pr \left[ w(D, O^*) \leq OPT(D) - \frac{2\Delta}{\epsilon} \left( \log \frac{|Outputs|}{|O_{OPT}|} + t \right) \right] \leq e^{-t}
\]

Suppose there are 4 nationalities

Outputs = \{Chinese, Indian, American, Greek\}

Exponential mechanism will output some nationality that is shared by at least K people with probability \(1-e^{-3}(=0.95)\), where

\[
K \geq OPT - 2(\log(4) + 3)/\epsilon = OPT - 6.8/\epsilon
\]
Laplace versus Exponential Mechanism

• Let $f$ be a function on tables that returns a real number.

• Define: score function $w(D,O) = |f(D) - O|

• Sensitivity of $w = \max_{D,D'} (|f(D) - O| - |f(D') - O|)
  \leq \max_{D,D'} |f(D) - f(D')| = \text{sensitivity of } f$

• Exponential mechanisms returns an output $f(D) + \eta$ with probability proportional to

$$e^{\frac{\epsilon}{2\Delta} |f(D) - f(D') - \eta|}$$

Laplace noise with parameter $2\Delta/\epsilon$
Summary of Exponential Mechanism

• Differential privacy for cases when output perturbation does not make sense.

• Idea: Make better outputs exponentially more likely; Sample from the resulting distribution.

• Every differentially private algorithm is captured by exponential mechanism.
  – By choosing the appropriate score function.
Summary of Exponential Mechanism

• Utility of the mechanism only depends on $\log(|\text{Outputs}|)$
  – Can work well even if output space is exponential in the input

• However, sampling an output may not be computationally efficient if output space is large.
Statistical Database Privacy (untrusted collector)

Perturb records to ensure privacy for individuals and utility for server
Randomized Response (a.k.a. local randomization)

With probability $p$, Report true value
With probability $1-p$, Report flipped value
Differential Privacy Analysis

- Consider 2 databases $D, D'$ (of size $M$) that differ in the $j^{th}$ value
  - $D[j] \neq D'[j]$. But, $D[i] = D'[i]$, for all $i \neq j$

- Consider some output $O$

\[
\frac{P(D \rightarrow O)}{P(D' \rightarrow O)} \leq e^\varepsilon \iff \frac{1}{1 + e^\varepsilon} < p < \frac{e^\varepsilon}{1 + e^\varepsilon}
\]
Utility Analysis

• Suppose n1 out of N people replied “yes”, and rest said “no”
• What is the best estimate for $\pi = \text{fraction of people with disease } = Y$?
  $$\pi_{\text{hat}} = \frac{n1/n - (1-p)}{(2p-1)}$$

• $E(\pi_{\text{hat}}) = \pi$

• $\text{Var}(\pi_{\text{hat}}) =$
  $$\frac{\pi(1 - \pi)}{n} + \frac{1}{n(16(p - 0.5)^2 - 0.25)}$$

  Sampling Variance due to coin flips
Laplace Mechanism vs Randomized Response

Privacy

• Provide the same $\varepsilon$-differential privacy guarantee

• Laplace mechanism assumes data collected is trusted

• Randomized Response does not require data collected to be trusted
  – Also called a *Local* Algorithm, since each record is perturbed
Laplace Mechanism vs Randomized Response

Utility

• Suppose a database with N records where μN records have disease = Y.
• Query: # rows with Disease=Y

• Std dev of Laplace mechanism answer: O(1/ε)
• Std dev of Randomized Response answer: O(√N/ε)
Randomized response for larger domains

• Suppose area is divided into $k \times k$ uniform grid.

• What is the probability of reporting the true location?

• What is the probability of reporting a false location?